System and Organization Controls (SOC) 2 Report

Report on the Description of GCommerce's Commerce Bridge Relevant to Security and Processing Integrity and on the Suitability of the Design and Operating Effectiveness of Its Controls

For the period from October 17, 2020 through October 16, 2021

With the Independent Service Auditors' Report, including tests performed and results thereof

LWBJ®
CPA | Consulting | M&A

lwbj.com

GCommerce

System and Organization Controls (SOC) 2 Report
For the period from October 17, 2020 through October 16, 2021

Contents

Section 1:

Independent Service Auditors' Report

Independent Service Auditors' Report

GCommerce
Board of Directors
Des Moines, Iowa 50309

Scope

We have examined GCommerce's (the Company or service organization) accompanying description of its Commerce Bridge titled "Management's Description of GCommerce's Commerce Bridge" for the period from October 17, 2020 through October 16, 2021 (the Description) based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (the Description Criteria) and the suitability of the design and operating effectiveness of controls stated in the Description for the period from October 17, 2020 through October 16, 2021, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to security and processing integrity (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The Company uses subservice organizations to provide data center hosting, data backup and storage services to support aspects of its Commerce Bridge. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The Description presents the Company's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Company's controls. The Description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The Description presents the Company's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the Company's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

The information included in Section 5, titled "Other Information Provided by GCommerce that is Not Covered by the Independent Service Auditors' Report" is presented by management of the Company to provide additional information and is not part of the Description. The information presented has not been

4200 University Avenue, Suite 410
West Des Moines, IA 50266
515-222-5680
www.lwbj.com

subjected to the procedures applied in the examination of the Description and of the suitability of the design and operating effectiveness of controls to achieve the Company's service commitments and system requirements based on the applicable trust services criteria, and accordingly, we express no opinion on it.

Service Organization's Responsibilities

The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled "GCommerce's Management Assertion" (the Assertion) about the Description and the suitability of design and operating effectiveness of controls stated therein. The Company is also responsible for preparing the Description and Assertion, including the completeness, accuracy, and method of presentation of the Description and Assertion; providing the services covered by the Description; selecting the applicable trust services criteria and stating the related controls in the Description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of design and operating effectiveness of controls stated in the Description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the Description is presented in accordance with the Description Criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the Company's service commitments and system requirements.
- Assessing the risks that the Description is not presented in accordance with the Description Criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the Description Criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the Description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.

- Evaluating the overall presentation of the Description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, "Independent Service Auditors' Description of Procedures Conducted Regarding Controls and Results" of this report.

Controls That Did Not Operate During the Period Covered by the Report

The Company's accompanying description of the Commerce Bridge discusses its Incident Response Plan, which includes the controls implemented and operated to respond to, and recover from, security incidents. However, during the period from October 17, 2020 through October 16, 2021, the Company did not experience a security incident that would warrant the operation of the Incident Response Plan. Because these controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using trust services criteria CC7.3. CC7.4 or CC7.5. Similarly, the Description discusses sanitization mechanisms and procedures in place prior to equipment disposal, re-use or release from GCommerce's control. However, during the period from October 17, 2020 through October 16, 2021, the Company did not dispose, re-use or release equipment from the Company's control that would warrant the operation of sanitation mechanisms and procedures. Because these controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using trust services criteria CC6.5. In addition, the Description discusses the Company's new vendor selection process. However, during the period from October 17, 2020 through October 16, 2021, the Company did not obtain any new vendors that would warrant the operation of the new vendor selection procedures. Because this control did not operate during the period, we were unable to test, and did not test, the operating effectiveness of the control as evaluated using trust services criteria CC9.2.

Opinion

In our opinion, in all material respects,

a) The Description presents the Company's Commerce Bridge, that was designed and implemented for the period from October 17, 2020 through October 16, 2021, in accordance with the Description Criteria.

b) The controls stated in the Description were suitably designed for the period from October 17, 2020 through October 16, 2021, to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of the Company's controls throughout that period.

c) The controls stated in the Description operated effectively for the period from October 17, 2020 through October 16, 2021, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Company's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of the Company, user entities of Company's Commerce Bridge during some or all of the period from October 17, 2020 through October 16, 2021, business partners of the Company subject to risks arising from interactions with the Commerce Bridge, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

LWBJ, LLP

December 28, 2021
West Des Moines, IA

Section 2:
GCommerce's Management Assertion

700 Locust Street, Suite 201
Des Moines, IA 50309

GCommerce's Management Assertion

We have prepared the accompanying description titled "Management's Description of GCommerce's Commerce Bridge" for the period from October 17, 2020 through October 16, 2021 (the Description) based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (the Description Criteria). The Description is intended to provide report users with information about GCommerce's (the Company) Commerce Bridge that may be useful when assessing the risks arising from interactions with the Company's system, particularly information about system controls that the Company has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and processing integrity (the applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The Company uses subservice organizations to provide data center hosting, data backup and storage services to support aspects of its Commerce Bridge. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The Description presents the Company's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Company's controls. The Description does not disclose the actual controls at the subservice organizations.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The Description presents the service organization's controls, the applicable trust service criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

The Description discusses the Company's Incident Response Plan, which includes the controls implemented and operated to respond to, and recover from, security incidents. However, during the period from October 17, 2020 through October 16, 2021, the Company did not experience a security incident that would warrant the operation of the Incident Response Plan for the applicable trust services criteria CC7.3. CC7.4 or CC7.5. Similarly, the Description discusses sanitization mechanisms and procedures in place prior to equipment disposal, re-use or release from GCommerce's control. However, during the period from October 17, 2020 through October 16, 2021, the Company did not dispose, re-use or release equipment from the Company's controls that would warrant the operation of sanitation mechanisms and procedures for applicable trust services criteria CC6.5. In addition, the Description discusses the Company's new vendor selection process. However, during the period from October 17, 2020 through October 16, 2021, the Company did not obtain any new vendors that would warrant the operation of the new vendor selection procedures for applicable trust services criteria CC9.2.

We confirm, to the best of our knowledge and belief, that:

1) The Description presents the Commerce Bridge that was designed and implemented for the period from October 17, 2020 through October 16, 2021 in accordance with the Description Criteria.

2) The controls stated in the Description were suitably designed for the period from October 17, 2020 through October 16, 2021 to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of the Company's controls throughout that period.

3) The controls stated in the Description operated effectively for the period from October 17, 2020 through October 16, 2021 to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization and user entity controls assumed in the design of the Company's controls operated effectively throughout that period.

Management of GCommerce

Section 3:

Management's Description of GCommerce's Commerce Bridge

Management's Description of GCommerce's Commerce Bridge
For the Period from October 17, 2020 through October 16, 2021

Company Overview

Formed in 2000 and based in Des Moines, Iowa, GCommerce (the Company) is a leading provider of cloud-based automation solutions to the durable goods distribution industries. The Company's services reduce the time and expense of electronic document exchange and enable E-Commerce in the distribution supply chain. More specifically, GCommerce drives commerce in the automotive and industrial aftermarkets through an interoperable suite of software solutions called the Commerce Bridge. The Commerce Bridge helps the distribution supply chain increase sales at decreased operational costs through:

- Electronic Messaging
- Supply Chain Visibility
- Product Data Content
- Fulfillment
- Web Store Front
- Business Analytics

GCommerce manages an extensive network of trading partner connections including over 2,000 manufacturer distributors and retailer customers. This results in over 6,000+ trading partner connections which facilitate more than 30 million transactions per year to the markets the Company serves. The Commerce Bridge is a suite of products designed to offer a full scope of solutions to distribution supply chain markets. The Commerce Bridge is a suite of interoperable solutions enabling clients to identify, locate, buy, and track shipments, reconcile receipts, and report on activity. It allows retailers, distributors, and suppliers to focus on providing a first-rate buying experience for their customers while managing the operations and processes required to support a seamless omnichannel experience.

Commerce Bridge Overview

GCommerce offers a suite of SaaS based services under the product name Commerce Bridge. The GCommerce Commerce Bridge consists of the following services:

Internet Data Exchange
– Electronic Messaging Solution

Fulfillment Master
– Fulfillment

Virtual Inventory Cloud
–Supply Chain Visibility Solution

VIC Data Services
– Business Analytics

TrueSKU & PBEPro
– Product Data Content

The Commerce Bridge is a collection of services that fill a part of the procurement life cycle in distribution supply chain markets. These services run on one of three network platforms, Microsoft Azure Cloud Services (Azure or Microsoft Azure), Amazon Web Services (AWS), or on-premise in the LightEdge datacenter located in Altoona, IA. Some of these services are stand-alone services and some of them utilize a hybrid cloud model, whereby some of the functions of the service are fulfilled by the on-premise network and other functions by the cloud network, Azure or AWS.

Internet Data Exchange (IDE) is a SaaS based private cloud solution which connects retailers to manufacturer distributors/suppliers to facilitate the distribution supply chain procurement process through standards-based Electronic Data Interchange (EDI) methods. The private cloud is located in a co-located datacenter owned and managed by LightEdge. Compliance for data connectivity, power, cooling, and protection from natural disasters or illegal access is subject to LightEdge's compliance review referenced here: https://www.LightEdge.com/about/compliance/. The Company's IDE acts as a proxy translator allowing disparate business systems to communicate as if they were using the same communication protocols and document formats.

Virtual Inventory Cloud (VIC) is a SaaS based system operating on the Microsoft Azure Cloud using .NET, Azure Web and App Services. VIC was designed to provide inventory visibility and efficiency for drop ship special orders using Microsoft Azure. It has transformed the special-order cycle by 6,000% solving a $20 billion problem for auto parts retailers. This project was the first of its kind on Azure and covers these keys:

- High performing data processing across a hybrid cloud solution.
- High availability, high-security single sign-on model across a hybrid cloud solution.
- High throughput/performance between Windows Azure and SQL Azure DB.
- Highly scalable VIC database on SQL Azure DB.

VIC also includes the ability to act as an Internet Protocol Proxy for the automotive aftermarket. It provides access to an industry-created/approved Webservices Protocol called Internet Parts Ordering (IPO). VIC is the only solution that provides this feature to the automotive aftermarket.

VIC resides, and is managed in, Microsoft Azure, which is subject to Microsoft Azure Compliance referenced here: https://www.microsoft.com/en-us/trustcenter/compliance/soc.

TrueSKU & PBEPRO are data delivery-based services centered around Paint Body and Equipment (PBE) data, product data, and inventory data. These two solutions are data services solutions that allow customers to stay up to date on product-related changes to accurately describe and sell their products. TrueSKU's data is derived from inventory and product data delivered to GCommerce by manufacturers/suppliers throughout the day. This data is validated for part matching accuracy and completeness for publication, then delivered to customers. PBEPRO has a user interface that resides on a multi-tenant virtual machine on Microsoft Azure. Each customer's instance represents the user portal only, whereas the associated SQL server database is a single-tenant database segregating data per user. Customers manage their PBE product data through the portal and can export data into their on-premise system whenever necessary.

TrueSKU & PBEPro solutions reside, and are managed, on Microsoft Azure Cloud, which are subject to Microsoft Azure referenced here: https://www.microsoft.com/en-us/trustcenter/compliance/soc.

Fulfillment Master (or FM) is a SaaS based system operating using Linux virtual machines which resides, and is managed, on the Amazon Elastic Cloud and Amazon Relational Database Service (RDS). FM enables large scale eCommerce fulfillment and shipping management involving multiple business system integrations and extensive IT resources. It provides EDI and API connectivity with leading marketplaces and e-tailers – aka SELLERS – and offers built-in integrations with popular carriers and shipping methods that allow the Fulfillment Master Client – aka WAREHOUSE – to focus on managing the business while Fulfillment Master manages connectivity and shipping automation. This system resides, and is managed on, Amazon Web Services, which is subject to Amazon's compliance referenced here: https://aws.amazon.com/artifact/getting-started/.

Principle Service Commitments and System Requirements

The Company's policies and procedures are based on the service commitments it makes to user entities; the laws and regulations that govern its services; and the financial, operational, and compliance requirements that GCommerce has established for its services. GCommerce's security and privacy commitments are documented and communicated to user entities in Statements of Work (SOWs), Service Level Agreements (SLAs), and other contracts. These commitments include, but are not limited to:

- Security principles within the design of the above-named systems are designed to permit system users to access only the information they need, based on their role and permissions in the system, while restricting them from accessing information not needed for their role.
- GCommerce makes available both Secured/Encrypted and Secured/Unencrypted data transport methods to meet customer needs.
- GCommerce processes customer actions completely, accurately, and timely.

GCommerce has developed and implemented standard operational procedures that support the achievement of its services, security, and privacy commitments; relevant laws and regulations; and other system requirements. Such requirements are communicated in the GCommerce policies and procedures, system design documentation, and contracts with clients.

Components of the Commerce Bridge

The boundaries of the Commerce Bridge include the services outlined above and the five (5) components described below: infrastructure, software, people, procedures, and data.

Infrastructure

This includes the physical and hardware components of the Commerce Bridge, including the facilities, equipment, and networks utilized.

Physical and Environmental Protection

GCommerce resides in the physical office space located at 700 Locust Street, Suite 201, Des Moines, IA 50309; which houses equipment storage and a server room that manages physical operations while the majority of resources relative to the Commerce Bridge are hosted by subservice organizations. This office space has three available entrances which are managed by an RFID card management system. Each employee is given an individual access card which grants them permission to enter the parking garage as

well as the three entrances to the office space. Additional access to sensitive areas, including the server room and other Information Technology department resources, is granted per cardholder to specified spaces specific to the employee's job role.

GCommerce also contracts the use of datacenter services from LightEdge located at 1435 Northridge Cir, Altoona, IA 50009. Security access to the Company's area of servers, as well as access to the building, is controlled by LightEdge. Compliance for data connectivity, power, cooling, and protection from natural disasters or illegal access is subject to LightEdge's compliance review referenced here: https://www.LightEdge.com/about/compliance/.

Equipment and Network

The GCommerce Commerce Bridge platform consists of Cisco networking infrastructure and cloud components configured for implicit deny. The servers primarily run the Microsoft technology stack including Microsoft Windows Server OS and SQL Server, with Linux, Azure and AWS cloud components. That environment is isolated off-site and only approved IT staff have remote and physical access to it with their Cisco Secure Endpoint and Malwarebytes Cloud protected Company-issued machines. Servers are deployed with as few roles installed as possible, all Windows updates applied, Windows firewall activated, and Cisco Secure Endpoint and Malwarebytes Cloud installed for endpoint protection.

The Company's networks are segmented to keep the production environment and cloud infrastructure isolated from non-production users and assets. The production environment is segmented by location between an on-premise network, AWS cloud virtual network, and Azure virtual network, both of which are connected to the on-premise network via persistent VPNs. Firewalls are deployed at the perimeter with only necessary Access Control List (ACL) exceptions added to the implicit Deny All configuration. Exceptions for customer traffic are applied to ACLs configured to only allow traffic from verified customer IPs to access required internal web servers on only the necessary ports.

Logical Access Management

All users are required to use their unique usernames for all activities, and their passwords expire every 90 days. System admins have Domain Admin privileges, all other users have bare minimum credentials required to perform their work tasks. Users are added to Active Directory groups based on their roles. Changes to an employee's access require management approval and can only be made at the request of approving management. Remote sessions auto log-off after 2 hours of inactivity. Internal user access to the production environment is granted based on a specific need, and approval, from the CIO/CTO. All Active Directory and Local user accounts are reviewed for removal bi-annually. External vendors are assigned bare minimum permissions to do work as needed and are removed from the system as soon as the need is satisfied. Vendors that must access the network do so after appropriate vetting and they access the Company's network via restrictive permissions and VPN connectivity.

Terminating users (whether voluntary or involuntary) is a critical component of the user identity, provisioning, and access rights. GCommerce utilizes comprehensive measures for ensuring that all terminated users are appropriately removed from having access to any GCommerce information systems.

Customers have no direct access to the Company's production environment. Their access to the customer-facing products is controlled by an extensive proprietary rules-based engine that restricts access to only specified customer information/data and services. Client access is granted based on products purchased,

and access to GCommerce services is restricted by username, password and domain name. Some system services, like VIC, require an extension of permissions inside a customer account. To achieve this in VIC, the Company created a sub-account level of provisioning which can be managed by the specified customer administrator account only. Customer access is revoked when they discontinue service with GCommerce.

Information systems enforce approved authorizations, identity-based, role-based, and attribute-based requirements for logical access to the systems. Logical access security policies, infrastructure, and architectures have been implemented to support the following areas:

User Account Management

- Account Request and Authentication
  - Establishing accounts upon verification of valid access authorization, identification of intended system usage, and other attributes, as required by the business requirements.
  - Creating accounts and assign custom roles.
  - Identifying the account types (Customer, Integration, Sales, Admin) to assign appropriate roles.
- Role-Based Authorization
  - Authorizing permissions based on the account types.
  - Restricting authorized internal and external user access to system components.
  - The following list shows each pre-configured role and the permissions assigned to it. All permissions are assigned to the Administrators role. A subset of permissions is assigned to each of the other roles.

Role	Permission
Administrators	The System Administrators, CIO/CTO and Network Admins are granted all permissions by default.
Connection Status Owners	Setup Trading Partners, rules, and establish relationships between trading partners.
Sales	Can view and download transaction metrics.
Mappers	Create and upload document maps to Dev and Staging environments.
Customer	Can view document transactions via GCommerce. Can fill and submit forms.

- Administration and Maintenance
  - Notifications to Admins when accounts are no longer needed.
  - Administer access authorizations and privileges are in accordance with access and functional requirement.
  - Modifying or removing system access when the assignment, job responsibility, or business requirement for access changes or is no longer needed.
  - Deactivating and deleting accounts that are no longer required, and accounts of terminated or transferred users.
  - Ensuring that user accounts are automatically locked after 3 consecutive unsuccessful login attempts.
  - Terminating Remote Access based on account terminations and IT needs.

Identity & Password Security Management

- Multi-factor authentication (MFA) solution to comply with security mandates.
- Leveraging a mobile device or email to accept authentication requests (MFA).
- Passwords will expire every 90 days and the user will be prompted to reset them via a secured channel.
- User identity is verified before performing password resets.
- Passwords will not be displayed when entered.
- Password complexity requirements include uppercase letters, lowercase letters, and a minimum password length.
- Passwords are changed whenever there is any indication of possible system or password compromise.

Identity Access Logging/Monitoring

User activity and transactions are logged to identify unauthorized access and for debugging system errors. Every login attempt logs all the additional user information listed below:

- User ID and User Domain.
- Login failed or successful.
- User's browser version.
- The total activity times.
- Environment (e.g. environment variables, other settings, etc.) on application startup.
- All errors and warnings during the user activity.
- All metrics related to the Rest and SOAP APIs.

Information Flow Management

GCommerce uses both Secured/Encrypted and Secured/Unencrypted protocols. These protocols include FTP, SFTP, AS2, and HTTPS/TLS to exchange documents between customers and various systems.

All requests made against the Azure storage accounts take place over secured connections and are only made from the Company's internal systems.

- **Automated data encryption**—All data written into Azure Storage is encrypted by using Storage Service Encryption (SSE). This includes metadata.
- **Role-Based Access Control (RBAC)**—Roles with different permissions are assigned to resource groups storage accounts and individual containers.

Software

GCommerce leverages a variety of application and operating system software relevant to the systems, applications, and utilities applicable to the Commerce Bridge Platform.

Data Backup and Recovery

GCommerce uses VEEAM backup and recovery for data recovery and individual system recovery, utilizing backup to disk, then copy to tape, and backup to Azure for offsite storage. Full backups run weekly and incremental backups run nightly. Network Admins monitor the backup software and remediate any failures, as need. Additionally, the Company uses Azure Site Recovery to maintain a DR site for catastrophic failover.

System and Security Monitoring Tools

GCommerce uses Nagios to monitor, alert and report on all systems and services. Metrics monitored include availability, uptime, CPU/MEM/network/disk utilization and rate, extra SQL metrics, IIS metrics, and system logs for supported systems. Uptime Robot is also utilized to monitor the Company's external-facing services from offsite to ensure public access to the Company's services.

The Company utilizes a 3rd party hosted SIEM for log forwarding, monitoring and alerting. The Company's Cisco FirePower router utilizes the latest IPS and Threat Response tactics and works in concert with the Company's Cisco Secure Endpoint protection, all backed by Cisco Talos Threat Intelligence. GCommerce undergoes annual port scans and is alerted by the Company's SIEM provider of any unknown access to any of the Company's infrastructure. The Company uses SalesForce.com for the Company's CRM and ticket management system. Tickets are entered manually on an as-needed basis and are assigned to the appropriate technician for that product and closed when resolved. Communication with clients includes email and phone calls, as needed, on a per-incident basis.

The Commerce Bridge platform is secured using AV/AM as well as anti-ransomware (AR) software. For anti-virus endpoint protection, the Company uses Cisco Secure Endpoint, which is also integrated with the Company's Firepower Cisco Firewall appliance for a complete platform protected solution. For anti-malware, the Company uses Malwarebytes with AR. Both Cisco Secure Endpoint and Malwarebytes are managed through a common administrator portal where the Company reviews the products' status. The GCommerce support team is notified if malicious files are detected and, as part of incident response, will evaluate/research the form of malicious file and determine if it should remain quarantined or released. If quarantined, the incident response team will then determine the vector of receiving this file and take action to remediate any vulnerabilities found.

Application Development Tools

The Company's development/IT team uses a variety of tools to support the Commerce Bridge platform. These tools all have a specific purpose in allowing us to quickly produce high quality, secure solutions for the Company's customers.

Application Development Tools	Database Development Tools	Change Management/Release Management (CI and CD)
• Visual Studio Online • Visual Studio IDE • Visual Studio Code • Eclipse IDE • Sublime Text • IntelliJ • MacOS Terminal • PowerShell • Azure Simulation Tools • Fiddler Web Debugging Proxy • FileZilla • Notepad++	• Microsoft SQL Server • Microsoft Azure SQL • SQL Server Management Studio • PostgreSQL-SQL Manager • MySQL • SQL Server Reporting Services (SSRS) • SQL Server Integration Services (SSIS)	• Azure DevOps Repos (TFVC) • Azure DevOps Boards • Azure DevOps Pipelines • Azure ARM Templates • Azure ARM Resource Manager • Azure Monitor • Biztalk Deployment Tool (Inhouse)

Application Development Tools	Database Development Tools	Change Management/Release Management (CI and CD)
• Microsoft Visio • Microsoft Excel		

People

GCommerce Organizational Structure

The organizational structure of GCommerce provides the framework for achieving the Company's daily operational goals and entity-wide objectives. GCommerce is organized into 4 key functional departments, which are segregated according to job responsibilities:

- Human Resources – Supports the onboarding process for new hires, via the Bamboo HR software platform, and delivers new hire policy documents.
- Customer Operations – Manages support cases, customer contacts and participates in change requests.
- Information Technology – Manages new product development, creation, review and evaluation of policies and procedures, oversight of network operations and change management procedures.

Contracted Personnel

GCommerce utilizes a contracted personnel resources company, located in India, to supplement current staff with contracted personnel when unique skills are needed, or additional resources are necessary to meet deadlines and/or service commitments. This 3rd party is an offshore resource managed out of Seattle, WA with access to resources in India. GCommerce uses this 3rd party and its personnel to supplement development, quality assurance testing, and overnight/weekend support monitoring. The 3rd party resource access management is managed through GCommerce's Active Directory and is subject to strict vendor management review and oversight. Access is only granted to work areas associated with their specified job duties and promptly removed when no longer necessary.

Procedures

Application Development & Change Management

GCommerce follows a structured change management process for application development, which is documented within the GCommerce Project Life Cycle Process standards. This standard provides structure and consistency for a successful software project.

GCommerce follows an agile development process that offers an iterative approach to the design and development of the Company's software. This allows the company to embrace the constant changes that occur in allowing teams to break the lengthy requirements, build, and test phases down into smaller segments, ultimately delivering working software quickly and more frequently. The Project Life Cycle Process consists of the following phases and team/team member ownership:

- **Project Initiation/Project Prioritization** – The initiation phase aims to define, authorize and prioritize the project. The business analysts present the Project requests to the Project Round Table (PRT) committee. The PRT committee authorizes the project and identifies the primary requirements for the project.

- **Requirements** – Business Analysts will define the requirements for the iteration based on the product backlog, iteration backlog, customer and stakeholder feedback. Requirements are written as user stories from the user's perspective.
- **Development** – Application Developers will design and develop software based on defined requirements.
- **Testing** – An Application Tester will write test cases and Quality Assurance (QA) testing on defined requirements.
- **Training/Documentation development** – Business Analysts, in collaboration with the Customer Support team, will create documentation for internal and external training. Internal training will be completed by the Business Analyst and external user training will be completed by the Customer Support team.
- **Release for Production** – Once the system/application, feature or tool is successful in the test environment, GCommerce approves the release for production. The technical lead will move modules to the production servers where functionality is tested after all modules are updated.
- **Delivery** – The Implementation team/Specialist will integrate and deliver the working iteration into production. Once deployed to production, internal and external users are notified of the release features via email and training sessions are scheduled with customers, if necessary.
- **Feedback** – The Implementation team and Sales team will take customer and stakeholder feedback and work it into the next project requests review.

Throughout these phases within the Project Life Cycle Process, all personnel involved are collaborating to engage the business to actively participate, which will help requirements to evolve throughout the project to ensure the work being done is the right product.

Before the Project Life Cycle Process, all requests (changes, enhancements, new products) are submitted into DevOps as a "project request ticket" and must go through the rigorous decision process. All requests (changes, enhancements, new products) originate from one of the three sources below:

- Direct Customer requests
- Enhancement requests from internal resources to help them save time/effort
- Enhancement requests from internal resources that are raised to improve the existing system or to fulfill the "expected behavior" of the existing system

To review these requests, GCommerce has developed a PRT committee to ensure a project request aligns with the enterprise strategic priorities, to collaborate so that everyone is on the same page, minimize miscommunication, and reign in scope creep before it happens. The group is limited to the minimum while ensuring the attendees represent each department's perspective and priorities. The group will determine:

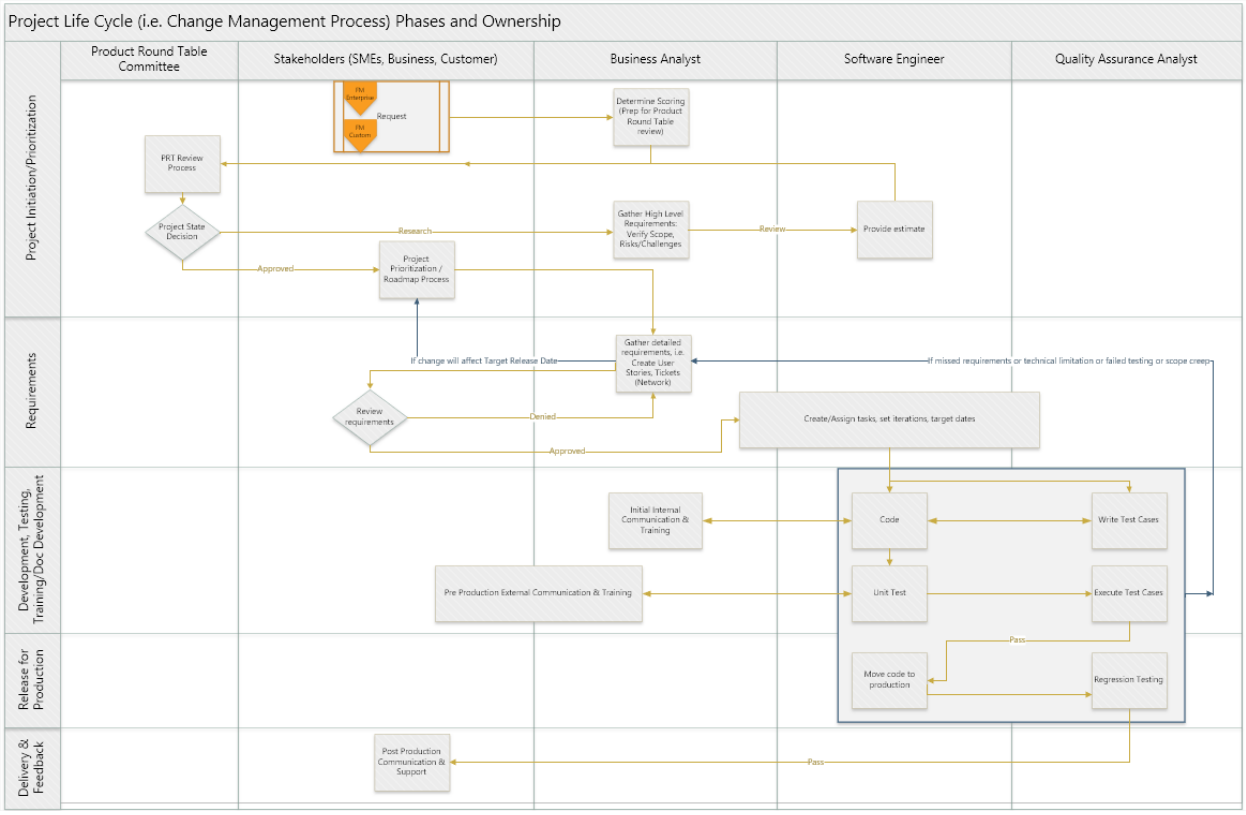
- Company strategic direction based on the Road Map and Capacity availability
- Risk/Impacts on the systems
- Required development effort
- Support and Customer Ops effort and historical context
- Implementation effort and customer representation
- Knowledge of sales efforts and plans

The PRT committee developed a Project Prioritization Model with a set of required questions to help determine the project request weight and priority. The Project Prioritization Model is based on the

weightage they hold in three categories: Alignment with Strategic Priorities, External Demand, and Projected Value. The PRT committee will then determine if the request will be:

- **Approved** – PRT approves requests and determined that request is necessary, which then begins the high-level requirements gathering phase.
- **Research** – More information is needed to understand requests.
    - Outcomes: the products, services, and/or results project will produce
    - Request Scope (characteristics/boundaries of requests)
    - Exclusions/Out of Scope
    - Risks/Impacts on the systems
    - Constraints/restrictions
    - Assumptions: Statements about requests
- **90 Day Review** – To put on hold and review again in 90 days.
- **Hold** – To be on hold until more customers request this change/enhancement.
- **Denied** – Determined that the request is not necessary.

The PRT process is the Company's change management process that has been implemented to identify, approve and track changes to the system. The following diagram summarizes the process, including all phases in the process and team ownership at each phase:



System changes are classified into the following three (3) categories:

1. Major Updates/New Product Requests – These updates are continuous maintenance and updates of the interface and middleware components developed within a project. Requests for change will be managed by the Product Round Table and a priority-driven approach, so that the risk to compromise the stability of the software deployed in a production environment is minimized. These prioritized requests are included in the project technical development plan. These are updates/requests that require more than 3 months of development time.
2. Maintenance and Minor Updates – These releases include interface or behavior changes that are backward-compatible with those of the corresponding major release. These are updates/requests that require less than 3 months of development.
3. Emergencies and Unplanned Outages – Emergency releases of components include changes fixing specific bugs found in production that require less than 24 hours of development and a notification to the customers if the production system must be down for more than 20 mins. Unplanned Outages are typically security-related defects found in production.

Software Maintenance

GCommerce has implemented a software maintenance standard for applying bug fixes and security updates to servers, workstations, and specified applications. Maintenance changes are categorized into the following four (4) classifications:

1. Major Updates – These updates are continuous maintenance and updates of the interface and middleware components developed within a project. Requests for change will be managed by the Product Round Table and will be taken as a priority-driven approach so that the risk to compromise the stability of the software deployed in a production environment is minimized. These prioritized requests are added to the project technical development plan.
2. Minor Updates – This release includes interface or behavior changes that are backward-compatible with those of the corresponding major release. Same as Major Updates, these requests follow the PRT and PLC processes following a priority-driven approach to mitigate risks.
3. Security Updates – These updates include software patches, new features and improvements to existing ones to keep the systems secure.
4. Bug Fixes –
    - If the product/system does not perform some action which is specified by the user story.
    - If the product/system does the action which should not be carried according to the user story.
    - If the product/system operates in the way which is not mentioned in the user story.
    - If the product/system does not execute the action which is not specified in the user story, but it should be.

Bug/Defect Fixes

All bugs/defects identified will be logged into DevOps and assigned to the QA Lead for review with the following information:

- Tagged with the highest environment in which the defect currently exists, if "Production" and/or "Staging".
- Area Path which indicates which system/product the bug is for OR, for the FM Bugs, add a tag for which Customer(s) it is for since we do not use Area Paths.
- Each Bug will be assigned the following **Severity Field**:

Option:	*Definition*
1 - Critical	The problem renders the system inoperable. This is serious enough to require immediate attention.
2 - High	The problem will cause significant impact to business functions, data integrity, business compliance, or calculations if the defect is not repaired. The issue could be a missing feature or a function that does not work as specified. Must be fixed before Sprint completes.
3 - Medium	The problem will impact production but there is a work-around or the impact is acceptable. The problem affects testing but testing may continue with additional effort or a reduced testing scope. These may be negotiated to a later release if the impact of the change is greater than the benefit. If not fixed in the current Sprint, must be approved by the Product Owner (PO) and moved to the Product Backlog to be prioritized.
4 - Low	The problem is cosmetic, has low impact on business functions, and has no impact on business compliance. These may be negotiated to a later release if the impact of the change is greater than the benefit. If not fixed in the current Sprint, must be approved by the PO and moved to the Product Backlog to be reprioritized.

- Each Bug will be assigned the following **Environment/Stage Tags**:

Option:	*Definition*
Production	If the highest-level environment in which the defect currently exists is production.
Staging	If the highest-level environment in which the defect currently exists is staging.
Testing	If the defect was identified while project is in testing stage.

- Each Bug will be assigned the following **Close Reason**:

Options	*Definitions*
As Designed	The defect is not a bug but how the system/application was purposely designed.
Cannot Reproduce	The defect cannot be reproduced in any environment and is no longer an issue.
Duplicate	The defect is the same issue as another defect.
Fixed and Verified	The defect was fixed, verified, and released to all environments affected.
Deferred	The defect was postponed due to low priority, low risk, and severity.
Will Not Fix	The defect was valid, but it was decided not to fix due to low priority, edge case, and/or business priority.

- If Fixed and Verified or As Designed, each Bug will be assigned the following **Root Cause**:

Options	*Definitions*
Deployment	The defect was caused by an incorrect or incomplete build deployment.
Development	The defect was caused by code or design differing from the documented acceptance criteria or an error in the database schema/design.
Configuration	The defect was caused by an incorrectly configured environment/setup.
Data	The defect was caused by incorrect data population or update in database.
External System	The defect was caused by a customer's system.
Other System	The defect was caused by another internal system.
Requirements	The defect was caused by an incomplete or incorrect User Story or Acceptance Criteria.
3rd Party Software	The defect was caused by third-party software.

- If As Designed, each bug will be assigned the following additional options for **Root Cause**:

Options	*Definitions*
User Error	The defect was identified as user error.
Enhancement/Change	The defect was identified as an enhancement/change to the system.

Once the QA lead has identified that logged bug/defect's severity, the development team will collaborate with the business to plan and schedule for the release.

Asset Management

Assets are inventoried and tracked by serial numbers in the Company's Nagios monitoring system as well as manually in our HR system for replacement and budget purposes. The lifecycle of all assets is reviewed annually during the Company's budgeting process. Subjectively, the CIO/CTO and Director of Network Operations review all assets and determine if they are nearing end-of-life and should be replaced or should be brought up for review in the following year.

Vendor Management

GCommerce does not make use of any third-party vendor to enhance the services offered under the Commerce Bridge that is not already covered under a separate SOC 2. Management obtains and reviews SOC 2® reports for all subservice organizations and ensures complimentary user entity controls are in place and operating effectively at GCommerce. All key vendors are subject to due diligence prior to contract execution to ensure proper security controls are in place. Annual reviews are conducted of all critical vendors to ensure the vendor continues to meet GCommerce's information security standards.

Incident Management

GCommerce has established an Incident Response Plan to escalate, respond to, and resolve identified security incidents and breaches to the Company. SIEM cases are utilized to track identified security incidents from identification through final resolution and reporting.

The IT Department uses a variety of security utilities to alert the Company to potential incidents and attempted access to systems and/or customer database files in real-time. These utilities include, but are not limited to, firewall notifications, SIEM alerts, IPS alerts, vulnerability scan reports, penetration test results, and operating system event logs. In addition, employees can report potential security incidents directly to the IT Department and clients can report them by contacting their account manager or the Support Department. Once notified, the IT Department works to analyze and isolate the threat, conduct a root cause analysis, remediate the issue, and establish future prevention techniques. For due diligence, the IT Department uses the Eight Disciplines (8D) process to approach and to resolve problems. The 8D problem-solving process ensures the right actions are taken to identify, correct, and eliminate recurring problems promoting continuous process improvements.

There have been no security incidents reported by, or to, GCommerce during the scope period of this report that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements that had been reported by, or to, GCommerce during the year.

Business Continuity Management

GCommerce has a Business Continuity and Disaster Recovery (BC/DR) Plan to guide the business in the case of a disaster or disruption to ensure the rapid resumption of critical services in a timely manner. GCommerce's BC/DR Plan leverage a risk-based analysis (from the Risk Assessment) that also includes specific policies, procedures, and supporting initiatives relating to all information systems.

GCommerce's Assessment Objectives are:

- Recovery Time Objective - the duration of time and a service level within which a business process must be restored after a disaster or disruption in order to avoid unacceptable consequences associated with a break in business continuity.
- Recovery Point Objective - the maximum tolerable period during which data might be lost.

The BC/DR framework follows the standard management method Plan, Do, Check, Act (PDCA) will be applied to the design and implementation of the business continuity program.

Plan (establish)

- Documented business continuity policy, objectives, targets, controls, processes, and procedures, relevant to improving business continuity in order to deliver results that align with the corporate strategy.

Do (implement and operate)

- Implementation of the policy, controls, processes and procedures through:
    - Documented business impact analysis and operational risk assessment.
    - Identification of appropriate business continuity strategies.
    - Establishing an incident response structures and processes.

- Documenting business continuity plans for key products and services and areas key to the delivery of the corporate strategy.
- Implementation of exercises to validate the effectiveness of plans.

Check (monitor and review)

- Program performance evaluation through methods of monitoring, measurement, analysis, and evaluation of processes, including audits of plans and management reviews.

Act (maintain and improve)

- Implementation and follow-up of lessons learned, as identified from incidents and exercises.
- Continual improvement through the identification of nonconformity and corrective action plans.

Data

Information used, and supported, by the Commerce Bridge system/application includes:

EDI Code	EDI Transactions
810	Invoice
846	Inventory Inquiry
850	Purchase Order
855	Purchase Order Acknowledgement
856	Advance Ship Notice
9GC	GCommerce Patented Acknowledgement
921	Product Data
997	Acknowledgment

Other data used by the Commerce Bridge include customer connectivity certificates, endpoint URLs, and data configuration/connectivity rules.

Data Classification

All data except for Company financial, corporate and technical documentation is classified equally as moderate to low security. This means all internal staff can view and work with customer data but cannot share this data outside the Company's organization or approved authorized contractors without customer consent. Financial, corporate, and technical data access is managed by group policies within the Commerce Bridge Network.

Data Transfers and Encryption

Customer data is encrypted in transit and sent to GCommerce via multiple transmission protocols including SFTP, FTPS, AS2, Web Services, and direct Web Page uploads. The Company also allows standard FTP based on customer needs. All transmission services include encryption options. Data collected during the Sales and onboarding processes are gathered directly over the phone or via email. All sensitive client data is stored in the Company's internal SQL database in an encrypted format following the industry standard AES-256 encryption algorithm. AS2 is encrypted using SHA256 encryption and signing, FTP is encrypted using at 1024+ TLS protocol as needed. All web services are encrypted in-flight via SSL between endpoints.

Data Files and Databases

The Company uses the structured file system on production to persist in client data files. The Company's production database access is limited to the following roles:

- CIO/CTO, Chief Information Officer/Chief Technology Officer
- Director of Network Administrator

The Company's Commerce Bridge applications have different databases running on multiple platforms including Azure cloud, AWS S3 Cloud and LightEdge. Database Server Access Control Management listed below:

- Production database access requires remote login into the Company's production web servers (VM) and then RDP into the actual database server.
- Every step in the process is authenticated at the finite level to ensure no other individuals have access to the production environment.
- The credentials used for production database access are entirely different than the staging and the development environments.
- Development tools are not allowed in the production environment.
- All the database operations, such as backups/restores, are restricted to a specific environment.
- Data flow to staging and development environments is meticulously restricted from production.
- No tunnels are set-up for data transfer to the lower environments.
- The database backups can be restored to the lower environments from the backup tapes from the data center that has restricted access.

The different platforms that the databases reside on are:

- Microsoft Azure Cloud
    - Database engines: Azure SQL Server
- Amazon Relational Database Service (RDS)
    - Database engines: MySQL, PostgreSQL
- On-Premise Data Center
    - Database engines: SQL Server

Web Portals

GCommerce has the following Web Portals in place:

Message Center

- Portal to view exchanged business documents and view transactions.
- Monitor the transactions happening through GCommerce.
- Setup trading partner information and business rules.
- Visual error tracking screens to track any failures reported while processing files.

Web Gateway

- Web Gateway allows retailers and distributors to be EDI capable with no investment in system integration and a minimal monthly cost based on message volume.
- Web Gateway portal allows users to:
    - View the Purchase Orders they received from their customers in a readable format populated on web forms.
    - Acknowledge the receipt of the orders.

- View and fill the blank or pre-populated Advance Shipping Notices (ASN) and invoices and post them on the portal to be received by the buyers.
- Print UCC-128 Labels.
- Print the PO, ASN and invoice documents.
- Change language option.

Virtual Inventory Cloud (VIC)

- VIC allows distributors and retailers to locate and order non-stocked items without reaching for the phone or browsing the supplier's web site.
- VIC portal allows users to:
  - Search for parts availability.
  - View pricing.
  - Estimated shipping costs.
  - Estimated ship dates and special.
  - Real-time visibility to the inventory of all their dropship suppliers.
  - Manage freight rules.
  - Manage authorizations to sub-accounts.
  - Manage holidays.

Cloud Match3

- Match3 system is a 3-way match process that receives the electronic documents sent by the EDI suppliers and performs the reconciliation automatically based on the buyer's rules and tolerances.
- Match3 portal allows the user to:
  - View all the procurement documents – purchase orders, ship notices, and invoices.
  - Review the exceptions on reconciled transactions based on purchase orders, packing slips and invoices.
  - Set up rules and tolerances.
  - Set up Fill rate rules.
  - Export approved invoices by vendor or date range for upload to the user's payable system.

Fulfillment Master (FM)

- Fulfillment Master provides EDI and API connectivity with the marketplaces and retailers. It has built-in integrations with popular carriers and shipping methods that help with connectivity and shipping automation.
- Fulfillment master portal allows users to:
  - Check stock, place orders and get shipment information via APIs.
  - View purchase orders received and track invoices and shipments.
  - Determine the most efficient box size based on weights and dimensions.
  - Setup e-commerce customers.
- Manage authorization to different roles.

PBEPRO

- PBEPRO provides rich product content to PBE distributors and body shops in multiple formats to the collision repair industry.
- PBEPRO portal allows users to view product content from all participating brands.

Subservice Organizations

GCommerce uses the following third-party service organizations to provide services related to the trust services criteria of this report, and the activities performed by this/these external subservice organizations are required to meet the various trust services criteria. This report includes only those controls at GCommerce and does not include the controls of the subservice organization set forth in the table below.

User entities should evaluate and perform the necessary procedures related to the activities performed by the following external subservice organization accordingly.

Subservice Organization Name	Services Provided
LightEdge	Rack Space Hosting, Power Management, Internet Access Management, Secured Server Hosting, Natural Disaster Protection.
AWS	Cloud Tools, VM Hosting, Database Services.
Microsoft Azure	Cloud Tools, DevOps Tools, Source Code Repo, VM Hosting, Compute Services, DR Services, Backup Retention, Database Services.
Pratum	vCISO, SIEM, and Penetration Testing Services

The following complementary subservice organization controls are expected to be implemented at the subservice organizations; however, they should not be regarded as a comprehensive list of all the controls that should be employed by the subservice organizations.

Applicable Trust Services Criteria	Complementary Subservice Organization Controls
CC6.1 and CC6.2 (Logical Security)	Pratum, LightEdge, Microsoft Azure and AWS are responsible for restricting logical access to programs, data, and computer resources to authorized and appropriate users and those users are restricted from performing authorized and appropriate actions.
CC6.4 (Physical Security)	Pratum, LightEdge, Microsoft Azure and AWS are responsible for implementing physical security controls to restrict access to the data centers, backup media, and other system components to authorized personnel.
CC6.5 (Device Destruction)	LightEdge, Microsoft Azure and AWS are responsible for securely decommissioning and physically destroying physical production assets in its control.
CC7.2 (Systems Operations)	Microsoft Azure is responsible for offsite backup and replication.
CC8.1 (Change Management)	Pratum, LightEdge, Microsoft Azure and AWS responsible for implementing change management procedures that engage GCommerce when changes are expected to impact the GCommerce environment provided by Pratum, LightEdge, Microsoft Azure and AWS.

GCommerce also utilizes other, less significant, third-party service organizations to support its services. These organizations are generally referred to as vendors.

Trust Services Categories

GCommerce believes the Processing Integrity and Security categories are the most applicable trust services categories relevant to GCommerce's Commerce Bridge system and the Management Description. As defined by the AICPA, the trust services categories include security, availability, processing integrity, confidentiality, and privacy.

The scope of the examination included the data processing services and processes provided by the Commerce Bridge system and performed by GCommerce. The applicable trust services criteria and GCommerce's related control activities are included in Section 4 (Independent Service Auditors' Description of Procedures Conducted Regarding Controls and Results) of this report to eliminate redundancy from including them here. Although the criteria and controls are included in Section 4, they are, nonetheless, an integral part of GCommerce's description of the Commerce Bridge system.

Description of Internal Controls

Control Environment

The control environment at GCommerce begins at the highest level of the Company. It is the foundation for other components of internal control by providing discipline and structure. The Executive Leadership Team plays important roles in establishing the Company's "one thing", core values, and focus on integrity. GCommerce follows organizational strategies defined by the "Great Game of Business" (GGOB) concepts. These concepts help implement an open dialog around a strategic plan with long term and short-term goals that are reviewed by the Executive Leadership Team quarterly.

Executive Leadership Team Oversight

GCommerce's Executive Leadership Team is responsible for the vision and direction of the Company, along with directing and controlling operations for service delivery. The Executive Leadership Team meets daily to understand and monitor business risks, discuss operational issues, and take corrective action, where needed. This allows them to establish, communicate, and monitor control policies and procedures in accordance with business objectives and to meet service commitments.

Policies, Procedures, and Standards

Management is committed to implementing administrative, physical and technical control environments to ensure the confidentiality, integrity and availability of information systems and associated data. Management has developed policies and procedures that reflect the Company's overall approach to security and internal control and comply with the Company's overall business objectives. The policies and procedures are aimed at the minimization of risk through preventative measures, timely identification of security issues, limitation of losses, and timely restoration/correction. The policies also include the assignment/scope of responsibilities, reporting lines, and disciplinary actions associated with failing to comply with the policies and procedures. These documents are reviewed and updated annually to ensure they align with current processes and procedures and reflect current industry best standards. Listed below are policy documents and groupings of policies within the documents relating to security:

- GCommerce Handbook and Acceptable Use Policy
    - Use of Communication and Computer Systems
    - Email Policy
    - Social Media Policy
    - Personal and Company-Provided Portable
    - Remote User Access Policy
    - Password Policy
    - Cyber Security Awareness, Training, and Education
    - BYOD Policy
    - Internet Usage Policy
    - Incident Response to Organizational Assets
    - Physical and Environmental Securities Policies
    - Software Usage Policy

- Information Security Policy (ISP)
    - Access Management
    - Asset Management
    - Business Continuity and Disaster Recovery
    - Change Management
    - Configuration Management
    - Data Governance
    - Managing Third Parties
    - Monitoring
    - Computer Provisioning and Baseline Hardening
    - Network Security Policy
    - Securing and Updating Systems
    - System Development
    - Vulnerability Management
    - Wireless Environment
- Information Security Risk Management Policy

Personnel Administration

The competence of employees is a key element of the control environment and is expressed in the Company's personnel policies. GCommerce's commitment to competence begins with recruiting, which is the joint responsibility of Human Resources /Finance and the business unit managers. Hiring decisions are based on various factors, including educational background, prior relevant experience, past accomplishments, and company culture fit to fulfill job descriptions. Human Resources /Finance performs applicable background screenings and completes the employee onboarding process, which includes initial orientation and training. Employees are provided information and training on information security and privacy, security policy, code of conduct, and other topics during their first days on the job.

Performance monitoring is provided to all employees through the use of annual performance evaluations and interactions with the employee on a daily basis. Employees are evaluated based on the job role and expectations defined by their manager. GCommerce's culture is to manage results so performance evaluations are discussed in terms of individual and company goals that are discussed and evaluated with each employee once a quarter.

Risk Assessment

GCommerce utilizes an information technology risk management program designed to identify, assess, and manage risks that could affect its ability to achieve its operational, financial, and compliance objectives. The Company assesses and manages risk that could affect its ability to provide reliable services to its clients on an ongoing basis.

Risk Identification and Assessment

The risk management process begins with the identification and assessment of risks to the Company, which includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and determining appropriate actions to address them. A risk matrix is used to track the risks faced by the Company and the controls implemented to mitigate these risks to acceptable levels. Significant risks that require actionable steps are added to a risk register and are tracked by management through project resolution. Management reviews risks on an annual basis to ensure the Company is appropriately addressing risk.

In addition to the formal risk assessment process, managers discuss and resolve issues as they arise within their areas and monitor and adjust the control processes for which they are responsible for on an as-

needed basis. This process is performed both informally and formally through regularly scheduled meetings with teams and individuals.

Information and Communication

GCommerce establishes and maintains a secure and monitored information system and network environment designed to ensure the integrity, confidentiality, and availability of information generated from the various systems and applications. Pertinent information is identified, captured, and communicated in a form and time frame that enables employees to carry out their assigned responsibilities. A high-level description of the information system is provided in the "Commerce Bridge Overview" section above.

To help align GCommerce's business strategies and goals with operating performance, management is committed to maintaining effective communication with personnel. All users are made aware of security and company policy expectations and are trained on how to fulfill these expectations. Management provides orientation and training to all employees and distributes relevant information, including system changes, to all users via email and system notifications. Organizational values and behavioral work standards are communicated to personnel via the Company's Employee Handbook and a Standards of Business Conduct is signed by all employees upon hire.

Clients are provided with pertinent information to enable them to understand the boundaries of the Commerce Bridge system. This is primarily accomplished through the use of service agreements, training, user manuals, notification and general emails, and telephone.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified, as appropriate, for changes in conditions. Management and key personnel are responsible for monitoring the quality of the internal control environment as a regular part of their activities. GCommerce utilizes the services and tools from an independent 3rd party (Pratum) to perform vulnerability scanning and penetration testing to test the effectiveness and efficiency of the control environment for the Commerce Bridge system. Independent security assessments and audits are performed on a recurring basis to ensure controls are updated and modified, as necessary. These processes are performed under the guidance and approval of GCommerce senior management.

Firewall configurations are reviewed by management frequently to ensure all established rules have business justification and unnecessary rules are removed timely. Replacement rules are created, tested and implemented, as appropriate.

GCommerce also utilizes a managed security services provider (MSSP) to provide SIEM services. Alerts are generated and reviewed at the MSSP for suspicious critical activity and security tickets are opened and an IT team member is notified of the potential issue. The IT team member will then investigate and, if necessary, remediate the issue and provide resolution details to the MSSP so the security ticket can be updated and closed for tracking and reporting purposes. A monthly meeting is held with the MSSP to review reports, ticket status, and current configurations. These processes are performed under the guidance and approval of GCommerce senior management.

Processing Integrity

Processing integrity encompasses the completeness, validity, accuracy, timeliness, and authorization of system processing and addresses whether the Commerce Bridge achieves the purpose for which it exists and whether it performs its intended function, to process customer transactions in an unimpaired manner, free from unauthorized or inadvertent manipulation. The processing integrity criteria addresses input, processing, output, and storage of data within the system.

GCommerce has identified critical business processes and components required to ensure the Commerce Bridge maintains the processing integrity of customer data. GCommerce's critical business processes and components used to maintain processing integrity are Application Development/Change Management processes as described in the Procedures section, Implementation Onboarding processes, and EDI Super Specs to help simplify data mapping which includes complete data definitions and descriptions for the trading partners.

Changes in Controls

There have been no material changes to the security controls within GCommerce's Commerce Bridge system during the period under examination that would affect user entities' understanding of the Commerce Bridge system and the services provided. However, AutosoEZ was removed from the scope of the SOC2 exam. It was removed because GCommerce has discontinued and no longer provide AutosoEZ as a product.

In addition, additional internal controls, which were not new to GCommerce, were added to the scope of the exam to continually improve transparency to GCommerce's clients and strengthen the Company's security posture.

Complementary User Entity Controls

The processes and services provided by GCommerce were designed with the assumption that certain controls would be implemented by user entities to meet their specific operational needs. In particular situations, the application of specified internal controls at user entities contributes significantly to the overall achievement of various trust services criteria included in this report.

User entities should consider whether the following key controls and responsibilities have been placed in operation at the user entities:

- User entity must maintain up to date authentication certificates for encryption and notify GCommerce of any changes.
- The user entity should notify GCommerce of maintenance downtime scheduled on their systems.
- The user entity should notify GCommerce of known errors in their files or disruption in transmitting their files to GCommerce for processing.
- The user entity shall assign a unique username and password to each user and passwords should be changed based on their internal security policy.
- User entity management shall ensure access is terminated for users who are no longer authorized and shall notify GCommerce of all new, and changes to existing, user accounts.

This list of complementary user entity controls and responsibilities presented above does not represent a comprehensive set of all controls that should be employed by user entities. Other controls may be required at user organizations.

Section 4:

Independent Service Auditors' Description of Procedures Conducted Regarding Controls and Results

Independent Service Auditors' Description of Procedures Conducted Regarding Controls and Results

Introduction

This System and Organization Controls (SOC 2®) Report is intended to provide interested parties with information sufficient to understand the basic structure of internal controls within GCommerce's (the Company) Commerce Bridge (the System) to meet the criteria of the security and process integrity trust services categories. This report, when combined with an understanding of controls in place at user entity organizations, is intended to permit an evaluation of the internal control environment surrounding the Company's System.

Our examination was restricted to the services provided by GCommerce, the boundaries of that System, the security and processing integrity trust services categories, as defined in Section 3 of this report, and Management's Description of GCommerce's Commerce Bridge (the Description) for the period from October 17, 2020 through October 16, 2021 and, accordingly, did not extend to controls (e.g. policies and procedures) in effect at user entities using the Company's services. It is each interested parties responsibility to evaluate this information in relation to internal controls in place at their entities to obtain an understanding and assess the total internal control environment. The key complementary user entity controls, listed in Section 3 of this report, and GCommerce's controls must be evaluated together. If effective user entity controls are not in place, GCommerce's controls may not compensate for such weaknesses. Since the Company utilized the 'carve-out' method to present its subservice organizations, LightEdge, Microsoft Azure, AWS and Pratum, our examination procedures did not extend to these subservice organizations.

Description of the Testing Procedures Performed

On the pages that follow, the controls to meet the applicable trust services criteria have been specified by, and are the responsibility of, GCommerce. The procedures performed and results are the responsibility of LWBJ, LLP (LWBJ).

Our tests of the design and the operating effectiveness of the controls detailed in the Description, including controls over the control environment, risk assessment, information and communication, and monitoring of controls, included a combination of:

- Inquiry of controls with the appropriate management and/or supervisory personnel who are responsible for developing, implementing, operating and maintaining the controls;
- Observation of specific processes and/or service activities being performed by personnel, as determined appropriate by LWBJ;
- Inspection of GCommerce's documents and records including, but not limited to, review of policies and procedures and examination of evidentiary matter; and
- Evaluation of the overall presentation of the Description, including an independent assessment of the risk that the Description, and the control activities stated therein, is not fairly presented.

We performed audit sampling in accordance with the AICPA authoritative literature in such a way that samples were expected to be representative of the entire population. This required the use of professional judgment to consider tolerable deviation rate, audit risk, the characteristics of the population, and other factors.

Testing the completeness and accuracy of information provided by GCommerce is not specified in the testing procedures listed in this section; however, it was performed as part of our procedures to support the sufficiency and reliability of the information used by us. This includes the observation and inspection of system-generated reports, custom-developed queries, system screen prints, and relevant listings utilized in our testing of the specified control activities.

The extent and timing of the procedures performed, sample size calculations, and the results of the tests were designed to provide reasonable, but not absolute, assurance of the design and operating effectiveness of the internal controls designed to achieve the specified control activities for the period from October 17, 2020 through October 16, 2021. The results of each test applied are listed in the following testing matrix. As inquiries were performed for substantially all of GCommerce's controls, the tests were not listed individually for every control in the matrix.

Security Category and Criteria Table

Common Criteria Related to Control Environment

CC1.1: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC1.1.1	GCommerce's Employee Handbook, Information Security Policy (ISP), and Acceptable Use Policy outline standards of conduct and the commitment to integrity and ethical values within the Company.	Inspected the Employee Handbook, ISP, and Acceptable Use Policy to ascertain the expectations for business conduct and importance of integrity and ethical values.	No exceptions noted.
CC1.1.2	GCommerce's Employee Handbook, ISP, and Acceptable Use Policy are reviewed and approved on an annual basis by senior management.	Reviewed the Employee Handbook, ISP, and Acceptable Use Policy to ascertain the documents were reviewed and approved by senior management during the year.	No exceptions noted.
CC1.1.3	The reviewed and approved GCommerce Employee Handbook, ISP and Acceptable Use Policy are published and communicated to all employees.	Observed the Employee Handbook ISP, and Acceptable Use Policy were published to the Company intranet providing access to all employees.	No exceptions noted.
CC1.1.4	All employees and contractors are required to sign acknowledgement of GCommerce's Employee or Consultant Handbook, ISP, Acceptable Use Policy and any policies or procedures outlining standards of conduct upon hire and annually thereafter.	Inspected the ISP to ascertain the requirements for annual review of the security policies for all personnel. Obtained a list of new employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, ISP, and Acceptable Use Policy for a sample of new employees.	No exceptions noted.

Common Criteria Related to Control Environment (continued)

CC1.1: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC1.1.4	(continued)	Obtained a list of all employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, ISP, and Acceptable Use Policy for a sample of employees.	(continued)
CC1.1.5	The Employee and Consultant Handbooks, ISP and Acceptable Use Policies detail the Company's commitment to security.	Inspected the Employee Handbook, Consultant Handbook and ISP to ascertain they document the Company's commitment to security and include the system's security requirements, procedures to accomplish those security requirements, and individuals assigned with responsibilities of those procedures.	No exceptions noted.
CC1.1.6	GCommerce policies, standards procedures are developed and implemented to address risk factors.	Inspected the ISP, Employee Handbook and related security policies to ascertain the development and implementation standards to address risk factors.	No exceptions noted.
CC1.1.7	GCommerce policies and standard procedures are developed and implemented for controls over technology.	Inspected the ISP, Employee Handbook and related security policies to ascertain the development and implementation standards for controls over technology.	No exceptions noted.

Common Criteria Related to Control Environment (continued)

CC1.1: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC1.1.8	GCommerce utilizes a ticketing process for control activities.	Inquired with management and reviewed security policies to ascertain that key control activities are subject to a ticketing process. Obtained a list of application and infrastructure changes and inspected the change management ticket for a sample of changes to verify each change was accompanied by a detailed ticket. Inspected the project, and ticket details, created to remediate a sample of penetration test findings. Inspected the support ticket for example significant system issues, along with the 8D analysis, to verify a ticket was created to track significant issues through resolution.	No exceptions noted.
CC1.1.9	GCommerce has access management policies and procedures in place.	Inspected the ISP and Remote Work Policy to ascertain the inclusion of access management policies and procedures.	No exceptions noted.
CC1.1.10	Internal user account creation, modification, and deletion must be requested via access provisioning tool.	Obtained a listing of new employees and contractors and inspected system evidence of management's approval of access for a sample of new individuals. Obtained a listing of terminated employees and contractors and inspected the termination email, along with system evidence, for a sample of individuals, to verify access was removed.	No exceptions noted.

Common Criteria Related to Control Environment (continued)

CC1.2: COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC1.2.1	The roles and responsibilities of the Board of Directors (the Board) are outlined in the Board of Directors section of the Stockholders Agreement and are segregated from the roles and responsibilities of management.	Inspected the Board of Directors section of the Stockholders Agreement to verify the roles and responsibilities of the Board are outlined and are required to be segregated from the roles and responsibilities of management.	No exceptions noted.
CC1.2.2	The Board is composed of members from varying backgrounds and industries to allow for objective evaluation and decision making.	Inspected the member biographies of the Board to verify members had diverse backgrounds and came from diverse industries.	No exceptions noted.
CC1.2.3	The Board includes members who are independent from the executive leadership team to maintain independence from management.	Inspected the Stockholders Agreement to ascertain at least one (1) Board member must be independent from management. Inspected the composition of the Board and the members biographies to verify there were members who were independent from management.	No exceptions noted.
CC1.2.4	GCommerce includes information security and processing efforts as part of its annual budget to include necessary resources and assign specialized expertise.	Inspected the financial packet for a sample of months to verify they included budgeted development expenses, including payroll and operational (processing) costs.	No exceptions noted.

Common Criteria Related to Control Environment (continued)

CC1.2: COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC1.2.5	GCommerce established a process that allows open communication channels to allow input from stakeholders.	Inspected the Company's website to ascertain a support email and phone number were included in the contact information for GCommerce. Obtained a list of all new customers and inspected the signed service agreement, which included customer support information. Observed system evidence that a Fulfillment Master customer was assigned a GCommerce employee as a contact for open communication and evidence of communication between the customer and GCommerce following the implementation of services.	No exceptions noted.
CC1.2.6	Internal user account creation, modification, and deletion must be requested via access provisioning tool.	Obtained a listing of new employees and contractors and inspected system evidence of management's approval of access for a sample of new individuals. Obtained a listing of terminated employees and contractors and inspected the termination email, along with system evidence, for a sample of individuals, to verify access was removed.	No exceptions noted.

Common Criteria Related to Control Environment (continued)

CC1.3: COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC1.3.1	Management has established an organizational chart to define its organizational structures, reporting lines, and areas of authority.	Inspected the organizational chart and discussed it with management, noting appropriate reporting lines have been established.	No exceptions noted.
CC1.3.2	GCommerce outlines the responsibility and accountability of the CIO/CTO and senior management in regards to control design, implementation and monitoring.	Inspected the ISP to verify the responsibility and accountability of the CIO/CTO and senior management regarding control design, implementation and monitoring are defined.	No exceptions noted.
CC1.3.3	Roles and responsibilities are defined in written job descriptions and communicated to employees.	Obtained a listing of employees and inspected the job description for a sample of employees, made available to the employee for their review through the Company intranet, to verify the roles and responsibilities were documented for the position.	No exceptions noted.
CC1.3.4	GCommerce utilizes a management tool to communicate and centrally manage information security policies and requirements.	Inspected the information security policies and procedures were centralized in the Company's HR application for easy access by employees.	No exceptions noted.
CC1.3.5	GCommerce includes information security and processing efforts as part of its annual budget to include necessary resources and assign specialized expertise.	Inspected the financial packet for a sample of months to verify they included budgeted development expenses, including payroll and operational (processing) costs.	No exceptions noted.

Common Criteria Related to Control Environment (continued)

CC1.3: COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC1.3.6	GCommerce's Employee Handbook, ISP, and Acceptable Use Policy are reviewed and approved on an annual basis by senior management.	Reviewed the Employee Handbook, ISP, and Acceptable Use Policy to ascertain the documents were reviewed and approved by senior management during the year.	No exceptions noted.

Common Criteria Related to Control Environment (continued)

CC1.4: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC1.4.1	GCommerce evaluates candidates to fill a position.	Inspected the ISP to ascertain the requirements for detailed interviews to be conducted as a prerequisite to being hired. Obtained a list of new employees and verified a sample of new employees were hired through a recruiting agency, who is responsible for completing an interview process and review of the candidates' qualifications prior to hire.	No exceptions noted.
CC1.4.2	GCommerce provides training to personnel on the correct use and operation of the implemented security functions, controls and/or mechanism, as needed.	Inspected the ISP to verify information security training requirements are detailed for new and existing employees. Obtained a list of new employees and contractors and verified a sample of individuals completed the required onboarding security training. Obtained a list of all employees and contractors and verified a sample of individuals completed the required annual security training during the period under scope.	No exceptions noted.

Common Criteria Related to Control Environment (continued)

CC1.4: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC1.4.3	Management defines monitoring of individuals such as probationary periods for new employee.	Inspected the Employee Handbook to ascertain the requirements for employee performance evaluations. Obtained a list of new employees and inspected system evidence of the completed probationary period for a sample of new employees.	No exceptions noted.
CC1.4.4	Management establishes development and improvement programs for employees.	Inspected the Employee Handbook to ascertain the development and improvement programs established for employees. Obtained a list of all employees and observed system evidence the employee's supervisor evaluated, tracked and updated goals and established a development and improvement program for a sample of employees.	No exceptions noted.
CC1.4.5	GCommerce's Employee Handbook, Information Security Policy (ISP), and Acceptable Use Policy outline standards of conduct and the commitment to integrity and ethical values within the Company.	Inspected the Employee Handbook, ISP, and Acceptable Use Policy to ascertain the expectations for business conduct and importance of integrity and ethical values.	No exceptions noted.

Common Criteria Related to Control Environment (continued)

CC1.4: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC1.4.6	Management establishes the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the Company and implement corrective action, as necessary.	Inspected the Employee Handbook to ascertain procedures in place to communicate and hold individuals accountable for performance of internal control responsibilities across the Company and implement corrective action as necessary. Obtained a list of all employees and observed system evidence the employee and his/her supervisor evaluated, tracked and updated goals for a sample of employees.	No exceptions noted.
CC1.4.7	Management establishes performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the Company, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and long-term objectives.	Inspected the Employee Handbook to ascertain established procedures for performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the Company. Obtained a list of all employees and observed system evidence the employee and his/her supervisor evaluated, tracked and updated goals, which included short-term and long-term objectives and established incentives and other rewards for high performance, for a sample of employees.	No exceptions noted.

Common Criteria Related to Control Environment (continued)

CC1.4: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC1.4.8	GCommerce requires a review of the Employee or Consultant Handbook and Acceptable Use Policy on an annual basis, with acknowledgement from all personnel indicating that they have read, understood, and agree to abide by the rules of behavior.	Obtained a list of all employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, which included acceptable use policies, for a sample of individuals.	No exceptions noted.
CC1.4.9	In addition to requiring a review of the Employee or Consultant Handbook and Acceptable Use Policy, GCommerce requires employees and contractors to sign agreements that include provisions and asset protection responsibilities upon hire.	Obtained a list of new employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, which included asset protection responsibilities, for a sample of new individuals.	No exceptions noted.

Common Criteria Related to Control Environment (continued)

CC1.5: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC1.5.1	Management establishes the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the Company and implement corrective action, as necessary.	Inspected the Employee Handbook to ascertain procedures in place to communicate and hold individuals accountable for performance of internal control responsibilities across the Company and implement corrective action as necessary. Obtained a list of all employees and observed system evidence the employee and his/her supervisor evaluated, tracked and updated goals for a sample of employees.	No exceptions noted.
CC1.5.2	Management establishes performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the Company, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and long-term objectives.	Inspected the Employee Handbook to ascertain established procedures for performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the Company. Obtained a list of all employees and observed system evidence the employee and his/her supervisor evaluated, tracked and updated goals, which included short-term and long-term objectives and established incentives and other rewards for high performance, for a sample of employees.	No exceptions noted.

Common Criteria Related to Control Environment (continued)

CC1.5: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC1.5.3	Management aligns incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.	Reviewed the ISP and Employee Handbook to ascertain the alignment of incentives and rewards with internal control responsibilities. Obtained a list of all employees and observed system evidence the employee and his/her supervisor evaluated, tracked and updated set goals, which included the achievement of internal control responsibilities and established incentives and other rewards for high performance, for a sample of employees.	No exceptions noted.
CC1.5.4	Management evaluates and adjusts pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.	Reviewed the ISP and Employee Handbook to verify the requirement for management to evaluate and adjust pressures associated with the achievement of security objectives. Obtained a list of all employees and observed system evidence the employee and his/her supervisor evaluated, tracked and updated set goals, which included adjusting priorities and pressures, for a sample of employees.	No exceptions noted.

Common Criteria Related to Control Environment (continued)

CC1.5: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC1.5.5	Management evaluates the performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and provides rewards or exercises disciplinary action, as appropriate.	Reviewed the ISP and Employee Handbook to verify the requirement for management to evaluate performance of internal control responsibilities. Obtained a list of all employees and observed system evidence the employee and his/her supervisor evaluated, tracked and updated set goals, which include achievement of internal control responsibilities and established incentives and other rewards for high performance, for a sample of employees.	No exceptions noted.
CC1.5.6	GCommerce's Employee Handbook, ISP, and Acceptable Use Policy are reviewed and approved on an annual basis by senior management.	Reviewed the Employee Handbook, ISP, and Acceptable Use Policy to ascertain the documents were reviewed and approved by senior management during the year.	No exceptions noted.
CC1.5.7	All employees and contractors are required to sign acknowledgement of GCommerce's Employee or Consultant Handbook, ISP, Acceptable Use Policy and any policies or procedures outlining standards of conduct upon hire and annually thereafter.	Inspected the ISP to ascertain the requirements for annual review of the security policies for all personnel. Obtained a list of new employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, ISP, and Acceptable Use Policy for a sample of new employees.	No exceptions noted.

Common Criteria Related to Control Environment (continued)

CC1.5: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC1.5.7	(continued)	Obtained a list of all employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, ISP, and Acceptable Use Policy for a sample of employees.	(continued)
CC1.5.8	GCommerce outlines the responsibility and accountability of the CIO/CTO and senior management in regards to control design, implementation and monitoring.	Inspected the ISP to verify the responsibility and accountability of the CIO/CTO and senior management regarding control design, implementation and monitoring are defined.	No exceptions noted.
CC1.5.9	Management defines monitoring of individuals such as probationary periods for new employee.	Inspected the Employee Handbook to ascertain the requirements for employee performance evaluations. Obtained a list of new employees and inspected system evidence of the completed probationary period for a sample of new employees.	No exceptions noted.

Common Criteria Related to Communication and Information

CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC2.1.1	GCommerce has a system user manual in place that outlines the systems in scope for services provided, their boundaries, and instructions on the proper operation of the System.	Reviewed the system user manuals and verified each document appropriately outlined the systems in scope for services provided, their boundaries, and instructions on the proper operation of the system.	No exceptions noted.
CC2.1.2	GCommerce performs risk assessments on system processes that support the internal control and achievement of the Company's service commitments and system requirements.	Inspected the ISP to ascertain the procedures for an annual risk assessment and continual development of a risk register. Inspected the annual risk assessment executive report, noting it was comprehensive, identified and assessed risks within the System, and summarized risks to remediate.	No exceptions noted.
CC2.1.3	GCommerce uses real-time monitoring to identify if systems and processes are not running as expected.	Inspected example performance and system availability rules and alert configurations to verify alerts are generated when predefined criteria are exceeded and appropriate individuals receive the notifications for research and resolution. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely.	No exceptions noted.

Common Criteria Related to Communication and Information (continued)

CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC2.1.4	Changes to scheduled jobs require management approval and follow the change management procedures.	Inspected the Product Round Table (PRT) Process to ascertain the procedures required for processing changes to scheduled jobs which include management approval. Obtained a system log of all changes to scheduled jobs and inspected the change ticket details to verify the approval of management was obtained for a sample of changes to scheduled jobs.	No exceptions noted.
CC2.1.5	A system job runs three (3) times daily to search for any files not pulled off the FTP server and a report summarizing any such files is generated and sent to the IT department for research and resolution.	Obtained the 1st, 2nd or 3rd Non-Delivered Report generated for a sample of days and inspected evidence that a sample transaction error from each Non-Delivered Report had been resolved timely by the IT department.	No exceptions noted.
CC2.1.6	GCommerce has implemented various processes and procedures relevant to security to produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained.	Reviewed the ISP and related security compliance policies to ascertain the processes and procedures relevant to produce information that meets service commitments.	No exceptions noted.

Common Criteria Related to Communication and Information (continued)

CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC2.1.7	GCommerce subscribes to information security alerts and groups and uses them to update SIEM rules and monitor the impact of emerging technologies and security.	Inspected the Company's Cybrary membership, which is used to provide security training and best practices. Inspected the BlackHat Conference information and email calendar invitations for team members, which is used to stay current on emerging security threats, trends, and industry best practices.	No exceptions noted.
CC2.1.8	GCommerce's Employee Handbook, Information Security Policy (ISP), and Acceptable Use Policy outline standards of conduct and the commitment to integrity and ethical values within the Company.	Inspected the Employee Handbook, ISP, and Acceptable Use Policy to ascertain the expectations for business conduct and importance of integrity and ethical values.	No exceptions noted.
CC2.1.9	Management has established an organizational chart to define its organizational structures, reporting lines, and areas of authority.	Inspected the organizational chart and discussed it with management, noting appropriate reporting lines have been established.	No exceptions noted.
CC2.1.10	GCommerce outlines the responsibility and accountability of the CIO/CTO and senior management in regards to control design, implementation and monitoring.	Inspected the ISP to verify the responsibility and accountability of the CIO/CTO and senior management regarding control design, implementation and monitoring are defined.	No exceptions noted.

Common Criteria Related to Communication and Information (continued)

CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC2.1.11	GCommerce utilizes a management tool to communicate and centrally manage information security policies and requirements.	Inspected the information security policies and procedures were centralized in the Company's HR application for easy access by employees.	No exceptions noted.
CC2.1.12	GCommerce requires a review of the Employee or Consultant Handbook and Acceptable Use Policy on an annual basis, with acknowledgement from all personnel indicating that they have read, understood, and agree to abide by the rules of behavior.	Obtained a list of all employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, which included acceptable use policies, for a sample of individuals.	No exceptions noted.
CC2.1.13	In addition to requiring a review of the Employee or Consultant Handbook and Acceptable Use Policy, GCommerce requires employees and contractors to sign agreements that include provisions and asset protection responsibilities upon hire.	Obtained a list of new employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, which included asset protection responsibilities, for a sample of new individuals.	No exceptions noted.
CC2.1.14	Security compliance and security literacy training is required by all personnel on an annual basis.	Inspected the ISP to verify information security training requirements are detailed for new and existing employees. Obtained a list of new employees and contractors and verified a sample of new individuals completed the required onboarding security training.	No exceptions noted.

Common Criteria Related to Communication and Information (continued)

CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC2.1.14	(continued)	Obtained a list of all employees and contractors and verified a sample of individuals completed the required annual security training.	(continued)
CC2.1.15	GCommerce has periodic security literacy and awareness campaigns as security threats arise within the Company or have been identified from threat intelligence and/or compliance resources.	Reviewed documents shared with GCommerce personnel for various security awareness campaigns conducted throughout the scope period.	No exceptions noted.
CC2.1.16	GCommerce support utilizes the 8D problem solving process to establish a permanent corrective action based on analysis of the problem.	Inspected the support ticket and 8D analysis for example system issues to verify the 8D process was followed for significant issues.	No exceptions noted.
CC2.1.17	GCommerce's formal Information Security Risk Management and Assessment Policy defines criteria for risk mitigation and acceptance.	Inspected the IT Risk Management Program to ascertain the criteria for risk mitigation and acceptance. Inspected the annual risk assessment, noting it detailed risk objectives, was comprehensive, assessed risks on varying tolerance levels, incorporated mitigating controls, and was reviewed by management.	No exceptions noted.

Common Criteria Related to Communication and Information (continued)

CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC2.1.18	GCommerce assesses risks for control families and controls applicable to the Company against the National Institute of Standards and Technology (NIST) 800-53, an industry standard framework.	Inspected the IT Risk Management Program to ascertain it detailed the scope, risk management components and procedures in place to identify and assess risks. Inspected the annual risk assessment executive report, noting it was performed against a subset of controls from NIST 800-53.	No exceptions noted.
CC2.1.19	GCommerce performs a risk assessment annually based on objectives incorporated from service commitments and system requirements.	Inspected the IT Risk Management Program to ascertain the procedures for an annual risk assessment and continual development of a risk register. Inspected the annual risk assessment executive report, noting it was comprehensive, identified and assessed risks within the System, and summarized risks to remediate.	No exceptions noted.
CC2.1.20	GCommerce's risk register is developed and maintained to continually update risks and controls.	Inspected the IT Risk Management Program to ascertain the procedures for an annual risk assessment and continual development of a risk register. Inspected the current risk register, noting risks are identified, tracked, and addressed, as deemed appropriate and had been updated recently.	No exceptions noted.

Common Criteria Related to Communication and Information (continued)

CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC2.1.21	GCommerce analyzes the various fraud types as fraudulent reporting, loss of assets, and fraud misconduct that can occur within its risk assessment to develop prevention techniques and deter misconduct.	Inspected the IT Risk Management Policy to ascertain the requirements to identify, assess, prioritize and mitigate risks based on the likelihood and impact of potential threats/risks, including fraud risks. Inspected the annual risk assessment executive report and the current risk register to ascertain the consideration and evaluation of fraud risks and summary of management's response to identified risks to be remediated.	No exceptions noted.
CC2.1.22	GCommerce assess fraud risks to identify incentives, pressures, opportunities, attitudes and rationalizations.	Inspected the IT Risk Management Policy to ascertain the requirements to identify, assess, prioritize and mitigate risks based on the likelihood and impact of potential threats/risks, including fraud risks. Inspected the annual risk assessment executive report to ascertain the consideration and evaluation of fraud risks.	No exceptions noted.

Common Criteria Related to Communication and Information (continued)

CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC2.1.23	Management subscribes to threat intelligence and/or compliance resources covering cybersecurity and risks present in the external environment.	Inspected the Company's Cybrary membership, which is used to provide cybersecurity training and best practices. Inspected the BlackHat Conference information and email calendar invitations for team members, which is used to stay current on emerging cybersecurity threats, trends, and industry best practices.	No exceptions noted.
CC2.1.24	Changes to technical environments are assessed for new risks to the GCommerce Bridge before they are implemented.	Inspected the PRT Process to ascertain that changes to technical environments are subject to a risk assessment prior to implementation. Obtained a listing of infrastructure changes and inspected the PRT risk assessment performed prior to project acceptance for a sample of changes.	No exceptions noted.
CC2.1.25	GCommerce utilizes a formal process to authenticate and authorize users.	Inspected the ISP to ascertain that all users must be identified by a unique user ID, utilize a secure password, and use MFA for access. Inspected a list of key application users to verify each user was assigned a unique identity. Inspected system evidence of the MFA configurations to verify MFA is required for system access.	No exceptions noted.

Common Criteria Related to Communication and Information (continued)

CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC2.1.26	Changes considered in scope are requested, reviewed, approved and tracked via the Change Management Standard.	Reviewed the Change Management Standard, within the ISP, to ascertain requirements for tracking procedures for the request, review and approval of changes to infrastructure and applications. Obtained a listing of all changes to infrastructure and applications and inspected the change tickets for a sample of changes to verify the change was requested, reviewed, approved, tested, and tracked according to the Change Management Standard.	No exceptions noted.
CC2.1.27	Testing is performed on all significant changes prior to release to production.	Inspected the Change Management Standard to ascertain the testing procedures required on significant system and application changes. Obtained a listing of all infrastructure and application changes and inspected the change ticket details for a sample of system changes to verify the change was tested, including peer code reviews and user acceptance, within the change management system. Inspected the network diagram, device listing, and change management system to verify that separate environments have been established for development, staging, and production usage.	No exceptions noted.

Common Criteria Related to Communication and Information (continued)

CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC2.1.28	Segregation of duties is enforced for the deployment of code to production.	Inspected the Change Management Standard to ascertain it detailed procedures to support the segregation of duties. Obtained a list of all infrastructure and application changes and inspected the ticket details for a sample of system changes to verify segregation of duties was enforced in accordance with the Change Management Standard.	No exceptions noted.
CC2.1.29	Appropriate approval is required for in-scope changes according to the Change Management Standard.	Inspected the Change Management Standard to ascertain the approval requirements for significant system and application changes. Obtained a listing of all infrastructure and application changes and inspected the ticket details for a sample of system changes to verify the change was requested, reviewed and approved in accordance with the Change Management Standard.	No exceptions noted.
CC2.1.30	Changes to scheduled jobs require management approval and follow the change management procedures.	Inspected the Product Round Table (PRT) Process to ascertain the procedures required for processing changes to scheduled jobs which include management approval.	No exceptions noted.

Common Criteria Related to Communication and Information (continued)

CC2.1: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC2.1.31	GCommerce has prepared a data flow/ process diagram, detailing the sources of information, relevant systems utilized, and data processing points, to allow for the proper processing, and security, of client data.	Inspected the data flow/process diagram and verified it included details regarding the sources of information, relevant systems utilized, and data processing points.	No exceptions noted.

Common Criteria Related to Communication and Information (continued)

CC2.2: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC2.2.1	The Employee and Consultant Handbooks, ISP and Acceptable Use Policies detail the Company's commitment to security.	Inspected the Employee Handbook, Consultant Handbook and ISP to ascertain they document the Company's commitment to security and include the system's security requirements, procedures to accomplish those security requirements, and individuals assigned with responsibilities of those procedures.	No exceptions noted.
CC2.2.2	GCommerce requires a review of the Employee or Consultant Handbook and Acceptable Use Policy on an annual basis, with acknowledgement from all personnel indicating that they have read, understood, and agree to abide by the rules of behavior.	Obtained a list of all employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, which included acceptable use policies, for a sample of individuals.	No exceptions noted.
CC2.2.3	In addition to requiring a review of the Employee or Consultant Handbook and Acceptable Use Policy, GCommerce requires employees and contractors to sign agreements that include provisions and asset protection responsibilities upon hire.	Obtained a list of new employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, which included asset protection responsibilities, for a sample of new individuals.	No exceptions noted.

Common Criteria Related to Communication and Information (continued)

CC2.2: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC2.2.4	Security compliance and security literacy training is required by all personnel on an annual basis.	Inspected the ISP to verify information security training requirements are detailed for new and existing employees. Obtained a list of new employees and contractors and verified a sample of new individuals completed the required onboarding security training. Obtained a list of all employees and contractors and verified a sample of individuals completed the required annual security training.	No exceptions noted.
CC2.2.5	GCommerce has periodic security literacy and awareness campaigns as security threats arise within the Company or have been identified from threat intelligence and/or compliance resources.	Reviewed documents shared with GCommerce personnel for various security awareness campaigns conducted throughout the scope period.	No exceptions noted.
CC2.2.6	GCommerce support utilizes the 8D problem solving process to establish a permanent corrective action based on analysis of the problem.	Inspected the support ticket and 8D analysis for example system issues to verify the 8D process was followed for significant issues.	No exceptions noted.

Common Criteria Related to Communication and Information (continued)

CC2.2: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC2.2.7	GCommerce's Employee Handbook, Information Security Policy (ISP), and Acceptable Use Policy outline standards of conduct and the commitment to integrity and ethical values within the Company.	Inspected the Employee Handbook, ISP, and Acceptable Use Policy to ascertain the expectations for business conduct and importance of integrity and ethical values.	No exceptions noted.
CC2.2.8	All employees and contractors are required to sign acknowledgement of GCommerce's Employee or Consultant Handbook, ISP, Acceptable Use Policy and any policies or procedures outlining standards of conduct upon hire and annually thereafter.	Inspected the ISP to ascertain the requirements for annual review of the security policies for all personnel. Obtained a list of new employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, ISP, and Acceptable Use Policy for a sample of new employees. Obtained a list of all employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, ISP, and Acceptable Use Policy for a sample of employees.	No exceptions noted.

Common Criteria Related to Communication and Information (continued)

CC2.3: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC2.3.1	GCommerce's Terms and Conditions detail the security and privacy responsibilities of external users.	Inspected the service agreement templates to ascertain the Terms and Conditions detail the security and privacy responsibilities of external users. Obtained a list of all new customers and inspected the signed service agreement, which included the Terms and Conditions, for a sample of customers.	No exceptions noted.
CC2.3.2	GCommerce established a process that allows open communication channels to allow input from stakeholders.	Inspected the Company's website to ascertain a support email and phone number were included in the contact information for GCommerce. Obtained a list of all new customers and inspected the signed service agreement, which included customer support information. Observed system evidence that a Fulfillment Master customer was assigned a GCommerce employee as a contact for open communication and evidence of communication between the customer and GCommerce following the implementation of services.	No exceptions noted.
CC2.3.3	GCommerce collaborates with other security teams in the automotive aftermarket industry.	Inspected the BlackHat Conference information, meeting schedules and email calendar invitations related to collaboration with other organizations' security teams.	No exceptions noted.

Common Criteria Related to Risk Assessment

CC3.1: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC3.1.1	GCommerce's formal Information Security Risk Management and Assessment Policy defines criteria for risk mitigation and acceptance.	Inspected the IT Risk Management Program to ascertain the criteria for risk mitigation and acceptance. Inspected the annual risk assessment, noting it detailed risk objectives, was comprehensive, assessed risks on varying tolerance levels, incorporated mitigating controls, and was reviewed by management.	No exceptions noted.
CC3.1.2	GCommerce assesses risks for control families and controls applicable to the Company against the National Institute of Standards and Technology (NIST) 800-53, an industry standard framework.	Inspected the IT Risk Management Program to ascertain it detailed the scope, risk management components and procedures in place to identify and assess risks. Inspected the annual risk assessment executive report, noting it was performed against a subset of controls from NIST 800-53.	No exceptions noted.
CC3.1.3	GCommerce performs a risk assessment annually based on objectives incorporated from service commitments and system requirements.	Inspected the IT Risk Management Program to ascertain the procedures for an annual risk assessment and continual development of a risk register. Inspected the annual risk assessment executive report, noting it was comprehensive, identified and assessed risks within the System, and summarized risks to remediate.	No exceptions noted.

Common Criteria Related to Risk Assessment (continued)

CC3.1: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC3.1.4	GCommerce's risk register is developed and maintained to continually update risks and controls.	Inspected the IT Risk Management Program to ascertain the procedures for an annual risk assessment and continual development of a risk register. Inspected the current risk register, noting risks are identified, tracked, and addressed, as deemed appropriate and had been updated recently.	No exceptions noted.
CC3.1.5	GCommerce analyzes the various fraud types as fraudulent reporting, loss of assets, and fraud misconduct that can occur within its risk assessment to develop prevention techniques and deter misconduct.	Inspected the IT Risk Management Policy to ascertain the requirements to identify, assess, prioritize and mitigate risks based on the likelihood and impact of potential threats/risks, including fraud risks. Inspected the annual risk assessment executive report and the current risk register to ascertain the consideration and evaluation of fraud risks and summary of management's response to identified risks to be remediated.	No exceptions noted.

Common Criteria Related to Risk Assessment (continued)

CC3.1: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC3.1.6	GCommerce assess fraud risks to identify incentives, pressures, opportunities, attitudes and rationalizations.	Inspected the IT Risk Management Policy to ascertain the requirements to identify, assess, prioritize and mitigate risks based on the likelihood and impact of potential threats/risks, including fraud risks. Inspected the annual risk assessment executive report to ascertain the consideration and evaluation of fraud risks.	No exceptions noted.
CC3.1.7	Management subscribes to threat intelligence and/or compliance resources covering cybersecurity and risks present in the external environment.	Inspected the Company's Cybrary membership, which is used to provide cybersecurity training and best practices. Inspected the BlackHat Conference information and email calendar invitations for team members, which is used to stay current on emerging cybersecurity threats, trends, and industry best practices.	No exceptions noted.
CC3.1.8	Changes to technical environments are assessed for new risks to the GCommerce Bridge before they are implemented.	Inspected the PRT Process to ascertain that changes to technical environments are subject to a risk assessment prior to implementation. Obtained a listing of infrastructure changes and inspected the PRT risk assessment performed prior to project acceptance for a sample of changes.	No exceptions noted.

Common Criteria Related to Risk Assessment (continued)

CC3.1: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC3.1.9	GCommerce utilizes a formal process to authenticate and authorize users.	Inspected the ISP to ascertain that all users must be identified by a unique user ID, utilize a secure password, and use MFA for access. Inspected a list of key application users to verify each user was assigned a unique identity. Inspected system evidence of the MFA configurations to verify MFA is required for system access.	No exceptions noted.
CC3.1.10	GCommerce has a formal IT Risk Management Policy to identify, assess, prioritize, and mitigate risks based on the likelihood and impact of the potential threats/risks, which is reviewed at least annually.	Inspected the IT Risk Management Policy to ascertain the requirements to identify, assess, prioritize and mitigate risks based on the likelihood and impact of potential threats/risks.	No exceptions noted.

Common Criteria Related to Risk Assessment (continued)

CC3.2: COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC3.2.1	GCommerce performs a risk assessment annually based on objectives incorporated from service commitments and system requirements.	Inspected the IT Risk Management Program to ascertain the procedures for an annual risk assessment and continual development of a risk register. Inspected the annual risk assessment executive report, noting it was comprehensive, identified and assessed risks within the System, and summarized risks to remediate.	No exceptions noted.
CC3.2.2	GCommerce's risk register is developed and maintained to continually update risks and controls.	Inspected the IT Risk Management Program to ascertain the procedures for an annual risk assessment and continual development of a risk register. Inspected the current risk register, noting risks are identified, tracked, and addressed, as deemed appropriate and had been updated recently.	No exceptions noted.
CC3.2.3	GCommerce's Employee Handbook, Information Security Policy (ISP), and Acceptable Use Policy outline standards of conduct and the commitment to integrity and ethical values within the Company.	Inspected the Employee Handbook, ISP, and Acceptable Use Policy to ascertain the expectations for business conduct and importance of integrity and ethical values.	No exceptions noted.

Common Criteria Related to Risk Assessment (continued)

CC3.2: COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC3.2.4	GCommerce's formal Information Security Risk Management and Assessment Policy defines criteria for risk mitigation and acceptance.	Inspected the IT Risk Management Program to ascertain the criteria for risk mitigation and acceptance. Inspected the annual risk assessment, noting it detailed risk objectives, was comprehensive, assessed risks on varying tolerance levels, incorporated mitigating controls, and was reviewed by management.	No exceptions noted.
CC3.2.5	GCommerce assesses risks for control families and controls applicable to the Company against the National Institute of Standards and Technology (NIST) 800-53, an industry standard framework.	Inspected the IT Risk Management Program to ascertain it detailed the scope, risk management components and procedures in place to identify and assess risks. Inspected the annual risk assessment executive report, noting it was performed against a subset of controls from NIST 800-53.	No exceptions noted.
CC3.2.6	GCommerce analyzes the various fraud types as fraudulent reporting, loss of assets, and fraud misconduct that can occur within its risk assessment to develop prevention techniques and deter misconduct.	Inspected the IT Risk Management Policy to ascertain the requirements to identify, assess, prioritize and mitigate risks based on the likelihood and impact of potential threats/risks, including fraud risks.	No exceptions noted.

Common Criteria Related to Risk Assessment (continued)

CC3.2: COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC3.2.6	(continued)	Inspected the annual risk assessment executive report and the current risk register to ascertain the consideration and evaluation of fraud risks and summary of management's response to identified risks to be remediated.	(continued)
CC3.2.7	GCommerce assess fraud risks to identify incentives, pressures, opportunities, attitudes and rationalizations.	Inspected the IT Risk Management Policy to ascertain the requirements to identify, assess, prioritize and mitigate risks based on the likelihood and impact of potential threats/risks, including fraud risks. Inspected the annual risk assessment executive report to ascertain the consideration and evaluation of fraud risks.	No exceptions noted.
CC3.2.8	Management subscribes to threat intelligence and/or compliance resources covering cybersecurity and risks present in the external environment.	Inspected the Company's Cybrary membership, which is used to provide cybersecurity training and best practices. Inspected the BlackHat Conference information and email calendar invitations for team members, which is used to stay current on emerging cybersecurity threats, trends, and industry best practices.	No exceptions noted.

Common Criteria Related to Risk Assessment (continued)

CC3.2: COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC3.2.9	Changes to technical environments are assessed for new risks to the GCommerce Bridge before they are implemented.	Inspected the PRT Process to ascertain that changes to technical environments are subject to a risk assessment prior to implementation. Obtained a listing of infrastructure changes and inspected the PRT risk assessment performed prior to project acceptance for a sample of changes.	No exceptions noted.
CC3.2.10	GCommerce utilizes a formal process to authenticate and authorize users.	Inspected the ISP to ascertain that all users must be identified by a unique user ID, utilize a secure password, and use MFA for access. Inspected a list of key application users to verify each user was assigned a unique identity. Inspected system evidence of the MFA configurations to verify MFA is required for system access.	No exceptions noted.
CC3.2.11	GCommerce has a formal IT Risk Management Policy to identify, assess, prioritize, and mitigate risks based on the likelihood and impact of the potential threats/risks, which is reviewed at least annually.	Inspected the IT Risk Management Policy to ascertain the requirements to identify, assess, prioritize and mitigate risks based on the likelihood and impact of potential threats/risks.	No exceptions noted.

Common Criteria Related to Risk Assessment (continued)

CC3.3: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC3.3.1	GCommerce analyzes the various fraud types as fraudulent reporting, loss of assets, and fraud misconduct that can occur within its risk assessment to develop prevention techniques and deter misconduct.	Inspected the IT Risk Management Policy to ascertain the requirements to identify, assess, prioritize and mitigate risks based on the likelihood and impact of potential threats/risks, including fraud risks. Inspected the annual risk assessment executive report and the current risk register to ascertain the consideration and evaluation of fraud risks and summary of management's response to identified risks to be remediated.	No exceptions noted.
CC3.3.2	GCommerce assess fraud risks to identify incentives, pressures, opportunities, attitudes and rationalizations.	Inspected the IT Risk Management Policy to ascertain the requirements to identify, assess, prioritize and mitigate risks based on the likelihood and impact of potential threats/risks, including fraud risks. Inspected the annual risk assessment executive report to ascertain the consideration and evaluation of fraud risks.	No exceptions noted.

Common Criteria Related to Risk Assessment (continued)

CC3.3: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC3.3.3	GCommerce's formal Information Security Risk Management and Assessment Policy defines criteria for risk mitigation and acceptance.	Inspected the IT Risk Management Program to ascertain the criteria for risk mitigation and acceptance. Inspected the annual risk assessment, noting it detailed risk objectives, was comprehensive, assessed risks on varying tolerance levels, incorporated mitigating controls, and was reviewed by management.	No exceptions noted.
CC3.3.4	GCommerce assesses risks for control families and controls applicable to the Company against the National Institute of Standards and Technology (NIST) 800-53, an industry standard framework.	Inspected the IT Risk Management Program to ascertain it detailed the scope, risk management components and procedures in place to identify and assess risks. Inspected the annual risk assessment executive report, noting it was performed against a subset of controls from NIST 800-53.	No exceptions noted.
CC3.3.5	GCommerce performs a risk assessment annually based on objectives incorporated from service commitments and system requirements.	Inspected the IT Risk Management Program to ascertain the procedures for an annual risk assessment and continual development of a risk register. Inspected the annual risk assessment executive report, noting it was comprehensive, identified and assessed risks within the System, and summarized risks to remediate.	No exceptions noted.

Common Criteria Related to Risk Assessment (continued)

CC3.3: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC3.3.6	GCommerce's risk register is developed and maintained to continually update risks and controls.	Inspected the IT Risk Management Program to ascertain the procedures for an annual risk assessment and continual development of a risk register. Inspected the current risk register, noting risks are identified, tracked, and addressed, as deemed appropriate and had been updated recently.	No exceptions noted.
CC3.3.7	Management subscribes to threat intelligence and/or compliance resources covering cybersecurity and risks present in the external environment.	Inspected the Company's Cybrary membership, which is used to provide cybersecurity training and best practices. Inspected the BlackHat Conference information and email calendar invitations for team members, which is used to stay current on emerging cybersecurity threats, trends, and industry best practices.	No exceptions noted.
CC3.3.8	Changes to technical environments are assessed for new risks to the GCommerce Bridge before they are implemented.	Inspected the PRT Process to ascertain that changes to technical environments are subject to a risk assessment prior to implementation. Obtained a listing of infrastructure changes and inspected the PRT risk assessment performed prior to project acceptance for a sample of changes.	No exceptions noted.

Common Criteria Related to Risk Assessment (continued)

CC3.3: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC3.3.9	GCommerce utilizes a formal process to authenticate and authorize users.	Inspected the ISP to ascertain that all users must be identified by a unique user ID, utilize a secure password, and use MFA for access. Inspected a list of key application users to verify each user was assigned a unique identity. Inspected system evidence of the MFA configurations to verify MFA is required for system access.	No exceptions noted.
CC3.3.10	GCommerce has a formal IT Risk Management Policy to identify, assess, prioritize, and mitigate risks based on the likelihood and impact of the potential threats/risks, which is reviewed at least annually.	Inspected the IT Risk Management Policy to ascertain the requirements to identify, assess, prioritize and mitigate risks based on the likelihood and impact of potential threats/risks.	No exceptions noted.

Common Criteria Related to Risk Assessment (continued)

CC3.4: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC3.4.1	Management subscribes to threat intelligence and/or compliance resources covering cybersecurity and risks present in the external environment.	Inspected the Company's Cybrary membership, which is used to provide cybersecurity training and best practices. Inspected the BlackHat Conference information and email calendar invitations for team members, which is used to stay current on emerging cybersecurity threats, trends, and industry best practices.	No exceptions noted.
CC3.4.2	Changes to technical environments are assessed for new risks to the GCommerce Bridge before they are implemented.	Inspected the PRT Process to ascertain that changes to technical environments are subject to a risk assessment prior to implementation. Obtained a listing of infrastructure changes and inspected the PRT risk assessment performed prior to project acceptance for a sample of changes.	No exceptions noted.
CC3.4.3	GCommerce's formal Information Security Risk Management and Assessment Policy defines criteria for risk mitigation and acceptance.	Inspected the IT Risk Management Program to ascertain the criteria for risk mitigation and acceptance. Inspected the annual risk assessment, noting it detailed risk objectives, was comprehensive, assessed risks on varying tolerance levels, incorporated mitigating controls, and was reviewed by management.	No exceptions noted.

Common Criteria Related to Risk Assessment (continued)

CC3.4: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC3.4.4	GCommerce assesses risks for control families and controls applicable to the Company against the National Institute of Standards and Technology (NIST) 800-53, an industry standard framework.	Inspected the IT Risk Management Program to ascertain it detailed the scope, risk management components and procedures in place to identify and assess risks. Inspected the annual risk assessment executive report, noting it was performed against a subset of controls from NIST 800-53.	No exceptions noted.
CC3.4.5	GCommerce performs a risk assessment annually based on objectives incorporated from service commitments and system requirements.	Inspected the IT Risk Management Program to ascertain the procedures for an annual risk assessment and continual development of a risk register. Inspected the annual risk assessment executive report, noting it was comprehensive, identified and assessed risks within the System, and summarized risks to remediate.	No exceptions noted.
CC3.4.6	GCommerce's risk register is developed and maintained to continually update risks and controls.	Inspected the IT Risk Management Program to ascertain the procedures for an annual risk assessment and continual development of a risk register. Inspected the current risk register, noting risks are identified, tracked, and addressed, as deemed appropriate and had been updated recently.	No exceptions noted.

Common Criteria Related to Risk Assessment (continued)

CC3.4: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC3.4.7	GCommerce utilizes a formal process to authenticate and authorize users.	Inspected the ISP to ascertain that all users must be identified by a unique user ID, utilize a secure password, and use MFA for access. Inspected a list of key application users to verify each user was assigned a unique identity. Inspected system evidence of the MFA configurations to verify MFA is required for system access.	No exceptions noted.
CC3.4.8	GCommerce has a formal IT Risk Management Policy to identify, assess, prioritize, and mitigate risks based on the likelihood and impact of the potential threats/risks, which is reviewed at least annually.	Inspected the IT Risk Management Policy to ascertain the requirements to identify, assess, prioritize and mitigate risks based on the likelihood and impact of potential threats/risks.	No exceptions noted.

Common Criteria Related to Monitoring Activities

CC4.1: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC4.1.1	GCommerce works with external assessors to provide independent and objective reviews of risks assuring that the Company is appropriately addressing its risks.	Inspected the Statement of Work with the external assessor to ascertain the expectation to perform an annual risk assessment and penetration test. Inspected the results of the annual risk assessment and annual penetration test to ascertain the frequency of the tests, the independence of the assessor, and management's remediation approach to findings.	No exceptions noted.
CC4.1.2	GCommerce utilizes a ticketing process for all system changes, which are reviewed by the appropriate level of management before implemented.	Inspected the PRT Process to ascertain that system changes are subject to a ticketing process and are reviewed prior to implementation. Obtained a listing of all application and infrastructure changes and inspected the change management ticket to verify the appropriate level of management approved the change prior to deploying into production, as required by the PRT Process, for a sample of system changes.	No exceptions noted.
CC4.1.3	External penetration testing is performed on an annual basis. The results are reviewed by management and findings are remediated, where possible.	Inspected the ISP to ascertain an annual penetration test must be completed over information systems. Inspected the annual external penetration test results report and verified actionable steps were taken to remediate a sample of high risk findings.	No exceptions noted.

Common Criteria Related to Monitoring Activities (continued)

CC4.1: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC4.1.4	GCommerce utilizes a SIEM to monitor the effectiveness of controls.	Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely. Obtained a listing of SIEM devices being monitored and compared the detail to the inventory of critical IT assets to determine critical components of the system were subject to monitoring.	No exceptions noted.
CC4.1.5	GCommerce policies, standards procedures are developed and implemented to address risk factors.	Inspected the ISP, Employee Handbook and related security policies to ascertain the development and implementation standards to address risk factors.	No exceptions noted.
CC4.1.6	GCommerce policies and standard procedures are developed and implemented for controls over technology.	Inspected the ISP, Employee Handbook and related security policies to ascertain the development and implementation standards for controls over technology.	No exceptions noted.

Common Criteria Related to Monitoring Activities (continued)

CC4.1: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC4.1.7	GCommerce utilizes a ticketing process for control activities.	Inquired with management and reviewed security policies to ascertain that key control activities are subject to a ticketing process. Obtained a list of application and infrastructure changes and inspected the change management ticket for a sample of changes to verify each change was accompanied by a detailed ticket. Inspected the project, and ticket details, created to remediate a sample of penetration test findings. Inspected the support ticket for example significant system issues, along with the 8D analysis, to verify a ticket was created to track significant issues through resolution.	No exceptions noted.

Common Criteria Related to Monitoring Activities (continued)

CC4.2: COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC4.2.1	GCommerce uses the PRT process to review assessment findings, identifies changes/ enhancements that need to be implemented, and follows a formal Project Life Cycle (PLC) process for plan of action and milestones.	Reviewed the PRT process documentation to ascertain it details steps to review assessment findings, identify changes/ enhancements that need to be implemented, and follows a formal PLC process for plans of action and milestones. Inspected the results of the annual penetration test and inspected the change ticket for a sample of high risk findings from the annual penetration test to verify the finding was remediated timely in accordance with the PRT and PLC processes. Obtained a listing of all changes to infrastructure and applications and, for a sample of changes, inspected system evidence that the PRT Committee approved the change, and system evidence that the change following the PLC process, including testing, reviews, and approvals.	No exceptions noted.

Common Criteria Related to Monitoring Activities (continued)

CC4.2: COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC4.2.2	GCommerce works with external assessors to provide independent and objective review of risks assuring that the Company is appropriately addressing its risks.	Inspected the Statement of Work with the external assessor to ascertain the expectation to perform an annual risk assessment and penetration test. Inspected the results of the annual risk assessment and annual penetration test to ascertain the frequency of the tests, the independence of the assessor, and management's remediation approach to findings.	No exceptions noted.
CC4.2.3	GCommerce utilizes a ticketing process for all system changes, which are reviewed by the appropriate level of management before implemented.	Inspected the PRT Process to ascertain that system changes are subject to a ticketing process and are reviewed prior to implementation. Obtained a listing of all application and infrastructure changes and inspected the change management ticket to verify the appropriate level of management approved the change prior to deploying into production, as required by the PRT Process, for a sample of system changes.	No exceptions noted.

Common Criteria Related to Monitoring Activities (continued)

CC4.2: COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC4.2.4	External penetration testing is performed on an annual basis. The results are reviewed by management and findings are remediated, where possible.	Inspected the ISP to ascertain an annual penetration test must be completed over information systems. Inspected the annual external penetration test results report and verified actionable steps were taken to remediate a sample of high risk findings.	No exceptions noted.
CC4.2.5	GCommerce utilizes a SIEM to monitor the effectiveness of controls.	Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely. Obtained a listing of SIEM devices being monitored and compared the detail to the inventory of critical IT assets to determine critical components of the system were subject to monitoring.	No exceptions noted.
CC4.2.6	GCommerce policies, standards procedures are developed and implemented to address risk factors.	Inspected the ISP, Employee Handbook and related security policies to ascertain the development and implementation standards to address risk factors.	No exceptions noted.
CC4.2.7	GCommerce policies and standard procedures are developed and implemented for controls over technology.	Inspected the ISP, Employee Handbook and related security policies to ascertain the development and implementation standards for controls over technology.	No exceptions noted.

Common Criteria Related to Monitoring Activities (continued)

CC4.2: COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC4.2.8	GCommerce utilizes a ticketing process for control activities.	Inquired with management and reviewed security policies to ascertain that key control activities are subject to a ticketing process. Obtained a list of application and infrastructure changes and inspected the change management ticket for a sample of changes to verify each change was accompanied by a detailed ticket. Inspected the project, and ticket details, created to remediate a sample of penetration test findings. Inspected the support ticket for example significant system issues, along with the 8D analysis, to verify a ticket was created to track significant issues through resolution.	No exceptions noted.

Common Criteria Related to Control Activities

CC5.1: COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC5.1.1	GCommerce policies, standards procedures are developed and implemented to address risk factors.	Inspected the ISP, Employee Handbook and related security policies to ascertain the development and implementation standards to address risk factors.	No exceptions noted.
CC5.1.2	GCommerce policies and standard procedures are developed and implemented for controls over technology.	Inspected the ISP, Employee Handbook and related security policies to ascertain the development and implementation standards for controls over technology.	No exceptions noted.
CC5.1.3	GCommerce utilizes a ticketing process for control activities.	Inquired with management and reviewed security policies to ascertain that key control activities are subject to a ticketing process. Obtained a list of application and infrastructure changes and inspected the change management ticket for a sample of changes to verify each change was accompanied by a detailed ticket. Inspected the project, and ticket details, created to remediate a sample of penetration test findings. Inspected the support ticket for example significant system issues, along with the 8D analysis, to verify a ticket was created to track significant issues through resolution.	No exceptions noted.

Common Criteria Related to Control Activities (continued)

CC5.2: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC5.2.1	GCommerce policies and standard procedures are developed and implemented for controls over technology.	Inspected the ISP, Employee Handbook and related security policies to ascertain the development and implementation standards for controls over technology.	No exceptions noted.
CC5.2.2	GCommerce utilizes a ticketing process for control activities.	Inquired with management and reviewed security policies to ascertain that key control activities are subject to a ticketing process. Obtained a list of application and infrastructure changes and inspected the change management ticket for a sample of changes to verify each change was accompanied by a detailed ticket. Inspected the project, and ticket details, created to remediate a sample of penetration test findings. Inspected the support ticket for example significant system issues, along with the 8D analysis, to verify a ticket was created to track significant issues through resolution.	No exceptions noted.

Common Criteria Related to Control Activities (continued)

CC5.2: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC5.2.3	GCommerce utilizes a formal process to authenticate and authorize users.	Inspected the ISP to ascertain that all users must be identified by a unique user ID, utilize a secure password, and use MFA for access. Inspected a list of key application users to verify each user was assigned a unique identity. Inspected system evidence of the MFA configurations to verify MFA is required for system access.	No exceptions noted.
CC5.2.4	GCommerce's Employee Handbook, ISP, and Acceptable Use Policy are reviewed and approved on an annual basis by senior management.	Reviewed the Employee Handbook, ISP, and Acceptable Use Policy to ascertain the documents were reviewed and approved by senior management during the year.	No exceptions noted.
CC5.2.5	All employees and contractors are required to sign acknowledgement of GCommerce's Employee or Consultant Handbook, ISP, Acceptable Use Policy and any policies or procedures outlining standards of conduct upon hire and annually thereafter.	Inspected the ISP to ascertain the requirements for annual review of the security policies for all personnel. Obtained a list of new employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, ISP, and Acceptable Use Policy for a sample of new employees.	No exceptions noted.

Common Criteria Related to Control Activities (continued)

CC5.2: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC5.2.5	(continued)	Obtained a list of all employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, ISP, and Acceptable Use Policy for a sample of employees.	(continued)
CC5.2.6	GCommerce evaluates candidates to fill a position.	Inspected the ISP to ascertain the requirements for detailed interviews to be conducted as a prerequisite to being hired. Obtained a list of new employees and verified a sample of new employees were hired through a recruiting agency, who is responsible for completing an interview process and review of the candidates' qualifications prior to hire.	No exceptions noted.
CC5.2.7	Internal user account creation, modification, and deletion must be requested via access provisioning tool.	Obtained a listing of new employees and contractors and inspected system evidence of management's approval of access for a sample of new individuals. Obtained a listing of terminated employees and contractors and inspected the termination email, along with system evidence, for a sample of individuals, to verify access was removed.	No exceptions noted.

Common Criteria Related to Control Activities (continued)

CC5.3: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC5.3.1	A risk register is developed and maintained to continually update risks and controls.	Inspected the IT Risk Management Program to verify a risk register is to be developed and maintained in conjunction with the annual risk assessment. Inspected the current risk register, noting risks are identified, tracked, and addressed, as deemed appropriate, and had been updated recently.	No exceptions noted.
CC5.3.2	GCommerce's Employee Handbook, ISP, and Acceptable Use Policy are reviewed and approved on an annual basis by senior management.	Reviewed the Employee Handbook, ISP, and Acceptable Use Policy to ascertain the documents were reviewed and approved by senior management during the year.	No exceptions noted.
CC5.3.3	All employees and contractors are required to sign acknowledgement of GCommerce's Employee or Consultant Handbook, ISP, Acceptable Use Policy and any policies or procedures outlining standards of conduct upon hire and annually thereafter.	Inspected the ISP to ascertain the requirements for annual review of the security policies for all personnel. Obtained a list of new employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, ISP, and Acceptable Use Policy for a sample of new employees. Obtained a list of all employees and contractors and inspected the signed acknowledgement of the Employee or Consultant Handbook, ISP, and Acceptable Use Policy for a sample of employees.	No exceptions noted.

Common Criteria Related to Control Activities (continued)

CC5.3: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC5.3.4	Management has established an organizational chart to define its organizational structures, reporting lines, and areas of authority.	Inspected the organizational chart and discussed it with management, noting appropriate reporting lines have been established.	No exceptions noted.
CC5.3.5	GCommerce outlines the responsibility and accountability of the CIO/CTO and senior management in regards to control design, implementation and monitoring.	Inspected the ISP to verify the responsibility and accountability of the CIO/CTO and senior management regarding control design, implementation and monitoring are defined.	No exceptions noted.
CC5.3.6	GCommerce evaluates candidates to fill a position.	Inspected the ISP to ascertain the requirements for detailed interviews to be conducted as a prerequisite to being hired. Obtained a list of new employees and verified a sample of new employees were hired through a recruiting agency, who is responsible for completing an interview process and review of the candidates' qualifications prior to hire.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.1.1	GCommerce has access management policies and procedures in place.	Inspected the ISP and Remote Work Policy to ascertain the inclusion of access management policies and procedures.	No exceptions noted.
CC6.1.2	Internal privileged system users are required to change their passwords every 90 days.	Reviewed the ISP to ascertain the standards for user passwords, which include the requirement for system users to change their passwords every 90 days. Inspected the network domain settings to verify the network is configured to meet the password change requirements.	No exceptions noted.
CC6.1.3	System session timeouts are set for 60 minutes and desktop screensavers are set for 15 minutes to limit unauthorized access.	Reviewed the Acceptable Use Policy to ascertain the standards for session timeouts and desktop screensaver activations. Inspected the network domain settings to verify web session timeouts are configured for 60 minutes and desktop screensavers are configured for 15 minutes.	No exceptions noted.
CC6.1.4	Users are assigned unique identifiers and passwords within the system.	Inspected the ISP to ascertain that all users must be identified by a unique user ID and utilize a secure password that meets complexity requirements.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.1.4	(continued)	Inspected a list of network and key application users to verify each user was assigned a unique identity. Observed an employee log into the network using a unique user ID and password. Inspected the network domain settings to verify the network is configured to meet password requirements established by the ISP.	(continued)
CC6.1.5	Internal user account creation, modification, and deletion must be requested via access provisioning tool.	Obtained a listing of new employees and contractors and inspected system evidence of management's approval of access for a sample of new individuals. Obtained a listing of terminated employees and contractors and inspected the termination email, along with system evidence, for a sample of individuals, to verify access was removed.	No exceptions noted.
CC6.1.6	GCommerce has rules around configuration management and has created procedures by department and products.	Reviewed the ISP to ascertain it includes standardized rules for configuration management and procedures by department and products.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.1.7	GCommerce evaluates candidates to fill a position.	Inspected the ISP to ascertain the requirements for detailed interviews to be conducted as a prerequisite to being hired. Obtained a list of new employees and verified a sample of new employees were hired through a recruiting agency, who is responsible for completing an interview process and review of the candidates' qualifications prior to hire.	No exceptions noted.
CC6.1.8	Internal user accounts must be approved by management.	Inspected the ISP to ascertain the procedures for changes to internal user accounts which can only be made at the request of approving management. Obtained a listing of new employees and contractors and inspected system evidence of management's approval of access for a sample of users. Obtained a list of users with changes in application access and inspected evidence of management's approval of access for a sample of users.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.1.9	Internal users with revoked authorization are removed from the system timely.	Inspected the ISP to ascertain the requirements surrounding the removal of user accounts upon termination. Obtained a list of all employees with revoked authorization and inspected the email requesting the removal of security access and verified system credentials were updated within 24 hours.	No exceptions noted.
CC6.1.10	External users are required to complete a training program prior to using the application.	Reviewed the contract templates to ascertain the requirement for external users to complete a training program prior to using the application. Obtained a listing of new customers and, for a sample of customers, inspected evidence that training materials were provided to the customers prior to using the application.	No exceptions noted.
CC6.1.11	A formal process is in place to remove user access when an employee is terminated.	Inspected the ISP to ascertain the requirements surrounding the removal of user accounts upon termination. Obtained a listing of terminated employees and contractors and inspected the termination email, along with system evidence, for a sample of individuals, to verify access was removed.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.1.12	Changes in employment status require the review and/or termination of access.	Inspected the ISP to ascertain the procedures for changes to internal user accounts which can only be made at the request of approving management. Obtained a listing of employees with changes in selected application access and inspected evidence of management's approval of the access change for a sample of employees.	No exceptions noted.
CC6.1.13	Internal user account access must be approved by management and administrator access is limited to necessary employees based on their role in the system.	Inspected the ISP to ascertain the principle of least privilege is utilized by GCommerce. Inspected the administrator user listings for the network domain and key applications and reviewed the job titles for the users to ascertain that administrator user roles are limited. Obtained a listing of new employees and contractors and inspected system evidence of management's approval of access for a sample of users. Obtained a list of users with changes in application access and inspected evidence of management's approval for a sample of users with access changes.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.1.14	GCommerce requires VPN access for remote users and requires users to follow the Remote Work Policy and BYOD Policy for access outside of the Company network.	Inspected the Remote Work Policy and BYOD policy, within the Acceptable Use Policy, to ascertain a VPN is required to gain remote access to the Company network and cloud applications. Observed an employee access the network and cloud applications remotely, which required VPN access. Inspected the security group rule established that requires remote users to VPN into the home office before gaining access to Company systems.	No exceptions noted.
CC6.1.15	Changes considered in scope are requested, reviewed, approved and tracked via the Change Management Standard.	Reviewed the Change Management Standard, within the ISP, to ascertain requirements for tracking procedures for the request, review and approval of changes to infrastructure and applications. Obtained a listing of all changes to infrastructure and applications and inspected the change tickets for a sample of changes to verify the change was requested, reviewed, approved, tested, and tracked according to the Change Management Standard.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.1.16	Testing is performed on all significant changes prior to release to production.	Inspected the Change Management Standard to ascertain the testing procedures required on significant system and application changes. Obtained a listing of all infrastructure and application changes and inspected the change ticket details for a sample of system changes to verify the change was tested, including peer code reviews and user acceptance, within the change management system. Inspected the network diagram, device listing, and change management system to verify that separate environments have been established for development, staging, and production usage.	No exceptions noted.
CC6.1.17	Segregation of duties is enforced for the deployment of code to production.	Inspected the Change Management Standard to ascertain it detailed procedures to support the segregation of duties. Obtained a list of all infrastructure and application changes and inspected the ticket details for a sample of system changes to verify segregation of duties was enforced in accordance with the Change Management Standard.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.1.18	Appropriate approval is required for in-scope changes according to the Change Management Standard.	Inspected the Change Management Standard to ascertain the approval requirements for significant system and application changes. Obtained a listing of all infrastructure and application changes and inspected the ticket details for a sample of system changes to verify the change was requested, reviewed and approved in accordance with the Change Management Standard.	No exceptions noted.
CC6.1.19	Changes to scheduled jobs require management approval and follow the change management procedures.	Inspected the Product Round Table (PRT) Process to ascertain the procedures required for processing changes to scheduled jobs which include management approval.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.2.1	Internal user accounts must be approved by management.	Inspected the ISP to ascertain the procedures for changes to internal user accounts which can only be made at the request of approving management. Obtained a listing of new employees and contractors and inspected system evidence of management's approval of access for a sample of users. Obtained a list of users with changes in application access and inspected evidence of management's approval of access for a sample of users.	No exceptions noted.
CC6.2.2	Internal users with revoked authorization are removed from the system timely.	Inspected the ISP to ascertain the requirements surrounding the removal of user accounts upon termination. Obtained a list of all employees with revoked authorization and inspected the email requesting the removal of security access and verified system credentials were updated within 24 hours.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.2.3	External users are required to complete a training program prior to using the application.	Reviewed the contract templates to ascertain the requirement for external users to complete a training program prior to using the application. Obtained a listing of new customers and, for a sample of customers, inspected evidence that training materials were provided to the customers prior to using the application.	No exceptions noted.
CC6.2.4	A formal process is in place to remove user access when an employee is terminated.	Inspected the ISP to ascertain the requirements surrounding the removal of user accounts upon termination. Obtained a listing of terminated employees and contractors and inspected the termination email, along with system evidence, for a sample of individuals, to verify access was removed.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.2.5	Changes in employment status require the review and/or termination of access.	Inspected the ISP to ascertain the procedures for changes to internal user accounts which can only be made at the request of approving management. Obtained a listing of employees with changes in selected application access and inspected evidence of management's approval of the access change for a sample of employees.	No exceptions noted.
CC6.2.6	System session timeouts are set for 60 minutes and desktop screensavers are set for 15 minutes to limit unauthorized access.	Reviewed the Acceptable Use Policy to ascertain the standards for session timeouts and desktop screensaver activations. Inspected the network domain settings to verify web session timeouts are configured for 60 minutes and desktop screensavers are configured for 15 minutes.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.2.7	Users are assigned unique identifiers and passwords within the system.	Inspected the ISP to ascertain that all users must be identified by a unique user ID and utilize a secure password that meets complexity requirements. Inspected a list of network and key application users to verify each user was assigned a unique identity. Observed an employee log into the network using a unique user ID and password. Inspected the network domain settings to verify the network is configured to meet password requirements established by the ISP.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.3.1	Internal user account access must be approved by management and administrator access is limited to necessary employees based on their role in the system.	Inspected the ISP to ascertain the principle of least privilege is utilized by GCommerce. Inspected the administrator user listings for the network domain and key applications and reviewed the job titles for the users to ascertain that administrator user roles are limited. Obtained a listing of new employees and contractors and inspected system evidence of management's approval of access for a sample of users. Obtained a list of users with changes in application access and inspected evidence of management's approval for a sample of users with access changes.	No exceptions noted.
CC6.3.2	Users of the systems are assigned roles and permissions based on their needs.	Inspected the ISP to ascertain the principle of least privilege is utilized by GCommerce. Inspected the pre-defined network and key application security groups and roles to verify user roles are segregated within the network.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.3.2	(continued)	Obtained a listing of new employees and contractors and inspected evidence of management's approval of access for a sample of users to verify access was assigned based on job responsibilities and needs, as approved by management.	(continued)
CC6.3.3	Users are assigned unique identifiers and passwords within the system.	Inspected the ISP to ascertain that all users must be identified by a unique user ID and utilize a secure password that meets complexity requirements. Inspected a list of network and key application users to verify each user was assigned a unique identity. Observed an employee log into the network using a unique user ID and password. Inspected the network domain settings to verify the network is configured to meet password requirements established by the ISP.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.3.4	Internal user accounts must be approved by management.	Inspected the ISP to ascertain the procedures for changes to internal user accounts which can only be made at the request of approving management. Obtained a listing of new employees and contractors and inspected system evidence of management's approval of access for a sample of users. Obtained a list of users with changes in application access and inspected evidence of management's approval of access for a sample of users.	No exceptions noted.
CC6.3.5	Internal users with revoked authorization are removed from the system timely.	Inspected the ISP to ascertain the requirements surrounding the removal of user accounts upon termination. Obtained a list of all employees with revoked authorization and inspected the email requesting the removal of security access and verified system credentials were updated within 24 hours.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.3.6	External users are required to complete a training program prior to using the application.	Reviewed the contract templates to ascertain the requirement for external users to complete a training program prior to using the application. Obtained a listing of new customers and, for a sample of customers, inspected evidence that training materials were provided to the customers prior to using the application.	No exceptions noted.
CC6.3.7	A formal process is in place to remove user access when an employee is terminated.	Inspected the ISP to ascertain the requirements surrounding the removal of user accounts upon termination. Obtained a listing of terminated employees and contractors and inspected the termination email, along with system evidence, for a sample of individuals, to verify access was removed.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.3.8	Changes in employment status require the review and/or termination of access.	Inspected the ISP to ascertain the procedures for changes to internal user accounts which can only be made at the request of approving management. Obtained a listing of employees with changes in selected application access and inspected evidence of management's approval of the access change for a sample of employees.	No exceptions noted.
CC6.3.9	Systems are patched to ensure security vulnerabilities are remediated.	Inspected the ISP to ascertain system patches and updates are to be obtained and deployed in a timely manner. Inspected system settings to ascertain they were configured to automatically download and deploy Microsoft operating system updates to workstations. Obtained the critical asset inventory listing and inspected system evidence of operating system details on a sample of servers and workstations to verify the devices were current on updates to the operating system.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.3.10	The Change Management process and IT Risk Management Program address security impacts during the system lifecycle.	Inspected the Product Life Cycle Process and the IT Risk Management Program to ascertain they address security analysis and impacts of systems throughout their lifecycle. Obtained a listing of application and infrastructure changes and inspected system evidence within DevOps of a security risk assessment and security testing on a sample of changes prior to being implemented.	No exceptions noted.
CC6.3.11	Anti-malware software automatically checks for updates and updates software daily.	Inspected the ISP to ascertain that all information systems are to have anti-virus and anti-malware solutions deployed with the most current version available from the vendor, enabled for automatic updates and configured for conducting periodic scans, as necessary. Inspected system settings on anti-malware software to ascertain the software performs daily updates.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.3.12	The SIEM is configured to collect logs of Windows, network infrastructure, and firewall security events. Real-time alerts/tickets are generated to members of the IT department for research and resolution when pre-determined thresholds are met.	Inspected the ISP to ascertain information systems are monitored and procedures are in place for identifying, assessing, and resolving security alerts. Inspected the SIEM device listing and verified critical system components are being monitored. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely.	No exceptions noted.
CC6.3.13	Alerts are generated to the IT department when malicious software is detected on company-issued computers. All alerts are reviewed and resolved.	Inspected example alert rules from Cisco Endpoint Secure and Malwarebytes Cloud and alert configurations to verify alerts are generated when malicious activity is detected and appropriate individuals receive the notifications for research and resolution.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.4.1	GCommerce employees are given individual access cards which grants permission to enter office space.	Inspected the ISP noting the requirement to provide an access card to authorized individuals and remove access upon termination of need. Conducted physical observation of the facility to ascertain access cannot be granted without an access card. Obtained a list of new employees and inspected evidence of approval of privileged badge access for a sample of employees, as applicable.	No exceptions noted.
CC6.4.2	GCommerce limits access to sensitive areas (in house server room; media storage) by requiring a unique RF ID key card assigned to limited number of users approved by the CTO.	Inspected the ISP noting access to sensitive areas is limited and must be approved by the CTO. Obtained the list of RF ID key card users and profiles to ascertain that access to sensitive areas is provided to a limited number of users. Obtained a list of employees with new badge access to sensitive areas and inspected job titles for all employees to verify access is reasonable.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.4.3	GCommerce has a Visitor Policy in place and all visitors must sign-in at the front and be escorted at all times.	Inspected the Visitor Policy to ascertain standards for visitors, which included the requirement for all visitors to sign in and out at the front desk and be escorted through the office during their visit. Inspected the completed visitor log sheet for a sample of months, noting all pertinent information was included to identify each visitor.	No exceptions noted.
CC6.4.4	Systems are patched to ensure security vulnerabilities are remediated.	Inspected the ISP to ascertain system patches and updates are to be obtained and deployed in a timely manner. Inspected system settings to ascertain they were configured to automatically download and deploy Microsoft operating system updates to workstations. Obtained the critical asset inventory listing and inspected system evidence of operating system details on a sample of servers and workstations to verify the devices were current on updates to the operating system.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.4.5	The Change Management process and IT Risk Management Program address security impacts during the system lifecycle.	Inspected the Product Life Cycle Process and the IT Risk Management Program to ascertain they address security analysis and impacts of systems throughout their lifecycle. Obtained a listing of application and infrastructure changes and inspected system evidence within DevOps of a security risk assessment and security testing on a sample of changes prior to being implemented.	No exceptions noted.
CC6.4.6	Anti-malware software automatically checks for updates and updates software daily.	Inspected the ISP to ascertain that all information systems are to have anti-virus and anti-malware solutions deployed with the most current version available from the vendor, enabled for automatic updates and configured for conducting periodic scans, as necessary. Inspected system settings on anti-malware software to ascertain the software performs daily updates.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.4.7	The SIEM is configured to collect logs of Windows, network infrastructure, and firewall security events. Real-time alerts/tickets are generated to members of the IT department for research and resolution when pre-determined thresholds are met.	Inspected the ISP to ascertain information systems are monitored and procedures are in place for identifying, assessing, and resolving security alerts. Inspected the SIEM device listing and verified critical system components are being monitored. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely.	No exceptions noted.
CC6.4.8	Alerts are generated to the IT department when malicious software is detected on company-issued computers. All alerts are reviewed and resolved.	Inspected example alert rules from Cisco Endpoint Secure and Malwarebytes Cloud and alert configurations to verify alerts are generated when malicious activity is detected and appropriate individuals receive the notifications for research and resolution.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.5.1	GCommerce has sanitization mechanisms and procedures in place.	Inspected the ISP to ascertain all sensitive data is to be wiped, shredded, destroyed, and/or disintegrated prior to equipment disposal, re-use or release from GCommerce's control. Inquired of management, who stated there were no disposals, re-use or release of equipment from GCommerce's control during the period under scope and validated their response.	No exceptions noted. Control was properly designed but no tests over its operating effectiveness were performed as there were no disposals, re-use or release of equipment from GCommerce's control during the period under scope.
CC6.5.2	GCommerce reviews third-party vendor SOC2 reports on an annual basis.	Inspected the Third Party Risk Management section of the ISP to ascertain vendors are to be risk rated based on established criteria and the frequency of vendor risk assessments is outlined.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.5.2	(continued)	Obtained a listing of key vendors and subservice organizations and inspected evidence an annual vendor risk analysis had been performed in accordance with the Third Party Risk Management policy, for a sample of vendors and subservice organizations.	(continued)
CC6.5.3	Security analysts monitor security logs to identify and respond to potential threats.	Inspected the ISP to ascertain information systems are monitored and procedures are in place for identifying, assessing, and resolving security alerts. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely. Inspected example anti-malware rules and alert configurations to verify alerts are generated when predefined criteria are exceeded and appropriate individuals receive the notifications for research and resolution.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.5.4	Systems are patched to ensure security vulnerabilities are remediated.	Inspected the ISP to ascertain system patches and updates are to be obtained and deployed in a timely manner. Inspected system settings to ascertain they were configured to automatically download and deploy Microsoft operating system updates to workstations. Obtained the critical asset inventory listing and inspected system evidence of operating system details on a sample of servers and workstations to verify the devices were current on updates to the operating system.	No exceptions noted.
CC6.5.5	The Change Management process and IT Risk Management Program address security impacts during the system lifecycle.	Inspected the Product Life Cycle Process and the IT Risk Management Program to ascertain they address security analysis and impacts of systems throughout their lifecycle. Obtained a listing of application and infrastructure changes and inspected system evidence within DevOps of a security risk assessment and security testing on a sample of changes prior to being implemented.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.5.6	Anti-malware software automatically checks for updates and updates software daily.	Inspected the ISP to ascertain that all information systems are to have anti-virus and anti-malware solutions deployed with the most current version available from the vendor, enabled for automatic updates and configured for conducting periodic scans, as necessary. Inspected system settings on anti-malware software to ascertain the software performs daily updates.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.6.1	GCommerce requires encryption for sensitive data sent over a public network when connecting GCommerce resources.	Inspected the encryption certificate for the Commerce Bridge and a sample of other applications used for business processing, noting the certificates were valid and trusted and were issued by a reputable certificate management company. Observed the use of an HTTPS connection for the Commerce Bridge.	No exceptions noted.
CC6.6.2	GCommerce requires VPN access for remote users and requires users to follow the Remote Work Policy and BYOD Policy for access outside of the Company network.	Inspected the Remote Work Policy and BYOD policy, within the Acceptable Use Policy, to ascertain a VPN is required to gain remote access to the Company network and cloud applications. Observed an employee access the network and cloud applications remotely, which required VPN access. Inspected the security group rule established that requires remote users to VPN into the home office before gaining access to Company systems.	No exceptions noted.
CC6.6.3	GCommerce provides separate guest wireless access within the Company network.	Observed the use of separate wireless networks onsite, noting the corporate and guest networks were password protected.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.6.4	GCommerce has wireless policies and procedures in place for granting/restricting access and the required authentication methods.	Inspected the ISP to ascertain the requirements in place for granting and authenticating access to wireless networks.	No exceptions noted.
CC6.6.5	Firewalls are used to segment systems and data into security zones.	Inspected the Firewall Configuration Policy, within the ISP, to ascertain the requirements for the use of firewalls to segment systems and data into security zones. Inspected the data flow/process diagram to verify firewalls are located between the Internet and internal systems and servers, as appropriate.	No exceptions noted.
CC6.6.6	GCommerce utilizes anti-malware software and monitoring services to detect malicious network traffic and Pratum SIEM collects logs from infrastructure devices to identify security incidents.	Inspected the ISP to ascertain information systems are monitored and procedures are in place for identifying, assessing, and resolving security alerts. Obtained the critical asset inventory listing and verified endpoint anti-malware software has been installed on a sample of servers and workstations, enabled for automatic updates and configured for conducting periodic scans, as necessary.	No exceptions noted. 4 servers (out of 17 devices) did not have anti-malware software installed. LWBJ selected an additional 9 servers, noting no exceptions.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.6.6	(continued)	Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely.	No exceptions noted.
CC6.6.7	Firewall configurations are reviewed on an annual basis.	Inspected the ISP to ascertain the frequency and procedures in place for the review of firewall configurations. Inspected evidence that firewall configurations and security groups were reviewed annually.	No exceptions noted.
CC6.6.8	The SIEM collects event logs from network infrastructure devices to identify security incidents.	Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely. Obtained a listing of SIEM devices being monitored and compared the detail to the inventory of critical IT assets to determine critical components of the system were subject to monitoring.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.6.9	GCommerce has a mobile devices policy and procedures in place for granting/restricting access and the required authentication methods.	Inspected the ISP and Acceptable Use Policy to ascertain the requirements in place for granting and authenticating access from mobile devices, including laptops and personal devices.	No exceptions noted.
CC6.6.10	GCommerce uses SIEM to track malicious or inappropriate traffic within the network to a specific IP address.	Inspected the ISP to ascertain information systems are monitored and procedures are in place for identifying, assessing, and resolving security alerts. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely. Obtained a listing of SIEM devices being monitored and compared the detail to the inventory of critical IT assets to determine critical components of the system were subject to monitoring.	No exceptions noted.
CC6.6.11	Servers and workstations are required to have endpoint anti-malware tools installed.	Inspected the ISP to ascertain that all information systems are to have anti-virus and anti-malware solutions deployed with the most current version available from the vendor, enabled for automatic updates and configured for conducting periodic scans, as necessary.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.6.11	(continued)	Obtained the critical asset inventory listing and verified endpoint anti-malware software has been installed on a sample of servers and workstations, enabled for automatic updates and configured for conducting periodic scans, as necessary.	4 servers (out of 17 devices) did not have anti-malware software installed. LWBJ selected an additional 9 servers, noting no exceptions.
CC6.6.12	Systems are patched to ensure security vulnerabilities are remediated.	Inspected the ISP to ascertain system patches and updates are to be obtained and deployed in a timely manner. Inspected system settings to ascertain they were configured to automatically download and deploy Microsoft operating system updates to workstations. Obtained the critical asset inventory listing and inspected system evidence of operating system details on a sample of servers and workstations to verify the devices were current on updates to the operating system.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.6.13	The Change Management process and IT Risk Management Program address security impacts during the system lifecycle.	Inspected the Product Life Cycle Process and the IT Risk Management Program to ascertain they address security analysis and impacts of systems throughout their lifecycle. Obtained a listing of application and infrastructure changes and inspected system evidence within DevOps of a security risk assessment and security testing on a sample of changes prior to being implemented.	No exceptions noted.
CC6.6.14	Anti-malware software automatically checks for updates and updates software daily.	Inspected the ISP to ascertain that all information systems are to have anti-virus and anti-malware solutions deployed with the most current version available from the vendor, enabled for automatic updates and configured for conducting periodic scans, as necessary. Inspected system settings on anti-malware software to ascertain the software performs daily updates.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.6.15	The SIEM is configured to collect logs of Windows, network infrastructure, and firewall security events. Real-time alerts/tickets are generated to members of the IT department for research and resolution when pre-determined thresholds are met.	Inspected the ISP to ascertain information systems are monitored and procedures are in place for identifying, assessing, and resolving security alerts. Inspected the SIEM device listing and verified critical system components are being monitored. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely.	No exceptions noted.
CC6.6.16	Alerts are generated to the IT department when malicious software is detected on company-issued computers. All alerts are reviewed and resolved.	Inspected example alert rules from Cisco Endpoint Secure and Malwarebytes Cloud and alert configurations to verify alerts are generated when malicious activity is detected and appropriate individuals receive the notifications for research and resolution.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.7.1	GCommerce requires encryption on all sensitive data.	Inspected the ISP to ascertain the requirements for encryption on all sensitive data. Inspected the encryption certificate for the Commerce Bridge, noting the certificate was valid and trusted and was issued by a reputable certificate management company. Inspected system evidence of the encryption settings for the production databases and virtual machines, as applicable, to verify storage devices were encrypted at rest.	No exceptions noted.
CC6.7.2	GCommerce uses SIEM to track malicious or inappropriate traffic within the network to a specific IP address.	Inspected the ISP to ascertain information systems are monitored and procedures are in place for identifying, assessing, and resolving security alerts. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely. Obtained a listing of SIEM devices being monitored and compared the detail to the inventory of critical IT assets to determine critical components of the system were subject to monitoring.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.7.3	GCommerce limits the use of portable storage devices.	Inspected the ISP to ascertain the use of portable storage devices is limited and requires management approval. Inspected system settings to verify that devices with the ability to use portable storage devices is strictly limited.	No exceptions noted.
CC6.7.4	GCommerce has firewalls and switches in place to monitor and block unauthorized traffic.	Inspected the data flow/process diagram to ascertain the use of firewalls and switches in place to monitor and block unauthorized traffic. Inspected the ACLs configured on the firewall to ascertain rules are established to block unauthorized traffic.	No exceptions noted.
CC6.7.5	GCommerce has configured BIOS to disable the use of USB ports for removable storage devices.	Inspected the ISP to ascertain the use of USB devices is strictly prohibited. Inspected domain system settings to verify USB ports are disabled.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.7.6	Systems are patched to ensure security vulnerabilities are remediated.	Inspected the ISP to ascertain system patches and updates are to be obtained and deployed in a timely manner. Inspected system settings to ascertain they were configured to automatically download and deploy Microsoft operating system updates to workstations. Obtained the critical asset inventory listing and inspected system evidence of operating system details on a sample of servers and workstations to verify the devices were current on updates to the operating system.	No exceptions noted.
CC6.7.7	The SIEM is configured to collect logs of Windows, network infrastructure, and firewall security events. Real-time alerts/tickets are generated to members of the IT department for research and resolution when pre-determined thresholds are met.	Inspected the ISP to ascertain information systems are monitored and procedures are in place for identifying, assessing, and resolving security alerts. Inspected the SIEM device listing and verified critical system components are being monitored. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.7.8	Alerts are generated to the IT department when malicious software is detected on company-issued computers. All alerts are reviewed and resolved.	Inspected example alert rules from Cisco Endpoint Secure and Malwarebytes Cloud and alert configurations to verify alerts are generated when malicious activity is detected and appropriate individuals receive the notifications for research and resolution.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.8.1	Servers and workstations are required to have endpoint anti-malware tools installed.	Inspected the ISP to ascertain that all information systems are to have anti-virus and anti-malware solutions deployed with the most current version available from the vendor, enabled for automatic updates and configured for conducting periodic scans, as necessary. Obtained the critical asset inventory listing and verified endpoint anti-malware software has been installed on a sample of servers and workstations, enabled for automatic updates and configured for conducting periodic scans, as necessary.	No exceptions noted. 4 servers (out of 17 devices) did not have anti-malware software installed. LWBJ selected an additional 9 servers, noting no exceptions.
CC6.8.2	GCommerce uses an asset management tool to document active production assets and uses an HR management tool to track assigned assets and their age.	Inspected the Nagios server listing and tested its completeness. Inspected the workstation listing from the HR management tool and tested its completeness.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.8.3	GCommerce has a Software Use Policy in place that is reviewed by all employees annually.	Reviewed the Software Use Policy, included in the Employee Handbook, to ascertain the employee responsibilities and expectations for software use. Obtained a list of all employees and inspected the signed acknowledgement of the Employee Handbook, which captures software use, for a sample of employees.	No exceptions noted.
CC6.8.4	Systems are patched to ensure security vulnerabilities are remediated.	Inspected the ISP to ascertain system patches and updates are to be obtained and deployed in a timely manner. Inspected system settings to ascertain they were configured to automatically download and deploy Microsoft operating system updates to workstations. Obtained the critical asset inventory listing and inspected system evidence of operating system details on a sample of servers and workstations to verify the devices were current on updates to the operating system.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.8.5	The Change Management process and IT Risk Management Program address security impacts during the system lifecycle.	Inspected the Product Life Cycle Process and the IT Risk Management Program to ascertain they address security analysis and impacts of systems throughout their lifecycle. Obtained a listing of application and infrastructure changes and inspected system evidence within DevOps of a security risk assessment and security testing on a sample of changes prior to being implemented.	No exceptions noted.
CC6.8.6	Anti-malware software automatically checks for updates and updates software daily.	Inspected the ISP to ascertain that all information systems are to have anti-virus and anti-malware solutions deployed with the most current version available from the vendor, enabled for automatic updates and configured for conducting periodic scans, as necessary. Inspected system settings on anti-malware software to ascertain the software performs daily updates.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.8.7	GCommerce utilizes anti-malware software and monitoring services to detect malicious network traffic and Pratum SIEM collects logs from infrastructure devices to identify security incidents.	Inspected the ISP to ascertain information systems are monitored and procedures are in place for identifying, assessing, and resolving security alerts. Obtained the critical asset inventory listing and verified endpoint anti-malware software has been installed on a sample of servers and workstations, enabled for automatic updates and configured for conducting periodic scans, as necessary. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely.	No exceptions noted. 4 servers (out of 17 devices) did not have anti-malware software installed. LWBJ selected an additional 9 servers, noting no exceptions. No exceptions noted
CC6.8.8	The SIEM collects event logs from network infrastructure devices to identify security incidents.	Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely. Obtained a listing of SIEM devices being monitored and compared the detail to the inventory of critical IT assets to determine critical components of the system were subject to monitoring.	No exceptions noted.

Common Criteria Related to Logical and Physical Access Controls (continued)

CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC6.8.9	GCommerce uses SIEM to track malicious or inappropriate traffic within the network to a specific IP address.	Inspected the ISP to ascertain information systems are monitored and procedures are in place for identifying, assessing, and resolving security alerts. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely. Obtained a listing of SIEM devices being monitored and compared the detail to the inventory of critical IT assets to determine critical components of the system were subject to monitoring.	No exceptions noted.

Common Criteria Related to System Operations

CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.1.1	The SIEM is configured to collect logs of Windows, network infrastructure, and firewall security events. Real-time alerts/tickets are generated to members of the IT department for research and resolution when pre-determined thresholds are met.	Inspected the ISP to ascertain information systems are monitored and procedures are in place for identifying, assessing, and resolving security alerts. Inspected the SIEM device listing and verified critical system components are being monitored. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely.	No exceptions noted.
CC7.1.2	Alerts are generated to the IT department when malicious software is detected on company-issued computers. All alerts are reviewed and resolved.	Inspected example alert rules from Cisco Endpoint Secure and Malwarebytes Cloud and alert configurations to verify alerts are generated when malicious activity is detected and appropriate individuals receive the notifications for research and resolution.	No exceptions noted.

Common Criteria Related to System Operations (continued)

CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.1.3	IT department creates tickets for high and critical events, who are responsible for researching and taking corrective action, as necessary.	Inspected the change ticket for a sample of high risk findings from the annual penetration test to verify the finding was remediated timely. Inspected the support ticket for example significant system issues, along with the 8D analysis, to verify a ticket was created to track significant issues through resolution.	No exceptions noted.
CC7.1.4	Vulnerability scans are performed on a periodic basis using a scan tool. The results are reviewed by management and findings are mitigated, where possible. Findings which cannot be remediated are accepted and approved by management based on an assessment of acceptable risks.	Reviewed the ISP to ascertain the requirement to conduct vulnerability scans periodically under the direction and review of management. Inspected the annual external penetration test results report, which included a vulnerability scan, and verified actionable steps were taken to remediate a sample of high risk findings.	No exceptions noted.
CC7.1.5	Firewall configurations are reviewed on an annual basis.	Inspected the ISP to ascertain the frequency and procedures in place for the review of firewall configurations. Inspected evidence that firewall configurations and security groups were reviewed annually.	No exceptions noted.

Common Criteria Related to System Operations (continued)

CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.1.6	GCommerce utilizes anti-malware software and monitoring services to detect malicious network traffic and Pratum SIEM collects logs from infrastructure devices to identify security incidents.	Inspected the ISP to ascertain information systems are monitored and procedures are in place for identifying, assessing, and resolving security alerts. Obtained the critical asset inventory listing and verified endpoint anti-malware software has been installed on a sample of servers and workstations, enabled for automatic updates and configured for conducting periodic scans, as necessary. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely.	No exceptions noted. 4 servers (out of 17 devices) did not have anti-malware software installed. LWBJ selected an additional 9 servers, noting no exceptions. No exceptions noted
CC7.1.7	The SIEM collects event logs from network infrastructure devices to identify security incidents.	Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely. Obtained a listing of SIEM devices being monitored and compared the detail to the inventory of critical IT assets to determine critical components of the system were subject to monitoring.	No exceptions noted.

Common Criteria Related to System Operations (continued)

CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.1.8	GCommerce uses SIEM to track malicious or inappropriate traffic within the network to a specific IP address.	Inspected the ISP to ascertain information systems are monitored and procedures are in place for identifying, assessing, and resolving security alerts. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely. Obtained a listing of SIEM devices being monitored and compared the detail to the inventory of critical IT assets to determine critical components of the system were subject to monitoring.	No exceptions noted.
CC7.1.9	Servers and workstations are required to have endpoint anti-malware tools installed.	Inspected the ISP to ascertain that all information systems are to have the most current version of anti-virus and anti-malware solutions deployed, enabled for automatic updates and configured for conducting periodic scans, as necessary. Obtained the critical asset inventory listing and verified endpoint anti-malware software has been installed on a sample of servers and workstations, enabled for automatic updates and configured for conducting periodic scans, as necessary.	No exceptions noted. 4 servers (out of 17 devices) did not have anti-malware software installed. LWBJ selected an additional 9 servers, noting no exceptions.

Common Criteria Related to System Operations (continued)

CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.2.1	GCommerce's storage is backed up across multiple availability zones to ensure availability.	Inspected the ISP to ascertain the frequency of data backup required and standards for utilizing multiple availability zones. Inspected system evidence of backup configurations to ascertain backups are replicated to multiple locations, including Azure, to ensure availability.	No exceptions noted.
CC7.2.2	The SIEM is configured to continuously detect the addition of unauthorized components/devices into the System. Any attempt to insert or install a component/ device sends an alert to the IT department for research and resolution.	Inspected the SIEM device listing and verified all critical system components are being monitored. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely. Inspected the SIEM configuration rule/ alert listing to ascertain the settings to continuously detect the addition of unauthorized components/devices into the System.	No exceptions noted.

Common Criteria Related to System Operations (continued)

CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.2.3	Security events and anomalies are investigated and responded to timely.	Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely. Inspected example anti-malware rules and alert configurations to verify alerts are generated when predefined criteria are exceeded and appropriate individuals receive the notifications for research and resolution.	No exceptions noted.

Common Criteria Related to System Operations (continued)

CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.3.1	GCommerce's Incident Response Plan is utilized to escalate, respond to, and resolve suspected security incidents in a timely manner.	Inspected the Incident Response Plan to ascertain it addressed the definition of an incident, the responsible parties, and response plans over identified incidents. Inquired of management, who stated there were no security incidents identified or reported during the period under scope, and validated their response.	No exceptions noted. Control was properly designed but no tests over its operating effectiveness were performed as no incidents occurred during the period under scope.
CC7.3.2	The Company has implemented a Business Continuity & Disaster Recovery (BC/DR) Plan to address potential impairments to the Company's operations.	Inspected the BC/DR Plan to ascertain it addressed potential impairments to the Company's operations and outlined recovery procedures.	No exceptions noted.

Common Criteria Related to System Operations (continued)

CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.3.3	GCommerce tests aspects of the BC/DR Plan and Incident Response Plan using tabletop exercises at least semi-annually.	Inspected the BC/DR Plan and Incident Response Plan to ascertain they include a schedule for annual testing. Inspected a sample of the semi-annual tests of the BC/DR Plan, including the technical procedures performed, results, and actionable items. Inspected a sample of the semi-annual tests of the Incident Response Plan, including the test scenario, procedures performed, and results.	No exceptions noted.
CC7.3.4	GCommerce has an IT Risk Management Program in place to identify and evaluate risks and specify risk tolerance levels.	Inspected the IT Risk Management Program to ascertain it detailed the scope, risk management components and procedures in place for identification, analysis, review, and monitoring of risks. Inspected the annual risk assessment executive report, noting it was comprehensive, identified and assessed risks within the System, and summarized risks to remediate. Inspected the risk register to verify risks have project plans in place to further remediate the risk and are actively tracked by management.	No exceptions noted.

Common Criteria Related to System Operations (continued)

CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.3.5	GCommerce's BC/DR Plan and Incident Response Plan details steps to analyze events, restore systems to functional operations, implement changes, and prevention/detection of to avoid future occurrences.	Inspected the BC/DR and Incident Response Plans to ascertain procedures required including steps to analyze events, restore systems to functional operations, implement changes, and measures to prevent/detect future occurrences. Inquired of management, who stated there were no security incidents identified or reported during the period under scope, and validated their response.	No exceptions noted. Control was properly designed but no tests over its operating effectiveness were performed as no incidents occurred during the period under scope.

Common Criteria Related to System Operations (continued)

CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.3.6	GCommerce communicates security incidents to internal and external users with details of the incident, actions taken, and activities required to prevent future security incidents.	Inspected the Incident Response Plan to ascertain it addressed the definition of an incident, response plans, and required communication for identified incidents. Inquired of management, who stated there were no security incidents identified or reported during the period under scope, and validated their response.	No exceptions noted. Control was properly designed but no tests over its operating effectiveness were performed as no incidents occurred during the period under scope.

Common Criteria Related to System Operations (continued)

CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.4.1	GCommerce has an IT Risk Management Program in place to identify and evaluate risks and specify risk tolerance levels.	Inspected the IT Risk Management Program to ascertain it detailed the scope, risk management components and procedures in place for identification, analysis, review, and monitoring of risks. Inspected the annual risk assessment executive report, noting it was comprehensive, identified and assessed risks within the System, and summarized risks to remediate. Inspected the risk register to verify risks have project plans in place to further remediate the risk and are actively tracked by management.	No exceptions noted.
CC7.4.2	GCommerce's Incident Response Plan is utilized to escalate, respond to, and resolve suspected security incidents in a timely manner.	Inspected the Incident Response Plan to ascertain it addressed the definition of an incident, the responsible parties, and response plans over identified incidents. Inquired of management, who stated there were no security incidents identified or reported during the period under scope, and validated their response.	No exceptions noted. Control was properly designed but no tests over its operating effectiveness were performed as no incidents occurred during the period under scope.

Common Criteria Related to System Operations (continued)

CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.4.3	GCommerce tests aspects of the BC/DR Plan and Incident Response Plan using tabletop exercises at least semi-annually.	Inspected the BC/DR Plan and Incident Response Plan to ascertain they include a schedule for annual testing. Inspected a sample of the semi-annual tests of the BC/DR Plan, including the technical procedures performed, results, and actionable items. Inspected a sample of the semi-annual tests of the Incident Response Plan, including the test scenario, procedures performed, and results.	No exceptions noted.
CC7.4.4	GCommerce utilizes anti-malware software and monitoring services to detect malicious network traffic and Pratum SIEM collects logs from infrastructure devices to identify security incidents.	Inspected the ISP to ascertain information systems are monitored and procedures are in place for identifying, assessing, and resolving security alerts. Obtained the critical asset inventory listing and verified endpoint anti-malware software has been installed on a sample of servers and workstations, enabled for automatic updates and configured for conducting periodic scans, as necessary. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely.	No exceptions noted. 4 servers (out of 17 devices) did not have anti-malware software installed. LWBJ selected an additional 9 servers, noting no exceptions. No exceptions noted

Common Criteria Related to System Operations (continued)

CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.4.5	The SIEM collects event logs from network infrastructure devices to identify security incidents.	Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely. Obtained a listing of SIEM devices being monitored and compared the detail to the inventory of critical IT assets to determine critical components of the system were subject to monitoring.	No exceptions noted.
CC7.4.6	GCommerce uses SIEM to track malicious or inappropriate traffic within the network to a specific IP address.	Inspected the ISP to ascertain information systems are monitored and procedures are in place for identifying, assessing, and resolving security alerts. Obtained a listing of all SIEM monitoring alerts and, for a sample of alerts, inspected the support ticket to verify the alert was resolved appropriately and timely. Obtained a listing of SIEM devices being monitored and compared the detail to the inventory of critical IT assets to determine critical components of the system were subject to monitoring.	No exceptions noted.

Common Criteria Related to System Operations (continued)

CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.4.7	Servers and workstations are required to have endpoint anti-malware tools installed.	Inspected the ISP to ascertain that all information systems are to have anti-virus and anti-malware solutions deployed with the most current version available from the vendor, enabled for automatic updates and configured for conducting periodic scans, as necessary. Obtained the critical asset inventory listing and verified endpoint anti-malware software has been installed on a sample of servers and workstations, enabled for automatic updates and configured for conducting periodic scans, as necessary.	No exceptions noted. 4 servers (out of 17 devices) did not have anti-malware software installed. LWBJ selected an additional 9 servers, noting no exceptions.
CC7.4.8	GCommerce's BC/DR Plan and Incident Response Plan details steps to analyze events, restore systems to functional operations, implement changes, and prevention/detection of to avoid future occurrences.	Inspected the BC/DR and Incident Response Plans to ascertain procedures required including steps to analyze events, restore systems to functional operations, implement changes, and measures to prevent/detect future occurrences.	No exceptions noted.

Common Criteria Related to System Operations (continued)

CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.4.8	(continued)	Inquired of management, who stated there were no security incidents identified or reported during the period under scope, and validated their response.	Control was properly designed but no tests over its operating effectiveness were performed as no incidents occurred during the period under scope.
CC7.4.9	GCommerce communicates security incidents to internal and external users with details of the incident, actions taken, and activities required to prevent future security incidents.	Inspected the Incident Response Plan to ascertain it addressed the definition of an incident, response plans, and required communication for identified incidents. Inquired of management, who stated there were no security incidents identified or reported during the period under scope, and validated their response.	No exceptions noted. Control was properly designed but no tests over its operating effectiveness were performed as no incidents occurred during the period under scope.

Common Criteria Related to System Operations (continued)

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.5.1	GCommerce's BC/DR Plan and Incident Response Plan details steps to analyze events, restore systems to functional operations, implement changes, and prevention/detection of to avoid future occurrences.	Inspected the BC/DR and Incident Response Plans to ascertain procedures required including steps to analyze events, restore systems to functional operations, implement changes, and measures to prevent/detect future occurrences. Inquired of management, who stated there were no security incidents identified or reported during the period under scope, and validated their response.	No exceptions noted. Control was properly designed but no tests over its operating effectiveness were performed as no incidents occurred during the period under scope.
CC7.5.2	GCommerce communicates security incidents to internal and external users with details of the incident, actions taken, and activities required to prevent future security incidents.	Inspected the Incident Response Plan to ascertain it addressed the definition of an incident, response plans, and required communication for identified incidents. Inquired of management, who stated there were no security incidents identified or reported during the period under scope, and validated their response.	No exceptions noted. Control was properly designed but no tests over its operating effectiveness were performed as no incidents occurred during the period under scope.

Common Criteria Related to System Operations (continued)

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.5.3	GCommerce's Incident Response Plan is utilized to escalate, respond to, and resolve suspected security incidents in a timely manner.	Inspected the Incident Response Plan to ascertain it addressed the definition of an incident, the responsible parties, and response plans over identified incidents. Inquired of management, who stated there were no security incidents identified or reported during the period under scope, and validated their response.	No exceptions noted. Control was properly designed but no tests over its operating effectiveness were performed as no incidents occurred during the period under scope.
CC7.5.4	The Company has implemented a Business Continuity & Disaster Recovery (BC/DR) Plan to address potential impairments to the Company's operations.	Inspected the BC/DR Plan to ascertain it addressed potential impairments to the Company's operations and outlined recovery procedures.	No exceptions noted.
CC7.5.5	GCommerce tests aspects of the BC/DR Plan and Incident Response Plan using tabletop exercises at least semi-annually.	Inspected the BC/DR Plan and Incident Response Plan to ascertain they include a schedule for annual testing. Inspected a sample of the semi-annual tests of the BC/DR Plan, including the technical procedures performed, results, and actionable items.	No exceptions noted.

Common Criteria Related to System Operations (continued)

CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC7.5.5	(continued)	Inspected a sample of the semi-annual tests of the Incident Response Plan, including the test scenario, procedures performed, and results.	(continued)
CC7.5.6	GCommerce has an IT Risk Management Program in place to identify and evaluate risks and specify risk tolerance levels.	Inspected the IT Risk Management Program to ascertain it detailed the scope, risk management components and procedures in place for identification, analysis, review, and monitoring of risks. Inspected the annual risk assessment executive report, noting it was comprehensive, identified and assessed risks within the System, and summarized risks to remediate. Inspected the risk register to verify risks have project plans in place to further remediate the risk and are actively tracked by management.	No exceptions noted.
CC7.5.7	GCommerce has a formal IT Risk Management Policy to identify, assess, prioritize, and mitigate risks based on the likelihood and impact of the potential threats/risks, which is reviewed at least annually.	Inspected the IT Risk Management Policy to ascertain the requirements to identify, assess, prioritize and mitigate risks based on the likelihood and impact of potential threats/risks.	No exceptions noted.

Common Criteria Related to Change Management

CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC8.1.1	Changes considered in scope are requested, reviewed, approved and tracked via the Change Management Standard.	Reviewed the Change Management Standard, within the ISP, to ascertain requirements for tracking procedures for the request, review and approval of changes to infrastructure and applications. Obtained a listing of all changes to infrastructure and applications and inspected the change tickets for a sample of changes to verify the change was requested, reviewed, approved, tested, and tracked according to the Change Management Standard.	No exceptions noted.
CC8.1.2	Testing is performed on all significant changes prior to release to production.	Inspected the Change Management Standard to ascertain the testing procedures required on significant system and application changes. Obtained a listing of all infrastructure and application changes and inspected the change ticket details for a sample of system changes to verify the change was tested, including peer code reviews and user acceptance, within the change management system. Inspected the network diagram, device listing, and change management system to verify that separate environments have been established for development, staging, and production usage.	No exceptions noted.

Common Criteria Related to Change Management (continued)

CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC8.1.3	Segregation of duties is enforced for the deployment of code to production.	Inspected the Change Management Standard to ascertain it detailed procedures to support the segregation of duties. Obtained a list of all infrastructure and application changes and inspected the ticket details for a sample of system changes to verify segregation of duties was enforced in accordance with the Change Management Standard.	No exceptions noted.
CC8.1.4	Appropriate approval is required for in-scope changes according to the Change Management Standard.	Inspected the Change Management Standard to ascertain the approval requirements for significant system and application changes. Obtained a listing of all infrastructure and application changes and inspected the ticket details for a sample of system changes to verify the change was requested, reviewed and approved in accordance with the Change Management Standard.	No exceptions noted.
CC8.1.5	Changes to scheduled jobs require management approval and follow the change management procedures.	Inspected the Product Round Table (PRT) Process to ascertain the procedures required for processing changes to scheduled jobs which include management approval.	No exceptions noted.

Common Criteria Related to Change Management (continued)

CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC8.1.5	(continued)	Obtained a system log of all changes to scheduled jobs and inspected the change ticket details to verify the approval of management was obtained for a sample of changes to scheduled jobs.	(continued)
CC8.1.6	GCommerce follows a formal bug process to remediate flaws identified during and after testing.	Inspected the Change Management Standard to ascertain the agile process for significant system and application changes, which includes flaws and system bugs. Obtained a listing of all infrastructure and application changes and inspected the ticket details for a sample of system changes to verify flaws and bugs were identified, reviewed, tested and approved in accordance with the Change Management Standard, as applicable.	No exceptions noted.
CC8.1.7	Systems are patched to ensure security vulnerabilities are remediated.	Inspected the ISP to ascertain system patches and updates are to be obtained and deployed in a timely manner. Inspected system settings to ascertain they were configured to automatically download and deploy Microsoft operating system updates to workstations.	No exceptions noted.

Common Criteria Related to Change Management (continued)

CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC8.1.7	(continued)	Obtained the critical asset inventory listing and inspected system evidence of operating system details on a sample of servers and workstations to verify the devices were current on updates to the operating system.	(continued)
CC8.1.8	Changes to scheduled jobs require management approval and follow the change management procedures.	Inspected the Product Round Table (PRT) Process to ascertain the procedures required for processing changes to scheduled jobs which include management approval. Obtained a system log of all changes to scheduled jobs and inspected the change ticket details to verify the approval of management was obtained for a sample of changes to scheduled jobs.	No exceptions noted.
CC8.1.9	GCommerce performs a risk assessment annually based on objectives incorporated from service commitments and system requirements.	Inspected the IT Risk Management Program to ascertain the procedures for an annual risk assessment and continual development of a risk register. Inspected the annual risk assessment executive report, noting it was comprehensive, identified and assessed risks within the System, and summarized risks to remediate.	No exceptions noted.

Common Criteria Related to Change Management (continued)

CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC8.1.10	GCommerce's risk register is developed and maintained to continually update risks and controls.	Inspected the IT Risk Management Program to ascertain the procedures for an annual risk assessment and continual development of a risk register. Inspected the current risk register, noting risks are identified, tracked, and addressed, as deemed appropriate and had been updated recently.	No exceptions noted.
CC8.1.11	Changes to technical environments are assessed for new risks to the GCommerce Bridge before they are implemented.	Inspected the PRT Process to ascertain that changes to technical environments are subject to a risk assessment prior to implementation. Obtained a listing of infrastructure changes and inspected the PRT risk assessment performed prior to project acceptance for a sample of changes.	No exceptions noted.
CC8.1.12	The Change Management process and IT Risk Management Program address security impacts during the system lifecycle.	Inspected the Product Life Cycle Process and the IT Risk Management Program to ascertain they address security analysis and impacts of systems throughout their lifecycle. Obtained a listing of application and infrastructure changes and inspected system evidence within DevOps of a security risk assessment and security testing on a sample of changes prior to being implemented.	No exceptions noted.

Common Criteria Related to Risk Mitigation

CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC9.1.1	GCommerce has a formal IT Risk Management Policy to identify, assess, prioritize, and mitigate risks based on the likelihood and impact of the potential threats/risks, which is reviewed at least annually.	Inspected the IT Risk Management Policy to ascertain the requirements to identify, assess, prioritize and mitigate risks based on the likelihood and impact of potential threats/risks.	No exceptions noted.
CC9.1.2	GCommerce has purchased insurance policies including cybersecurity insurance, to offset the financial impact of business interruptions.	Inspected the cybersecurity insurance policy for the Company, noting the policy was in place throughout the scope period to offset financial impact of business interruptions.	No exceptions noted.

Common Criteria Related to Risk Mitigation (continued)

CC9.2: The entity assesses and manages risks associated with vendors and business partners.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC9.2.1	GCommerce has a formal IT Risk Management Policy to identify, assess, prioritize, and mitigate risks based on the likelihood and impact of the potential threats/risks of the third-party service organizations and is reviewed annually by management.	Reviewed the IT Risk Management Policy to ascertain the requirements to identify, assess, prioritize and mitigate risks based on the likelihood and impact of the potential threats/risks. Obtained a listing of key vendors and subservice organizations and inspected evidence an annual vendor risk analysis had been performed in accordance with the Third Party Risk Management policy, for a sample of vendors and subservice organizations.	No exceptions noted.
CC9.2.2	The vendor (and/or business partner) selection process includes a review of materials, including information security questionnaires, SOC reports, and other certifications of the vendor (and/or business partner), to ensure the risks associated with the vendor (and/or business partner) are understood.	Inspected the Third Party Risk Management section of the ISP to ascertain it detailed due diligence factors for vendor acceptance. Inquired of management of any new vendors, who stated there were none and validated the response.	No exceptions noted. Control was properly designed but no tests over its operating effectiveness were performed as there were no new vendors during the period under scope.

Common Criteria Related to Risk Mitigation (continued)

CC9.2: The entity assesses and manages risks associated with vendors and business partners. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
CC9.2.3	Service agreements are executed between GCommerce and key vendors and/or subservice organizations to ensure security responsibilities are defined for both parties and must include non-disclosure/ confidentiality clauses.	Obtained a listing of key vendors and subservice organizations and inspected the signed service agreement or similar evidence for a sample of vendors and subservice organizations.	No exceptions noted.
CC9.2.4	The Vendor Management Policy defines expectations for identifying and risk rating all vendor relationships.	Inspected the Third Party Risk Management section of the ISP to ascertain it established the criteria to risk rate vendors and detailed the vendor risk assessment review procedures.	No exceptions noted.

Additional Criteria for Processing Integrity

PI1.1: The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
PI1.1.1	GCommerce provides the data mapping, onboarding, training, testing and support needed to connect any two trading partners, regardless of their technology platform, data format or communication protocol.	Reviewed the contract templates, new user implementation guide and user manuals to ascertain the support provided by GCommerce to connect trading partners using a standardized data mapping process. Inspected the Company's product workflow diagrams to ascertain standardized onboarding, testing, and support is provided to new customers. Obtained a listing of new customers and obtained the contracts for a sample of customers to ascertain the commitments for GCommerce to provide data mapping, onboarding, training, testing and support and evidence that GCommerce connected the customer to its trading partners using the EDI Super Spec during the onboarding process.	No exceptions noted.
PI1.1.2	GCommerce provides an EDI Super Spec to help simplify data mapping, which includes complete data definitions and descriptions for the trading partners.	Reviewed the contract templates, the new user implementation guide and user manuals to ascertain the support provided by GCommerce to connect trading partners using an EDI Super Spec. Reviewed the EDI Super Spec documents developed and maintained by GCommerce in close cooperation with the Automotive Aftermarket Industry Association.	No exceptions noted.

Additional Criteria for Processing Integrity (continued)

PI1.1: The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
PI1.1.2	(continued)	Obtained a listing of new customers and obtained evidence that GCommerce provided the EDI Super Spec documents to the customer and connected the customer to its trading partners using the EDI Super Spec during the onboarding process.	(continued)

Additional Criteria for Processing Integrity (continued)

PI1.2: The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
PI1.2.1	System inputs are measured and recorded completely, accurately, and timely to meet the Company's processing integrity commitments and system requirements.	Reviewed the Nagios dashboards reviewed by IT personnel to monitor, alert and report on all systems. Metrics monitored include Availability, Uptime, CPU/MEM/network/disk utilization and rate, IIS metrics, and system logs for supported systems which are consistent with metrics identified in processing integrity commitments. Obtained the Non-Delivered/Tracking Errors Report for a selection of days and for a sample of processing errors, which included input errors, inspected evidence that the error was resolved timely to ensure inputs are being recorded completely, accurately, and timely.	No exceptions noted.
PI1.2.2	GCommerce provides internal Commerce Bridge application users the ability to manually resubmit files.	Reviewed instructions for resubmitting files verifying only an internal user has the responsibility and ability to manually perform the task. Inspected the Commerce Bridge user listing to ascertain the ability to manually resubmit files is limited to internal users and verified access was approved for a sample of new employees and access was removed for a sample of terminated employees.	No exceptions noted.

Additional Criteria for Processing Integrity (continued)

PI1.2: The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
PI1.2.3	GCommerce ensures that input validation errors are reviewed and resolved.	Reviewed the ISP and related security documents to ascertain the procedures for oversight of validation errors, which includes a review of input validation errors, which the Company is alerted to in instances where files do not process. Obtained the Non-Delivered/Tracking Errors Report for a selection of days and for a sample of processing errors, which included input errors, inspected evidence that the error was resolved timely.	No exceptions noted.
PI1.2.4	GCommerce has prepared a data flow/ process diagram, detailing the sources of information, relevant systems utilized, and data processing points, to allow for the proper processing, and security, of client data.	Inspected the data flow/process diagram and verified it included details regarding the sources of information, relevant systems utilized, and data processing points.	No exceptions noted.

Additional Criteria for Processing Integrity (continued)

PI1.3: The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
PI1.3.1	GCommerce has procedures to prevent, or detect and correct, processing errors to meet the Company's processing integrity commitments and system requirements.	Reviewed the ISP and related security documents to ascertain the procedures to prevent, or detect and correct, processing errors. Obtained the Non-Delivered/Tracking Errors Report for a selection of days and for a sample of processing errors, inspected evidence that the error was resolved timely. Obtained a listing of new customers and obtained evidence that GCommerce connected the customer to its trading partners using the EDI Super Spec during the onboarding process; ensuring standardized data connections were properly established to ensure processing integrity commitments are met.	No exceptions noted.
PI1.3.2	Modification of data, other than routine transaction processing, is authorized and processed to meet with the Company's processing integrity commitments and system requirements.	Inspected the data flow/process map to confirm routine transaction processing cannot be modified without oversite and authorization. Inquired of management, who stated that the Company does not modify client data/transactions identified in the Tracking Errors Report; employees identify the root cause of the error and notify the customer how to resolve the error and resubmit the file.	No exceptions noted.

Additional Criteria for Processing Integrity (continued)

PI1.3: The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
PI1.3.2	(continued)	Obtained a listing of new customers and obtained evidence that GCommerce connected the customer to its trading partners using the EDI Super Spec during the onboarding process; ensuring standardized data connections are properly established to ensure processing integrity commitments are met.	(continued)
PI1.3.3	Error tracking is only available to Commerce Bridge application users.	Inspected the ISP to ascertain administrative rights are restricted to users based on job responsibilities. Inspected the Commerce Bridge user listing to ascertain the ability to manually resubmit files is limited to internal users and verified access was approved for a sample of new employees and access was removed for a sample of terminated employees.	No exceptions noted.

Additional Criteria for Processing Integrity (continued)

PI1.3: The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
PI1.3.4	System output is complete, accurate, distributed, and retained to meet the GCommerce's processing integrity commitments and system requirements.	Obtained the Non-Delivered/Tracking Errors Report for a selection of days and for a sample of processing errors, inspected evidence that the error was resolved timely to ensure system output was complete, accurate and distributed. Inspected example performance and system availability rules and alert configurations to verify alerts are generated when predefined criteria are exceeded and appropriate individuals receive the notifications for research and resolution.	No exceptions noted.

Additional Criteria for Processing Integrity (continued)

PI1.4: The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
PI1.4.1	System output is complete, accurate, distributed, and retained to meet the GCommerce's processing integrity commitments and system requirements.	Obtained the Non-Delivered/Tracking Errors Report for a selection of days and for a sample of processing errors, inspected evidence that the error was resolved timely to ensure system output was complete, accurate and distributed. Inspected example performance and system availability rules and alert configurations to verify alerts are generated when predefined criteria are exceeded and appropriate individuals receive the notifications for research and resolution.	No exceptions noted.
PI1.4.2	GCommerce validates output from systems to ensure that the information is consistent with expected content.	Obtained the Non-Delivered/Tracking Errors Report for a selection of days and for a sample of processing errors, inspected evidence that the error was resolved timely. Obtained a listing of new customers and obtained evidence that GCommerce connected the customer to its trading partners using the EDI Super Spec during the onboarding process; ensuring standardized data connections are properly established to ensure processing integrity commitments are met.	No exceptions noted.

Additional Criteria for Processing Integrity (continued)

PI1.4: The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives. (continued)

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
PI1.4.3	GCommerce has prepared a data flow/ process diagram, detailing the sources of information, relevant systems utilized, and data processing points, to allow for the proper processing, and security, of client data.	Inspected the data flow/process diagram and verified it included details regarding the sources of information, relevant systems utilized, data processing points, and output.	No exceptions noted.

Additional Criteria for Processing Integrity (continued)

PI1.5: The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.

Control Reference	Control Activity (Provided by GCommerce)	Procedures Performed by LWBJ	Results
PI1.5.1	Data is stored and maintained completely, accurately, and in a timely manner for its specified life span to meet the GCommerce's processing integrity commitments and system requirements.	Inspected the ISP to ascertain the Company's policy to meet data storage and retention requirements for legal, regulatory and business requirements. Inspected system evidence of backup configurations to verify the frequency of full and incremental backups of customer and Company data. For a sample of days, inspected evidence that unsuccessful backups were researched and resolved timely.	No exceptions noted.
PI1.5.2	GCommerce has data retention policy in place.	Inspected the data retention policy, included within the ISP, to ascertain the Company's policy to meet data storage and retention requirements for legal, regulatory and business requirements.	No exceptions noted.

Section 5:

Other Information Provided by GCommerce that is Not Covered by the Independent Service Auditors' Report

Other Information Provided by GCommerce that is Not Covered by the Independent Service Auditors' Report

Summary of Exceptions and Management's Response

Trust Services Criteria	Control Activity (Provided by GCommerce)	Exception Noted (Provided by LWBJ)	Management's Response (Provided by Gcommerce)
CC6.6, CC6.8, CC7.1, CC7.4	GCommerce utilizes anti-malware software and monitoring services to detect malicious network traffic and Pratum SIEM collects logs from infrastructure devices to identify security incidents.	4 servers (out of 17 devices) did not have anti-malware software installed. LWBJ selected an additional 9 servers, noting no exceptions.	GCommerce has an open project to continuously improve the security of our products and have been working diligently with our CISCO partners trying to obtain licensing prior to installation to servers without anti-malware software to stay in compliance.
CC6.6, CC6.8, CC7.1, CC7.4	Servers and workstations are required to have endpoint anti-malware tools installed.		

Table of NIST Information

The below table represents the cross referencing of NIST 800-53 Rev. 5. GCommerce has mapped controls that meet the NIST requirements under revision 5 but have stated controls that do not apply to GCommerce from this revision due to GCommerce not being a federal organization or a company managing federal data. As stated in the NIST 800-53 Rev 5 abstract, the mapped controls establish assurances that GCommerce adheres to Computer Security requirement controls for GCommerce's Commerce Bridge information systems and the Company. This is in place to protect the Company and its customers from a diverse set of threats including hostile cyber-attacks, natural disasters, structural failures, and human errors (both intentional and unintentional).

TSC Ref. #	NIST 800-53
CC1.1.1	PS-6a.
CC1.1.2	PS-6b.
CC1.1.3	PS-6c.
CC1.1.4	PS-6c.1. PS-6c.2.
CC1.3.2	PM-2
CC1.3.3	PM-10b.
CC1.3.4	PL-9
CC1.3.5	PM-3a. PM-3b. PM-3c.
CC1.4.2	SA-16
CC1.4.3	SI-4 (21)
CC1.4.4	PM-13
CC1.5.1	PS-8a.
CC1.5.2	PS-8b.
CC1.5.3	PS-8b.
CC1.5.4	PS-8b.
CC1.5.5	PS-8b.
CC2.2.1 CC2.2.2 CC2.2.3	PL-4a. PL-4b. PL-4c. PL-4d. PL-4 (1)
CC2.2.4 CC2.2.5 CC2.2.6	AT-2a. AT-2a.1. AT-2a.2. AT-2b. AT-2c. AT-2d.

TSC Ref. #	NIST 800-53
CC2.2.4 CC2.2.5 CC2.2.6	AT-2(1) AT-2(2) AT-2(3) AT-2(4) AT-2(5) AT-2(6)(a) AT-2(6)(b) AT-3a. AT-3a.1. AT-3a.2. AT-3b. AT-3c. AT-3 (1) AT-3 (2) AT-3 (3) AT-3(5) AT-4a. AT-4b.
CC2.3.2	AC-8c. AC-8c.1. AC-8c.2. AC-8c.3.
CC2.3.3	PM-15 PM-15a. PM-15b. PM-15c.
CC3.1.1	RA-2a. RA-2b. RA-2c. RA-2(1)

TSC Ref. #	NIST 800-53
CC3.1.2	PM-11a. PM-11b. PM-11c.
CC3.2.1	RA-1a RA-1a.1. RA-1a.1.a. RA-1a.1.b. RA-1a.2 RA-1b. RA-1c. RA-1c.1. RA-1c.2.
CC3.2.2	RA-3a. RA-3a.1 RA-3a.2 RA-3a.3 RA-3b. RA-3c. RA-3d. RA-3e. RA-3f. PM-9a. PM-9a.1 PM-9a.2 PM-9b. PM-9c. PM-10c. PM-16
CC4.1.1	CA-2a. CA-2b.

TSC Ref. #	NIST 800-53
CC4.1.1	CM-6 CM-6a. CM-6b. CM-6c. CM-6d. CM-6 (1) CM-7 CM-7a. CM-7b. CM-7 (1) CM-7 (1)(a) CM-7 (1)(b) CM-7 (2) CM-7 (3) CM-8 CM-8a. CM-8a.1. CM-8a.2. CM-8a.3. CM-8a.4. CM-8b. CM-8 (1) CM-8 (2) CM-8 (3) CM-8 (3)(a) CM-8 (3)(b) CM-8 (4)
CC4.1.2	CA-2 (3)
CC4.1.3 CC4.1.4	CA-7 CA-7a. CA-7b. CA-7c. CA-7d. CA-7e. CA-7f. CA-7g. CA-7(1) CA-7(3) CA-7(4) CA-7(5) CA-7(6) CA-8 CA-8 (1) CA-8 (2)

TSC Ref. #	NIST 800-53
CC4.1.3 CC4.1.4	CA-8(3) RA-6 SC-31a. SC-31b. SC-31 (1) SC-31 (2) SC-31 (3) PM-6 PM-14a. PM-14a.1. PM-14a.1. PM-14a.1.
CC4.2.1	CA-5a. CA-5b. CA-5 (1)
CC5.1.1	IA-5c. SI-14 SI-14 (1)
CC5.2.1 CC5.2.2 CC5.2.3	AC-1a. AC-1a.1 AC-1a.1.a AC-1a.1.b AC-1a.2. AC-1b. AC-1c. AC-1c.1. AC-1c.2. AT-1a. AT-1a.1. AT-1a.1.a AT-1a.1.b AT-1a.2. AT-1b. AT-1c. AT-1c.1. AT-1c.2. AU-1a. AU-1a.1. AU-1a.1.a. AU-1a.1.b. AU-1a.2. AU-1b. AU-1c AU-1c.1.

TSC Ref. #	NIST 800-53
CC5.2.1 CC5.2.2 CC5.2.3	AC-1c.2. AT-1a. AT-1a.1. AT-1a.1.a AT-1a.1.b AT-1a.2. AT-1b. AT-1c. AT-1c.1. AT-1c.2. AU-1a. AU-1a.1. AU-1a.1.a. AU-1a.1.b. AU-1a.2. AU-1b. AU-1c AU-1c.1. AU-1c.2. CA-1a. CA-1a.1. CA-1a.1.a CA-1a.1.b CA-1a.2. CA-1b. CA-1c. CA-1c.1. CA-1c.2. CM-1a. CM-1a.1. CM-1a.1.a CM-1a.1.b CM-1a.2. CM-1b. CM-1c. CM-1c.1. CM-1c.2. IA-1a. IA-1a.1. IA-1a.1.a IA-1a.1.b IA-1a.2. IA-1b. IA-1c.

TSC Ref. #	NIST 800-53				
CC5.2.1 CC5.2.2 CC5.2.3	IA-1c.1. IA-1c.2. IA-5g. IR-1a. IR-1a.1. IR-1a.1(a) IR-1a.1(b) IR-1a.2. IR-1b. IR-1c. IR-1c.1. IR-1c.2. MA-1a. MA-1a.1(a) MA-1a.1(b) MA-1a.2. MA-1b. MA-1c. MA-1c.1. MA-1c.2. MP-1a. MP-1a.1.	MP-1a.1(a) MP-1a.1(b) MP-1a.2. MP-1b. MP-1c. MP-1c.1. MP-1c.2. PE-1a. PE-1a.1. PE-1a.1(a) PE-1a.1(b) PE-1a.2. PE-1b. PE-1c. PE-1c.1. PE-1c.2. PL-1a. PL-1a.1. PL-1a.1.(a) PL-1a.1.(b) PL-1a.2. PL-1b.	PL-1c.1. PL-1c.2. PL-7a. PL-7b. PL-8a. PL-8a.1. PL-8a.2. PL-8a.3. PL-8a.4. PL-8b. PL-8c. PL-8(1) PL-8(1)(a) PL-8(1)(b) PL-8(2) PS-1a. PS-1a.1. PS-1a.1.(a) PS-1a.1.(b) PS-1a.2. PS-1b. PS-1c.	PS-1c.1. PS-1c.2. SA-1a. SA-1a.1. SA-1a.1.(a) SA-1a.1.(b) SA-1a.2. SA-1b. SA-1c. SA-1c.1. SA-1c.2. SC-1a. SC-1a.1. SC-1a.1.(a) SC-1a.1.(b) SC-1a.2. SC-1b. SC-1c. SC-1c.1. SC-1c.2. SI-1a. SI-1a.1.	SI-1a.1.(a) SI-1a.1.(b) SI-1a.2. SI-1b. SI-1c. SI-1c.1. SI-1c.2. PM-1a. PM-1a.1. PM-1a.2. PM-1a.3. PM-1a.4. PM-1b. PM-1c. PM-4a. PM-4a.1. PM-4a.2. PM-4a.3. PM-4b. PM-10a.
CC5.3.1	PL-2a. PL-2a.1. PL-2a.2. PL-2a.3.	PL-2a.4. PL-2a.5. PL-2a.6. PL-2a.7.	PL-2a.8. PL-2a.9. PL-2a.10. PL-2a.11.	PL-2a.12. PL-2a.13. PL-2a.14. PL-2a.15.	PL-2b. PL-2c. PL-2d. PL-2e.
CC6.1.1 CC6.1.2 CC6.1.3 CC6.1.4 CC6.1.5	AC-2a. AC-2b. AC-2c. AC-2d. AC-2 (1) AC-2 (2) AC-2 (3) AC-2 (5) AC-2 (6) AC-2 (7) AC-2 (8) AC-2 (9) AC-2 (11) AC-3 AC-3 (2) AC-3(3) AC-3(3)(a) AC-3(3)(b)	AC-3(3)(b)(1) AC-3(3)(b)(2) AC-3(3)(b)(3) AC-3(3)(b)(4) AC-3(3)(b)(5) AC-3(3)(c) AC-3(4) AC-3(4)(a) AC-3(4)(b) AC-3(4)(c) AC-3(4)(d) AC-3(4)(e) AC-3(5) AC-3(7) AC-3(8) AC-3(9) AC-3(9)(a) AC-3(9)(b)	AC-4(10) AC-4 (11) AC-5a. AC-5b. AC-6 AC-6 (4) AC-6 (8) AC-6 (10) AC-7a. AC-7b. AC-10 AC-11a. AC-11b. AC-11 (1) AC-12 AC-12 (1) AC-14a. AC-14b.	AC-16a. AC-16b. AC-16c. AC-16d. AC-16e. AC-16f. AC-16 (1) AC-16 (2) AC-16 (3) AC-16 (4) AC-16 (6) AC-16 (7) AC-16 (8) AC-16 (9) AC-16 (10) AC-21 (1) AC-21 (2) AC-23	AC-24 (1) AC-24 (2) AC-25 AU-5 (3) AU-5 (4) IA-2 IA-2 (1) IA-2 (2) IA-2 (5) IA-2 (6) IA-2 (6)(a) IA-2 (6)(b) IA-2 (8) IA-2 (10) IA-2 (12) IA-2 (13) IA-3 IA-3 (1)

TSC Ref. #	NIST 800-53				
CC6.1.1 CC6.1.2 CC6.1.3 CC6.1.4 CC6.1.5	IA-3 (3)(a) IA-3 (3)(b) IA-3 (4) IA-5e. IA-5f. IA-5g. IA-5(1) IA-5(1)(a) IA-5(1)(b) IA-5(1)(c) IA-5(1)(d) IA-5(1)(e) IA-5(1)(f) IA-5(2)(a) IA-5(2)(a)(1) IA-5(2)(a)(2) IA-5 (2)(b) IA-5 (2)(b)(1) IA-5 (2)(b)(2) IA-5 (6)	IA-5 (8) IA-5 (9) IA-5 (10) IA-9 IA-10 IA-11 SC-2 SC-2(1) SC-2(2) SC-3 SC-3 (1) SC-3 (2) SC-3 (3) SC-3 (4) SC-3 (5) SC-4 SC-4 (2) SC-5a. SC-5b. SC-5 (1)	SC-12 SC-12 (1) SC-13(a) SC-13(b) SC-15a. SC-15b. SC-15 (1) SC-15 (3) SC-15 (4) SC-16 SC-16 (1) SC-16(2) SC-16(3) SC-17a. SC-17b. SC-20a. SC-20b. SC-20 (2) SC-21 SC-23	SC-23 (1) SC-23 (3) SC-23 (5) SC-24 SC-25 SC-28 SC-28(1) SC-28(2) SC-28(3) SC-30 (2) SC-30 (3) SC-30 (4) SC-30 (5) SC-32 SC-32(1) SC-34 SC-34a. SC-34b. SC-34 (1) SC-34 (2)	SC-35 SC-39 SC-39 (1) SC-39 (2) SC-43a. SC-43b. SI-7 (10) CM-7(6) SI-7 (12) CM-7(7) CM-7(7)(a) CM-7(7)(b) SI-16 PM-5 PM-5(1) PM-7 PM-7(1)
CC6.1.6	CM-6a. CM-6b. CM-6c. CM-6d. CM-6 (1) CM-7a.	CM-7b. CM-7 (1)(a) CM-7 (1)(b) CM-7 (2) CM-7 (3) CM-8a.	CM-8a.2. CM-8a.3. CM-8a.4. CM-8a.5. CM-8b. CM-8 (1)	CM-8 (2) CM-8 (3)(a) CM-8 (3)(b) CM-8 (4) CM-8 (6) CM-8 (7)	CM-8 (9)(a) CM-8 (9)(b)
CC6.2.1 CC6.2.2 CC6.2.3 CC6.2.4 CC6.2.5	AC-2d. AC-2e. AC-2f. AC-2g. AC-2h. AC-2h.1. AC-2h.2. AC-2h.3. AC-2i. AC-2i.1.	AC-2i.2. AC-2i.3. AC-2j. AC-2k. AC-2l. AC-2 (7)(a) AC-2 (7)(c) IA-4 IA-4a. IA-4b.	IA-4c. IA-4d. IA-4 (1) IA-4 (4) IA-4 (5) IA-4 (6) IA-4(8) IA-4(9) IA-5 IA-5a.	IA-5b. IA-5d. IA-5i. IA-5 (1) IA-5(1)(a) IA-5(1)(b) IA-5(1)(c) IA-5(1)(d) IA-5(1)(e) IA-5(1)(f)	IA-5(1)(g) IA-5(1)(h) IA-12(1) IA-12(2) IA-12(4) PS-4b.
CC6.3.1	AC-6(1)	AC-6(1)	AC-6(1)	AC-6(1)	
CC6.3.2	AC-6(3) AC-6 (5) AC-6 (6) AC-6 (7)(a)	AC-6 (7)(b) AC-21a. AC-21b. AC-22a.	AC-22b. AC-22c. AC-22d. AC-24	PS-4 PS-4a. PS-4e. PS-5a.	PS-5b. PS-5c. PS-5d.
CC6.4.1 CC6.4.2 CC6.4.3	MP-2 PE-2a. PE-2b.	PE-2c. PE-2d. PE-2 (1)	PE-2 (2) PE-2 (3) PE-3a.	PE-3a.1. PE-3a.2. PE-3b.	PE-3c. PE-3d. PE-3e.

TSC Ref. #	NIST 800-53				
CC6.4.1 CC6.4.2 CC6.4.3	PE-3f. PE-3g. PE-3(1) PE-3(2) PE-4 PE-5	PE-5 (2) PE-22 PE-6a. PE-6b. PE-6c. PE-6 (2)	PE-6(4) PE-8a. PE-8b. PE-8c. PE-8(1) PE-8(3)	PE-16a. PE-16b. PE-17a. PE-17b. PE-17c. PE-17d.	PE-19 PE-19(1) PE-20 PS-4d. SC-7(14)
CC6.5.1 CC6.5.2 CC6.5.3	AC-7 (2) MA-2c. MA-2d. MA-3 (3) MA-3 (3)(a) MA-3 (3)(b)	MA-3 (3)(c) MA-3 (3)(d) MA-3 (4) MA-3(5) MA-3(6) MP-4a.	MP-4b. MP-4 (2) MP-6a. MP-6b. MP-6 (1) MP-6 (2)	MP-6 (3) MP-6 (7) MP-6 (8) MP-8a. MP-8b. MP-8c.	MP-8d. MP-8 (1) MP-8 (2) MP-8 (3) MP-8 (4)
CC6.6.1 CC6.6.2	AC-17a. AC-17b.	AC-17 (1) AC-17 (2)	AC-17 (3) AC-17(4)(a)	AC-17(4)(b) AC-17(9)	AC-17(10)
CC6.6.3 CC6.6.4 CC6.6.5	AC-18a.	AC-18b.	AC-18 (1)		
CC6.6.6 CC6.6.7 CC6.6.8	AC-18 (3)	AC-18 (4)	AC-18 (5)	AC-19a.	
CC6.6.9	AC-19b. AC-19 (4)(a) AC-19 (4)(b) AC-19 (4)(b)(1) AC-19 (4)(b)(2) AC-19 (4)(b)(3) AC-19 (4)(b)(4) AC-19 (4)(c) AC-19 (5) AC-20 (3) AC-20 (4) AC-20(5) CA-3a. CA-3b. CA-3c. CA-3(6)	CA-3(7)(a) CA-3(7)(b) CM-2 (7)(a) CM-2 (7)(b) MA-4a. MA-4b. MA-4c. MA-4d. MA-4e. PS-4c. PS-4 (1)(a) PS-4 (1)(b) PS-4 (2) PS-6(3)(a) PS-6(3)(b) SC-7a.	SC-7b. SC-7c. SC-7 (3) SC-7(4)(a) SC-7(4)(b) SC-7(4)(c) SC-7(4)(d) SC-7(4)(e) SC-7(4)(h) SC-7(5) SC-7(7) SC-7(8) SC-7(11) SC-7(12) SC-7(13) SC-7(15)	SC-7(16) SC-7(17) SC-7(18) SC-7(19) SC-7(20) SC-7(21) SC-7(22) SC-7(23) SC-7(24) SC-7(24)(a) SC-7(24)(b) SC-7(24)(c) SC-7(24)(d) SC-7(28) SC-7(29) SC-10	SC-11a. SC-11b. SC-11(1)(a) SC-11(1)(b) SC-40 SC-40 (1) SC-40 (2) SC-40 (3) SC-40 (4) SC-42a. SC-42b. SC-42 (1) SC-42 (2) SC-42(4) SC-42(5)
CC7.1.1 CC7.1.2 CC7.1.3 CC7.1.4 CC7.1.5	CM-3(5) CM-6(2) RA-5a. RA-5b. RA-5b.1.	RA-5b.2. RA-5b.3. RA-5c. RA-5d. RA-5e.	RA-5f. RA-5(2) RA-5(3) RA-5(4) RA-5(5)	RA-5(6) RA-5(8) RA-5(10) RA-5(11) RA-5(6)	
CC7.2.1 CC7.2.2 CC7.2.3	AC-2g. AC-2(4) AC-2(7)(b)	AC-2 (12)(a) AC-2(12)(b) AC-3(10)	AC-6 (9) AU-2a. AU-2b.	AU-2c. AU-2d. AU-2e.	AU-3 AU-3 (1) AU-3(3)

TSC Ref. #	NIST 800-53				
CC7.2.1 CC7.2.2 CC7.2.3	AU-4 AU-4 (1) AU-5a. AU-5b. AU-5 (1) AU-5 (2) AU-6(1) AU-6(3) AU-6(4) AU-6(5) AU-6(6) AU-6(7) AU-6(8) AU-6(9) AU-8a. AU-8b. SC-45 SC-45(1)(a) SC-45(1)(b) SC-45(2)(a) SC-45(2)(b) AU-9(a) AU-9(b) AU-9 (1) AU-9 (2) AU-9 (3)	AU-9 (4) AU-9 (5) AU-9 (6) AU-9(7) AU-10 AU-10(1)(a) AU-10(1)(b) AU-10(2)(a) AU-10(2)(b) AU-10(3) AU-10(4)(a) AU-10(4)(b) AU-11 AU-11 (1) AU-12a. AU-12b. AU-12c. AU-12(1) AU-12(2) AU-12(3) AU-12(4) AU-13a. AU-13b. AU-13b.1. AU-13b.2. AU-13(1)	AU-13(2) AU-13(3) AU-14a. AU-14b. AU-14 (1) AU-14 (3) AU-16 AU-16(1) AU-16(2) AU-16(3) IR-6a. IR-6b. IR-6 (1) MA-4(1)(a) MA-4(1)(b) SC-5 (3)(a) SC-5 (3)(b) SC-26 SC-36(1)(a) SC-36(1)(b) SC-42a. SC-42b. SI-4a. SI-4a.1. SI-4a.2. SI-4b.	SI-4c. SI-4c.1. SI-4c.2. SI-4d. SI-4e. SI-4f. SI-4g. SI-4 (1) SI-4 (2) SI-4 (3) SI-4(4)(a) SI-4(4)(b) SI-4(5) SI-4(7)(a) SI-4(7)(b) SI-4(9) SI-4(10) SI-4(11) SI-4(12) SI-4(13)(a) SI-4(13)(b) SI-4(13)(c) SI-4(14) SI-4(15) SI-4(16) SI-4(17)	SI-4(18) SI-4(19) SI-4(20) SI-4(22)(a) SI-4(22)(b) SI-4(23) SI-4(24) SI-4(25) SI-6a. SI-6b. SI-6c. SI-6d. SI-6(2) SI-6(3) SI-7a. SI-7b. SI-7(1) SI-7(2) SI-7(3) SI-7(6) SI-7(7) SI-7(8) SI-7(9)
CC7.3.1 CC7.3.2 CC7.3.3	AU-6a. AU-6b. AU-7	AU-7a. AU-7b. AU-7 (1)	SI-5a. SI-5b. SI-5c.	SI-5d. SI-5 (1) SI-7 (5)	SI-17 PM-12
CC7.5.1 CC7.5.2 CC7.5.3 CC7.5.4	AC-2 (13) IR-2a. IR-2a.1. IR-2a.2. IR-2a.3. IR-2b. IR-2(1) IR-2(2) IR-2(3) IR-3 IR-3 (1) IR-3 (2) IR-4a.	IR-4b. IR-4c. IR-4d. IR-4 (1) IR-4 (2) IR-4 (4) IR-4 (5) IR-4 (6) IR-4 (7) IR-4 (8) IR-4 (9) IR-4 (10) IR-5	IR-5 (1) IR-6 (2) IR-7 IR-7 (1) IR-7(2)(a) IR-7(2)(b) IR-8a. IR-8a.1. IR-8a.2. IR-8a.3. IR-8a.4. IR-8a.5. IR-8a.6.	IR-8a.7. IR-8a.8. IR-8a.9. IR-8a.10. IR-8b. IR-8c. IR-8d. IR-8e. IR-8(1) IR-8(1)a. IR-8(1)b. IR-8(1)c. IR-9	IR-9a. IR-9b. IR-9c. IR-9d. IR-9e. IR-9f. IR-9g. IR-9 (2) IR-9 (3) IR-9 (4)

TSC Ref. #	NIST 800-53				
CC8.1.1 CC8.1.2 CC8.1.3 CC8.1.4 CC8.1.5 CC8.1.6	CA-6a.	CM-3(2)	MA-2 (2)(b)	SA-4i.	SA-8(16)
	CA-6b.	CM-3(3)	MA-3a.	SA-4(1)	SA-8(17)
	CA-6c.	CM-3(4)	MA-3b.	SA-4(2)	SA-8(18)
	CA-6c.1.	CM-3(6)	MA-3 (1)	SA-4(3)	SA-8(19)
	CA-6c.2.	CM-3(7)	MA-4 (3)(a)	SA-4(3)(a)	SA-8(20)
	CA-6d.	CM-3(8)	MA-4 (3)(b)	SA-4(3)(b)	SA-8(21)
	CA-6e.	CM-4	MA-4 (4)	SA-4(3)(c)	SA-8(22)
	CA-6(1)	CM-4(1)	MA-4 (4)(a)	SA-4(5)	SA-8(23)
	CA-6(2)	CM-4(2)	MA-4 (4)(b)	SA-4(5)(a)	SA-8(24)
	CA-9a.	CM-5	MA-4(4)(b)(1)	SA-4(5)(b)	SA-8(25)
	CA-9b.	CM-5(1)(a)	MA-4(4)(b)(2)	SA-5a.	SA-8(26)
	CA-9c.	CM-5(1)(b)	MA-4 (5)	SA-5a.1.	SA-8(27)
	CA-9d.	CM-5 (4)	MA-4 (5)(a)	SA-5a.2.	SA-8(28)
	CA-9 (1)	CM-5 (5)(a)	MA-4 (5)(b)	SA-5a.3.	SA-8(29)
	CM-2	CM-5 (5)(b)	MA-4 (6)	SA-5b.	SA-8(30)
	CM-2.a.	CM-5 (6)	MA-4 (7)	SA-5b.1.	SA-8(31)
	CM-2.b.	CM-7 (4)(a)	SA-2a.	SA-5b.2.	SA-8(32)
	CM-2.b.1.	CM-7 (4)(b)	SA-2b.	SA-5b.3.	SA-8(33)
	CM-2.b.2.	CM-7 (4)(c)	SA-2c.	SA-5c.	SA-10
	CM-2 (2)	CM-7 (5)(a)	SA-3a.	SA-5d.	SA-10a.
	CM-2 (3)	CM-7 (5)(b)	SA-3b.	SA-8	SA-10b.
	CM-2 (6)	CM-7 (5)(c)	SA-3c.	SA-8(1)	SA-10c.
	CM-3a.	CM-9	SA-3d.	SA-8(2)	SA-10d.
	CM-3b.	CM-9a.	SA-3(1)	SA-8(3)	SA-10e.
	CM-3c.	CM-9b.	SA-3(2)(a)	SA-8(4)	SA-10(1)
	CM-3d.	CM-9c.	SA-3(2)(b)	SA-8(5)	SA-10(2)
	CM-3e.	CM-9d.	SA-3(3)	SA-8(6)	SA-10(3)
	CM-3f.	CM-9e.	SA-4	SA-8(7)	SA-10(4)
	CM-3g.	CM-9 (1)	SA-4a.	SA-8(8)	SA-10(5)
	CM-3(1)	IA-5 (5)	SA-4b.	SA-8(9)	SA-10(6)
	CM-3(1)(a)	IA-5 (7)	SA-4c.	SA-8(10)	SA-10(7)
	CM-3(1)(b)	MA-2a.	SA-4d.	SA-8(11)	SA-11
	CM-3(1)(c)	MA-2b.	SA-4e.	SA-8(12)	SA-11a.
	CM-3(1)(d)	MA-2e.	SA-4f.	SA-8(13)	SA-11b.
	CM-3(1)(e)	MA-2f.	SA-4g.	SA-8(14)	SA-11c.
	CM-3(1)(f)	MA-2 (2)(a)	SA-4h.	SA-8(15)	

TSC Ref. #	NIST 800-53				
CC8.1.6	SA-11d. SA-11e. SA-11 (1) SA-11 (2) SA-11(2)(a) SA-11(2)(b) SA-11(2)(c) SA-11(2)(d) SA-11(3)(a) SA-11(3)(b) SA-11(4) SA-11(5) SA-11(5)(a) SA-11(5)(b) SA-11 (6) SA-11 (7) SA-11 (8) SA-11(9)	SA-15a. SA-15a.1. SA-15a.2. SA-15a.3. SA-15a.4. SA-15b. SA-15(1) SA-15(1)(a) SA-15(1)(b) SA-15(2) SA-15(3) SA-15(3)(a) SA-15(3)(b) SA-15(5) SA-15(6) SA-15(7) SA-15(7)(a) SA-15(7)(b)	SA-15(7)(c) SA-15(7)(d) SA-15 (8) SA-15 (10) SA-15 (11) SA-15(12) SA-17 SA-17a. SA-17b. SA-17c. SA-17(1) SA-17(1)(a) SA-17(1)(b) SA-17(2) SA-17(2)(a) SA-17(2)(b) SA-17(3) SA-17(3)(a)	SA-17(3)(b) SA-17(3)(c) SA-17(3)(d) SA-17(3)(e) SA-17(4) SA-17(4)(a) SA-17(4)(b) SA-17(4)(c) SA-17(4)(d) SA-17(4)(e) SA-17(5) SA-17(5)(a) SA-17(5)(b) SA-17(6) SA-17(7) SA-22a. SA-22b. SC-27	SC-29 SC-29 (1) SC-30 SC-38 SI-2a. SI-2b. SI-2c. SI-2d. SI-2(2) SI-2(3)(a) SI-2(3)(b) SI-2(4) SI-2(5) SI-2(6) PM-8

NIST Not Applicable

TSC Ref. #	NIST 800-53			Reason
CC1.4	MA-5a. MA-5b. MA-5c. MA-5 (2) MA-5 (3) MA-5(4)	MA-5(4)(a) MA-5(4)(b) MA-5(5) PS-3a. PS-3b. PS-3(1)	PS-3(2) PS-3(3) PS-3(3)(a) PS-3(3)(b) PS-3(4)	GCommerce does not handle information that requires compliance with statutory/regulatory requirements such as healthcare data, law enforcement data, or intelligence data.
	SA-21 SA-21a. SA-21b.		PS-2a. PS-2b. PS-2c.	GCommerce does not work with national or economic security interests of the United States.
CC2.1	AC-8 AC-8a. AC-8a.1. AC-8a.2. AC-8a.3. AC-8a.4.		AC-8b. AC-8c. AC-8c.1. AC-8c.2. AC-8c.3.	GCommerce does not work with Government Information Systems.
CC6.1	IA-5e. IA-5f. IA-5 (1)(a) IA-5 (1)(b) IA-5 (1)(c) IA-5 (1)(d) IA-5 (1)(e) IA-5 (1)(f) IA-5 (2) IA-5 (2)(a) IA-5 (2)(b)	IA-5 (2)(c) IA-5 (2)(d) IA-5 (6) IA-5 (8) IA-5 (9) IA-5 (10) IA-5 (12) IA-5 (13) IA-5 (14) IA-5 (15) IA-6	IA-7 IA-8 IA-8 (1) IA-8 (2)(a) IA-8 (2)(b) IA-8 (4) IA-8 (5) IA-8 (6) SC-12 (2) SC-12 (3)	GCommerce does not complete any Federal Information Processing.
CC6.3	PS-6 (2) PS-6 (2)(a)		PS-6 (2)(b) PS-6 (2)(c)	GCommerce does not handle information that requires compliance with statutory/regulatory requirements such as healthcare data, law enforcement data, or intelligence data.
CC6.6	SC-7(25) SC-7(26)		SC-7(27)	
CC7.4		IR-6 (3)		GCommerce is not a supply chain organization.
CC8.1	MA-5c. MA-5 (1)(a) MA-5 (1)(a)(1) MA-5 (1)(a)(2)	MA-5 (1)(b) SA-4 (6)(a) SA-4 (6)(b) SA-4 (7)(a)	SA-4 (7)(b) SA-4 (8) SA-4 (9) SA-4 (10)	GCommerce does not work with Government Information Systems.

NIST 800-53 Definitions

NIST 800-53	NIST 800-53 Description
AC-1a.	Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
AC-1a.1	[Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that:
AC-1a.1.a	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
AC-1a.1.b	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
AC-1a.2.	Procedures to facilitate the implementation of the access control policy and associated access controls; and
AC-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and
AC-1c.	Review and update the current access control:
AC-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
AC-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
AC-2a.	Define and document the types of accounts allowed and specifically prohibited for use within the system;
AC-2b.	Assign account managers;
AC-2c.	Require [Assignment: organization-defined prerequisites and criteria] for group and role membership;
AC-2d.	Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account;
AC-2e.	Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts;
AC-2f.	Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria];
AC-2g.	Monitor the use of accounts;
AC-2h.	Notify account managers and [Assignment: organization-defined personnel or roles] within:
AC-2h.1.	[Assignment: organization-defined time period] when accounts are no longer required;
AC-2h.2.	[Assignment: organization-defined time period] when users are terminated or transferred; and

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AC-2h.3.	[Assignment: organization-defined time period] when system usage or need-to-know changes for an individual;
AC-2i.	Authorize access to the system based on:
AC-2i.1.	A valid access authorization;
AC-2i.2.	Intended system usage; and
AC-2i.3.	[Assignment: organization-defined attributes (as required)];
AC-2j.	Review accounts for compliance with account management requirements [Assignment: organization-defined frequency];
AC-2k.	Establish and implement a process for changing shared or group account authenticators (if deployed) when individuals are removed from the group; and
AC-2l.	Align account management processes with personnel termination and transfer processes.
AC-2(1)	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].
AC-2(2)	Automatically [Selection: remove; disable] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].
AC-2(3)	Disable accounts within [Assignment: organization-defined time period] when the accounts: (a) Have expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organizational policy; or (d) Have been inactive for [Assignment: organization-defined time period].
AC-2(4)	Automatically audit account creation, modification, enabling, disabling, and removal actions.
AC-2(5)	Require that users log out when [Assignment: organization-defined time period of expected inactivity or description of when to log out].
AC-2(6)	Disable accounts within [Assignment: organization-defined time period] when the accounts: (a) Have expired; (b) Are no longer associated with a user or individual; (c) Are in violation of organizational policy; or (d) Have been inactive for [Assignment: organization-defined time period].
AC-2(7)	(a) Establish and administer privileged user accounts in accordance with [Selection: a role-based access scheme; an attribute-based access scheme]; (b) Monitor privileged role or attribute assignments; (c) Monitor changes to roles or attributes; and (d) Revoke access when privileged role or attribute assignments are no longer appropriate.
AC-2(7)(a)	Establish and administer privileged user accounts in accordance with [Selection: a role-based access scheme; an attribute-based access scheme];

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AC-2(7)(b)	Monitor privileged role or attribute assignments;
AC-2(7)(c)	Monitor changes to roles or attributes; and
AC-2(8)	Create, activate, manage, and deactivate [Assignment: organization-defined system accounts] dynamically.
AC-2(9)	Only permit the use of shared and group accounts that meet [Assignment: organization-defined conditions for establishing shared and group accounts].
AC-2(11)	Enforce [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organization-defined system accounts].
AC-2(12)(a)	Monitor system accounts for [Assignment: organization-defined atypical usage]; and
AC-2(12)(b)	Report atypical usage of system accounts to [Assignment: organization-defined personnel or roles].
AC-2(13)	Disable accounts of individuals within [Assignment: organization-defined time period] of discovery of [Assignment: organization-defined significant risks].
AC-3	Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
AC-3(2)	Enforce dual authorization for [Assignment: organization-defined privileged commands and/or other organization-defined actions].
AC-3(3)	Enforce [Assignment: organization-defined mandatory access control policy] over the set of covered subjects and objects specified in the policy, and where the policy:
AC-3(3)(a)	Is uniformly enforced across the covered subjects and objects within the system;
AC-3(3)(b)	Specifies that a subject that has been granted access to information is constrained from doing any of the following;
AC-3(3)(b)(1)	Passing the information to unauthorized subjects or objects;
AC-3(3)(b)(2)	Granting its privileges to other subjects;
AC-3(3)(b)(3)	Changing one or more security attributes (specified by the policy) on subjects, objects, the system, or system components;
AC-3(3)(b)(4)	Choosing the security attributes and attribute values (specified by the policy) to be associated with newly created or modified objects; and
AC-3(3)(b)(5)	Changing the rules governing access control; and
AC-3(3)(c)	Specifies that [Assignment: organization-defined subjects] may explicitly be granted [Assignment: organization-defined privileges] such that they are not limited by any defined subset (or all) of the above constraints.
AC-3(4)	Enforce [Assignment: organization-defined discretionary access control policy] over the set of covered subjects and objects specified in the policy, and where the policy specifies that a subject that has been granted access to information can do one or more of the following:
AC-3(4)(a)	Pass the information to any other subjects or objects;

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AC-3(4)(b)	Grant its privileges to other subjects;
AC-3(4)(c)	Change security attributes on subjects, objects, the system, or the system's components;
AC-3(4)(d)	Choose the security attributes to be associated with newly created or revised objects; or
AC-3(4)(e)	Change the rules governing access control.
AC-3(5)	Prevent access to [Assignment: organization-defined security-relevant information] except during secure, non-operable system states.
AC-3(7)	Enforce a role-based access control policy over defined subjects and objects and control access based upon [Assignment: organization-defined roles and users authorized to assume such roles].
AC-3(8)	Enforce the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on [Assignment: organization-defined rules governing the timing of revocations of access authorizations].
AC-3(9)	Release information outside of the system only if:
AC-3(9)(a)	The receiving [Assignment: organization-defined system or system component] provides [Assignment: organization-defined controls]; and
AC-3(9)(b)	[Assignment: organization-defined controls] are used to validate the appropriateness of the information designated for release.
AC-3(10)	Employ an audited override of automated access control mechanisms under [Assignment: organization-defined conditions] by [Assignment: organization-defined roles].
AC-4	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].
AC-4(1)	Use [Assignment: organization-defined security and privacy attributes] associated with [Assignment: organization-defined information, source, and destination objects] to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.
AC-4(2)	Use protected processing domains to enforce [Assignment: organization-defined information flow control policies] as a basis for flow control decisions.
AC-4(3)	Enforce [Assignment: organization-defined information flow control policies].
AC-4(4)	Prevent encrypted information from bypassing [Assignment: organization-defined information flow control mechanisms] by [Selection (one or more): decrypting the information; blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; [Assignment: organization-defined procedure or method]].
AC-4(5)	Enforce [Assignment: organization-defined limitations] on embedding data types within other data types.
AC-4(6)	Enforce information flow control based on [Assignment: organization-defined metadata].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AC-4(7)	Enforce one-way information flows through hardware-based flow control mechanisms.
AC-4(8)(a)	Enforce information flow control using [Assignment: organization-defined security or privacy policy filters] as a basis for flow control decisions for [Assignment: organization-defined information flows]; and
AC-4(8)(b)	[Selection (one or more): Block; Strip; Modify; Quarantine] data after a filter processing failure in accordance with [Assignment: organization-defined security or privacy policy].
AC-4(9)	Enforce the use of human reviews for [Assignment: organization-defined information flows] under the following conditions: [Assignment: organization-defined conditions].
AC-4(10)	Provide the capability for privileged administrators to enable and disable [Assignment: organization-defined security or privacy policy filters] under the following conditions: [Assignment: organization-defined conditions].
AC-4(11)	Provide the capability for privileged administrators to configure [Assignment: organization-defined security or privacy policy filters] to support different security or privacy policies.
AC-4(12)	When transferring information between different security domains, use [Assignment: organization-defined data type identifiers] to validate data essential for information flow decisions.
AC-4(13)	When transferring information between different security domains, decompose information into [Assignment: organization-defined policy-relevant subcomponents] for submission to policy enforcement mechanisms.
AC-4(14)	When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] requiring fully enumerated formats that restrict data structure and content.
AC-4(15)	When transferring information between different security domains, examine the information for the presence of [Assignment: organization-defined unsanctioned information] and prohibit the transfer of such information in accordance with the [Assignment: organization-defined security or privacy policy].
AC-4(17)	Uniquely identify and authenticate source and destination points by [Selection (one or more): organization; system; application; service; individual] for information transfer.
AC-4(19)	When transferring information between different security domains, implement [Assignment: organization-defined security or privacy policy filters] on metadata.
AC-4(20)	Employ [Assignment: organization-defined solutions in approved configurations] to control the flow of [Assignment: organization-defined information] across security domains.
AC-4(21)	Separate information flows logically or physically using [Assignment: organization-defined mechanisms and/or techniques] to accomplish [Assignment: organization-defined required separations by types of information].
AC-4(22)	Provide access from a single device to computing platforms, applications, or data residing in multiple different security domains, while preventing information flow between the different security domains.
AC-4(23)	When transferring information between different security domains, modify non-releasable information by implementing [Assignment: organization-defined modification action].
AC-4(24)	When transferring information between different security domains, parse incoming data into an internal normalized format and regenerate the data to be consistent with its intended specification.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AC-4(25)	When transferring information between different security domains, sanitize data to minimize [Selection (one or more): delivery of malicious content, command and control of malicious code, malicious code augmentation, and steganography encoded data; spillage of sensitive information] in accordance with [Assignment: organization-defined policy]].
AC-4(26)	When transferring information between different security domains, record and audit content filtering actions and results for the information being filtered.
AC-4(27)	When transferring information between different security domains, implement content filtering solutions that provide redundant and independent filtering mechanisms for each data type.
AC-4(28)	When transferring information between different security domains, implement a linear content filter pipeline that is enforced with discretionary and mandatory access controls.
AC-4(29)	When transferring information between different security domains, employ content filter orchestration engines to ensure that:
AC-4(29)(a)	Content filtering mechanisms successfully complete execution without errors; and
AC-4(29)(b)	Content filtering actions occur in the correct order and comply with [Assignment: organization-defined policy].
AC-4(30)	When transferring information between different security domains, implement content filtering mechanisms using multiple processes.
AC-4(31)	When transferring information between different security domains, prevent the transfer of failed content to the receiving domain.
AC-4(32)	When transferring information between different security domains, the process that transfers information between filter pipelines:
AC-4(32)(a)	Does not filter message content;
AC-4(32)(b)	Validates filtering metadata;
AC-4(32)(c)	Ensures the content associated with the filtering metadata has successfully completed filtering; and
AC-4(32)(d)	Transfers the content to the destination filter pipeline.
AC-5a.	Identify and document [Assignment: organization-defined duties of individuals requiring separation]; and
AC-5b.	Define system access authorizations to support separation of duties.
AC-6	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.
AC-6(1)	Authorize access for [Assignment: organization-defined individuals or roles] to:
AC-6(1)(a)	[Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; and
AC-6(1)(b)	[Assignment: organization-defined security-relevant information].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AC-6(10)	Prevent non-privileged users from executing privileged functions.
AC-6(2)	Require that users of system accounts (or roles) with access to [Assignment: organization-defined security functions or security-relevant information] use non-privileged accounts or roles, when accessing nonsecurity functions.
AC-6(3)	Authorize network access to [Assignment: organization-defined privileged commands] only for [Assignment: organization-defined compelling operational needs] and document the rationale for such access in the security plan for the system.
AC-6(4)	Provide separate processing domains to enable finer-grained allocation of user privileges.
AC-6(5)	Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles].
AC-6(6)	Prohibit privileged access to the system by non-organizational users.
AC-6(7)(a)	Review [Assignment: organization-defined frequency] the privileges assigned to [Assignment: organization-defined roles or classes of users] to validate the need for such privileges; and
AC-6(7)(b)	Reassign or remove privileges, if necessary, to correctly reflect organizational mission and business needs.
AC-6(8)	Prevent the following software from executing at higher privilege levels than users executing the software: [Assignment: organization-defined software].
AC-6(9)	Log the execution of privileged functions.
AC-7a.	Enforce a limit of [Assignment: organization-defined number] consecutive invalid logon attempts by a user during a [Assignment: organization-defined time period]; and
AC-7b.	Automatically [Selection (one or more): lock the account or node for an [Assignment: organization-defined time period]; lock the account or node until released by an administrator; delay next logon prompt per [Assignment: organization-defined delay algorithm]; notify system administrator; take other [Assignment: organization-defined action]] when the maximum number of unsuccessful attempts is exceeded.
AC-7(2)	Purge or wipe information from [Assignment: organization-defined mobile devices] based on [Assignment: organization-defined purging or wiping requirements and techniques] after [Assignment: organization-defined number] consecutive, unsuccessful device logon attempts.
AC-8	The information system:
AC-8a.	Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:
AC-8a.1.	Users are accessing a U.S. Government system;
AC-8a.2.	System usage may be monitored, recorded, and subject to audit;

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AC-8a.3.	Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and
AC-8a.4.	Use of the system indicates consent to monitoring and recording;
AC-8b.	Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and
AC-8c.	For publicly accessible systems:
AC-8c.1.	Displays system use information [Assignment: organization-defined conditions], before granting further access;
AC-8c.2.	Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and
AC-8c.3.	Includes a description of the authorized uses of the system.
AC-9	Notify the user, upon successful logon to the system, of the date and time of the last logon.
AC-9(1)	Notify the user, upon successful logon, of the number of unsuccessful logon attempts since the last successful logon.
AC-9(2)	Notify the user, upon successful logon, of the number of [Selection: successful logons; unsuccessful logon attempts; both] during [Assignment: organization-defined time period].
AC-9(3)	Notify the user, upon successful logon, of changes to [Assignment: organization-defined security-related characteristics or parameters of the user's account] during [Assignment: organization-defined time period].
AC-9(4)	Notify the user, upon successful logon, of the following additional information: [Assignment: organization-defined additional information].
AC-10	Limit the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].
AC-11a.	Prevent further access to the system by [Selection (one or more): initiating a device lock after [Assignment: organization-defined time period] of inactivity; requiring the user to initiate a device lock before leaving the system unattended]; and
AC-11b.	Retain the device lock until the user reestablishes access using established identification and authentication procedures.
AC-11(1)	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.
AC-12	Automatically terminate a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect].
AC-12(1)	Provide a logout capability for user-initiated communications sessions whenever authentication is used to gain access to [Assignment: organization-defined information resources].
AC-12(2)	Display an explicit logout message to users indicating the termination of authenticated communications sessions.
AC-12(3)	Display an explicit message to users indicating that the session will end in [Assignment: organization-defined time until end of session].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AC-14a.	Identify [Assignment: organization-defined user actions] that can be performed on the system without identification or authentication consistent with organizational mission and business functions; and
AC-14b.	Document and provide supporting rationale in the security plan for the system, user actions not requiring identification or authentication.
AC-16a.	Provide the means to associate [Assignment: organization-defined types of security and privacy attributes] with [Assignment: organization-defined security and privacy attribute values] for information in storage, in process, and/or in transmission;
AC-16b.	Ensure that the attribute associations are made and retained with the information;
AC-16c.	Establish the following permitted security and privacy attributes from the attributes defined in AC-16a for [Assignment: organization-defined systems]: [Assignment: organization-defined security and privacy attributes];
AC-16d.	Determine the following permitted attribute values or ranges for each of the established attributes: [Assignment: organization-defined attribute values or ranges for established attributes];
AC-16e.	Audit changes to attributes; and
AC-16f.	Review [Assignment: organization-defined security and privacy attributes] for applicability [Assignment: organization-defined frequency].
AC-16(1)	Dynamically associate security and privacy attributes with [Assignment: organization-defined subjects and objects] in accordance with the following security and privacy policies as information is created and combined: [Assignment: organization-defined security and privacy policies].
AC-16(2)	Provide authorized individuals (or processes acting on behalf of individuals) the capability to define or change the value of associated security and privacy attributes.
AC-16(3)	Maintain the association and integrity of [Assignment: organization-defined security and privacy attributes] to [Assignment: organization-defined subjects and objects].
AC-16(4)	Provide the capability to associate [Assignment: organization-defined security and privacy attributes] with [Assignment: organization-defined subjects and objects] by authorized individuals (or processes acting on behalf of individuals).
AC-16(5)	Display security and privacy attributes in human-readable form on each object that the system transmits to output devices to identify [Assignment: organization-defined special dissemination, handling, or distribution instructions] using [Assignment: organization-defined human-readable, standard naming conventions].
AC-16(6)	Require personnel to associate and maintain the association of [Assignment: organization-defined security and privacy attributes] with [Assignment: organization-defined subjects and objects] in accordance with [Assignment: organization-defined security and privacy policies].
AC-16(7)	Provide a consistent interpretation of security and privacy attributes transmitted between distributed system components.
AC-16(8)	Implement [Assignment: organization-defined techniques and technologies] in associating security and privacy attributes to information.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AC-16(9)	Change security and privacy attributes associated with information only via regrading mechanisms validated using [Assignment: organization-defined techniques or procedures].
AC-16(10)	Provide authorized individuals the capability to define or change the type and value of security and privacy attributes available for association with subjects and objects.
AC-17a.	Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and
AC-17b.	Authorize each type of remote access to the system prior to allowing such connections.
AC-17(1)	Employ automated mechanisms to monitor and control remote access methods.
AC-17(2)	Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
AC-17(3)	Route remote accesses through authorized and managed network access control points.
AC-17(4)(a)	Authorize the execution of privileged commands and access to security-relevant information via remote access only in a format that provides assessable evidence and for the following needs: [Assignment: organization-defined needs]; and
AC-17(4)(b)	Document the rationale for remote access in the security plan for the system.
AC-17(6)	Protect information about remote access mechanisms from unauthorized use and disclosure.
AC-17(9)	Provide the capability to disconnect or disable remote access to the system within [Assignment: organization-defined time period].
AC-17(10)	Implement [Assignment: organization-defined mechanisms] to authenticate [Assignment: organization-defined remote commands].
AC-18a.	Establish configuration requirements, connection requirements, and implementation guidance for each type of wireless access; and
AC-18b.	Authorize each type of wireless access to the system prior to allowing such connections.
AC-18(1)	Protect wireless access to the system using authentication of [Selection (one or more): users; devices] and encryption.
AC-18(3)	Disable, when not intended for use, wireless networking capabilities embedded within system components prior to issuance and deployment.
AC-18(4)	Identify and explicitly authorize users allowed to independently configure wireless networking capabilities.
AC-18(5)	Select radio antennas and calibrate transmission power levels to reduce the probability that signals from wireless access points can be received outside of organization-controlled boundaries.
AC-19a.	Establish configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, to include when such devices are outside of controlled areas; and
AC-19b.	Authorize the connection of mobile devices to organizational systems.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AC-19(4)(a)	Prohibit the use of unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information unless specifically permitted by the authorizing official; and
AC-19(4)(b)	Enforce the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information:
AC-19(4)(b)(1)	Connection of unclassified mobile devices to classified systems is prohibited;
AC-19(4)(b)(2)	Connection of unclassified mobile devices to unclassified systems requires approval from the authorizing official;
AC-19(4)(b)(3)	Use of internal or external modems or wireless interfaces within the unclassified mobile devices is prohibited; and
AC-19(4)(b)(4)	Unclassified mobile devices and the information stored on those devices are subject to random reviews and inspections by [Assignment: organization-defined security officials], and if classified information is found, the incident handling policy is followed.
AC-19(4)(c)	Restrict the connection of classified mobile devices to classified systems in accordance with [Assignment: organization-defined security policies].
AC-19(5)	Employ [Selection: full-device encryption; container-based encryption] to protect the confidentiality and integrity of information on [Assignment: organization-defined mobile devices].
AC-20a.	[Selection (one or more): Establish [Assignment: organization-defined terms and conditions]; Identify [Assignment: organization-defined controls asserted to be implemented on external systems]], consistent with the trust relationships established with other organizations owning, operating, and/or maintaining external systems, allowing authorized individuals to:
AC-20a.1.	Access the system from external systems; and
AC-20a.2.	Process, store, or transmit organization-controlled information using external systems; or
AC-20b.	Prohibit the use of [Assignment: organizationally-defined types of external systems].
AC-20(1)	Permit authorized individuals to use an external system to access the system or to process, store, or transmit organization-controlled information only after:
AC-20(1)(a)	Verification of the implementation of controls on the external system as specified in the organization's security and privacy policies and security and privacy plans; or
AC-20(1)(b)	Retention of approved system connection or processing agreements with the organizational entity hosting the external system.
AC-20(2)	Restrict the use of organization-controlled portable storage devices by authorized individuals on external systems using [Assignment: organization-defined restrictions].
AC-20(3)	Restrict the use of non-organizationally owned systems or system components to process, store, or transmit organizational information using [Assignment: organization-defined restrictions].
AC-20(4)	Prohibit the use of [Assignment: organization-defined network accessible storage devices] in external systems.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AC-20(5)	Prohibit the use of organization-controlled portable storage devices by authorized individuals on external systems.
AC-21a.	Enable authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions for [Assignment: organization-defined information sharing circumstances where user discretion is required]; and
AC-21b.	Employ [Assignment: organization-defined automated mechanisms or manual processes] to assist users in making information sharing and collaboration decisions.
AC-21(1)	Employ [Assignment: organization-defined automated mechanisms] to enforce information-sharing decisions by authorized users based on access authorizations of sharing partners and access restrictions on information to be shared.
AC-21(2)	Implement information search and retrieval services that enforce [Assignment: organization-defined information sharing restrictions].
AC-22a.	Designate individuals authorized to make information publicly accessible;
AC-22b.	Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information;
AC-22c.	Review the proposed content of information prior to posting onto the publicly accessible system to ensure that nonpublic information is not included; and
AC-22d.	Review the content on the publicly accessible system for nonpublic information [Assignment: organization-defined frequency] and remove such information, if discovered.
AC-23	Employ [Assignment: organization-defined data mining prevention and detection techniques] for [Assignment: organization-defined data storage objects] to detect and protect against unauthorized data mining.
AC-24	[Selection: Establish procedures; Implement mechanisms] to ensure [Assignment: organization-defined access control decisions] are applied to each access request prior to access enforcement.
AC-24(1)	Transmit [Assignment: organization-defined access authorization information] using [Assignment: organization-defined controls] to [Assignment: organization-defined systems] that enforce access control decisions.
AC-24(2)	Enforce access control decisions based on [Assignment: organization-defined security or privacy attributes] that do not include the identity of the user or process acting on behalf of the user.
AC-25	Implement a reference monitor for [Assignment: organization-defined access control policies] that is tamperproof, always invoked, and small enough to be subject to analysis and testing, the completeness of which can be assured.
AT-1a.	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
AT-1a.1.	[Selection (one or more): Organization-level; Mission/business process-level; System-level] awareness and training policy that:
AT-1a.1.a	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
AT-1a.1.b	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AT-1a.2.	Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;
AT-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and
AT-1c.	Review and update the current awareness and training:
AT-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
AT-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
AT-2a.	Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
AT-2a.1.	As part of initial training for new users and [Assignment: organization-defined frequency] thereafter; and
AT-2a.2.	When required by system changes or following [Assignment: organization-defined events];
AT-2b.	Employ the following techniques to increase the security and privacy awareness of system users [Assignment: organization-defined awareness techniques];
AT-2c.	Update literacy training and awareness content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
AT-2d.	Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.
AT-2(1)	Provide practical exercises in literacy training that simulate events and incidents.
AT-2(2)	Provide literacy training on recognizing and reporting potential indicators of insider threat.
AT-2(3)	Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.
AT-2(4)	Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using [Assignment: organization-defined indicators of malicious code].
AT-2(5)	Provide literacy training on the advanced persistent threat.
AT-2(6)(a)	Provide literacy training on the cyber threat environment; and
AT-2(6)(b)	Reflect current cyber threat information in system operations.
AT-3a.	Provide role-based security and privacy training to personnel with the following roles and responsibilities: [Assignment: organization-defined roles and responsibilities]:
AT-3a.1.	Before authorizing access to the system, information, or performing assigned duties, and [Assignment: organization-defined frequency] thereafter; and
AT-3a.2.	When required by system changes;

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AT-3b.	Update role-based training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
AT-3c.	Incorporate lessons learned from internal or external security incidents or breaches into role-based training.
AT-3(1)	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of environmental controls.
AT-3(2)	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of physical security controls.
AT-3(3)	Provide practical exercises in security and privacy training that reinforce training objectives.
AT-3(5)	Provide [Assignment: organization-defined personnel or roles] with initial and [Assignment: organization-defined frequency] training in the employment and operation of personally identifiable information processing and transparency controls.
AT-4a.	Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and
AT-4b.	Retain individual training records for [Assignment: organization-defined time period].
AU-1a.	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
AU-1a.1.	[Selection (one or more): Organization-level; Mission/business process-level; System-level] audit and accountability policy that:
AU-1a.1.a.	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
AU-1a.1.b.	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
AU-1a.2.	Procedures to facilitate the implementation of the audit and accountability policy and the associated audit and accountability controls;
AU-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the audit and accountability policy and procedures; and
AU-1c	Review and update the current audit and accountability:
AU-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
AU-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
AU-2a.	Identify the types of events that the system is capable of logging in support of the audit function: [Assignment: organization-defined event types that the system is capable of logging];
AU-2b.	Coordinate the event logging function with other organizational entities requiring audit-related information to guide and inform the selection criteria for events to be logged;

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AU-2c.	Specify the following event types for logging within the system: [Assignment: organization-defined event types (subset of the event types defined in AU-2a.) along with the frequency of (or situation requiring) logging for each identified event type];
AU-2d.	Provide a rationale for why the event types selected for logging are deemed to be adequate to support after-the-fact investigations of incidents; and
AU-2e.	Review and update the event types selected for logging [Assignment: organization-defined frequency].
AU-3	Ensure that audit records contain information that establishes the following: a. What type of event occurred; b. When the event occurred; c. Where the event occurred; d. Source of the event; e. Outcome of the event; and f. Identity of any individuals, subjects, or objects/entities associated with the event.
AU-3(1)	Generate audit records containing the following additional information: [Assignment: organization-defined additional information].
AU-3(3)	Limit personally identifiable information contained in audit records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].
AU-4	Allocate audit log storage capacity to accommodate [Assignment: organization-defined audit log retention requirements].
AU-4(1)	Transfer audit logs [Assignment: organization-defined frequency] to a different system, system component, or media other than the system or system component conducting the logging.
AU-5a.	Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure; and
AU-5b.	Take the following additional actions: [Assignment: organization-defined additional actions].
AU-5(1)	Provide a warning to [Assignment: organization-defined personnel, roles, and/or locations] within [Assignment: organization-defined time period] when allocated audit log storage volume reaches [Assignment: organization-defined percentage] of repository maximum audit log storage capacity.
AU-5(2)	Provide an alert within [Assignment: organization-defined real-time period] to [Assignment: organization-defined personnel, roles, and/or locations] when the following audit failure events occur: [Assignment: organization-defined audit logging failure events requiring real-time alerts].
AU-5(3)	Enforce configurable network communications traffic volume thresholds reflecting limits on audit log storage capacity and [Selection: reject; delay] network traffic above those thresholds.
AU-5(4)	Invoke a [Selection: full system shutdown; partial system shutdown; degraded operational mode with limited mission or business functionality available] in the event of [Assignment: organization-defined audit logging failures], unless an alternate audit logging capability exists.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AU-6a.	Review and analyze system audit records [Assignment: organization-defined frequency] for indications of [Assignment: organization-defined inappropriate or unusual activity] and the potential impact of the inappropriate or unusual activity;
AU-6b.	Report findings to [Assignment: organization-defined personnel or roles];
AU-6(1)	Integrate audit record review, analysis, and reporting processes using [Assignment: organization-defined automated mechanisms].
AU-6(3)	Analyze and correlate audit records across different repositories to gain organization-wide situational awareness.
AU-6(4)	Provide and implement the capability to centrally review and analyze audit records from multiple components within the system.
AU-6(5)	Integrate analysis of audit records with analysis of [Selection (one or more): vulnerability scanning information; performance data; system monitoring information; [Assignment: organization-defined data/information collected from other sources]] to further enhance the ability to identify inappropriate or unusual activity.
AU-6(6)	Correlate information from audit records with information obtained from monitoring physical access to further enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity.
AU-6(7)	Specify the permitted actions for each [Selection (one or more): system process; role; user] associated with the review, analysis, and reporting of audit record information.
AU-6(8)	Perform a full text analysis of logged privileged commands in a physically distinct component or subsystem of the system, or other system that is dedicated to that analysis.
AU-6(9)	Correlate information from nontechnical sources with audit record information to enhance organization-wide situational awareness.
AU-7	Provide and implement an audit record reduction and report generation capability that:
AU-7a.	Supports on-demand audit record review, analysis, and reporting requirements and after-the-fact investigations of incidents; and
AU-7b.	Does not alter the original content or time ordering of audit records.
AU-7(1)	Provide and implement the capability to process, sort, and search audit records for events of interest based on the following content: [Assignment: organization-defined fields within audit records].
AU-8a.	Use internal system clocks to generate time stamps for audit records; and
AU-8b.	Record time stamps for audit records that meet [Assignment: organization-defined granularity of time measurement] and that use Coordinated Universal Time, have a fixed local time offset from Coordinated Universal Time, or that include the local time offset as part of the time stamp.
AU-9(a)	Protect audit information and audit logging tools from unauthorized access, modification, and deletion; and
AU-9(b)	Alert [Assignment: organization-defined personnel or roles] upon detection of unauthorized access, modification, or deletion of audit information.
AU-9(1)	Write audit trails to hardware-enforced, write-once media.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AU-9(2)	Store audit records [Assignment: organization-defined frequency] in a repository that is part of a physically different system or system component than the system or component being audited.
AU-9(3)	Implement cryptographic mechanisms to protect the integrity of audit information and audit tools.
AU-9(4)	Authorize access to management of audit logging functionality to only [Assignment: organization-defined subset of privileged users or roles].
AU-9(5)	Enforce dual authorization for [Selection (one or more): movement; deletion] of [Assignment: organization-defined audit information].
AU-9(6)	Authorize read-only access to audit information to [Assignment: organization-defined subset of privileged users or roles].
AU-9(7)	Store audit information on a component running a different operating system than the system or component being audited.
AU-10	Provide irrefutable evidence that an individual (or process acting on behalf of an individual) has performed [Assignment: organization-defined actions to be covered by non-repudiation].
AU-10(1)(a)	Bind the identity of the information producer with the information to [Assignment: organization-defined strength of binding]; and
AU-10(1)(b)	Provide the means for authorized individuals to determine the identity of the producer of the information.
AU-10(2)(a)	Validate the binding of the information producer identity to the information at [Assignment: organization-defined frequency]; and
AU-10(2)(b)	Perform [Assignment: organization-defined actions] in the event of a validation error.
AU-10(3)	Maintain reviewer or releaser credentials within the established chain of custody for information reviewed or released.
AU-10(4)(a)	Validate the binding of the information reviewer identity to the information at the transfer or release points prior to release or transfer between [Assignment: organization-defined security domains]; and
AU-10(4)(b)	Perform [Assignment: organization-defined actions] in the event of a validation error.
AU-11	Retain audit records for [Assignment: organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements.
AU-11(1)	Employ [Assignment: organization-defined measures] to ensure that long-term audit records generated by the system can be retrieved.
AU-12a.	Provide audit record generation capability for the event types the system is capable of auditing as defined in AU-2a on [Assignment: organization-defined system components];
AU-12b.	Allow [Assignment: organization-defined personnel or roles] to select the event types that are to be logged by specific components of the system; and
AU-12c.	Generate audit records for the event types defined in AU-2c that include the audit record content defined in AU-3.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AU-12(1)	Compile audit records from [Assignment: organization-defined system components] into a system-wide (logical or physical) audit trail that is time-correlated to within [Assignment: organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail].
AU-12(2)	Produce a system-wide (logical or physical) audit trail composed of audit records in a standardized format.
AU-12(3)	Provide and implement the capability for [Assignment: organization-defined individuals or roles] to change the logging to be performed on [Assignment: organization-defined system components] based on [Assignment: organization-defined selectable event criteria] within [Assignment: organization-defined time thresholds].
AU-12(4)	Provide and implement the capability for auditing the parameters of user query events for data sets containing personally identifiable information.
AU-13a.	Monitor [Assignment: organization-defined open-source information and/or information sites] [Assignment: organization-defined frequency] for evidence of unauthorized disclosure of organizational information; and
AU-13b.	If an information disclosure is discovered:
AU-13b.1.	Notify [Assignment: organization-defined personnel or roles]; and
AU-13b.2.	Take the following additional actions: [Assignment: organization-defined additional actions].
AU-13(1)	Monitor open-source information and information sites using [Assignment: organization-defined automated mechanisms].
AU-13(2)	Review the list of open-source information sites being monitored [Assignment: organization-defined frequency].
AU-13(3)	Employ discovery techniques, processes, and tools to determine if external entities are replicating organizational information in an unauthorized manner.
AU-14a.	Provide and implement the capability for [Assignment: organization-defined users or roles] to [Selection (one or more): record; view; hear; log] the content of a user session under [Assignment: organization-defined circumstances]; and
AU-14b.	Develop, integrate, and use session auditing activities in consultation with legal counsel and in accordance with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
AU-14(1)	Initiate session audits automatically at system start-up.
AU-14(3)	Provide and implement the capability for authorized users to remotely view and hear content related to an established user session in real time.
AU-16	Employ [Assignment: organization-defined methods] for coordinating [Assignment: organization-defined audit information] among external organizations when audit information is transmitted across organizational boundaries.
AU-16(1)	Preserve the identity of individuals in cross-organizational audit trails.
AU-16(2)	Provide cross-organizational audit information to [Assignment: organization-defined organizations] based on [Assignment: organization-defined cross-organizational sharing agreements].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
AU-16(3)	Implement [Assignment: organization-defined measures] to disassociate individuals from audit information transmitted across organizational boundaries.
CA-1a.	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
CA-1a.1.	[Selection (one or more): Organization-level; Mission/business process-level; System-level] assessment, authorization, and monitoring policy that:
CA-1a.1.a	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
CA-1a.1.b	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
CA-1a.2.	Procedures to facilitate the implementation of the assessment, authorization, and monitoring policy and the associated assessment, authorization, and monitoring controls;
CA-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the assessment, authorization, and monitoring policy and procedures; and
CA-1c.	Review and update the current assessment, authorization, and monitoring:
CA-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
CA-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
CA-2a.	Select the appropriate assessor or assessment team for the type of assessment to be conducted;
CA-2b.	Develop a control assessment plan that describes the scope of the assessment including:
CA-2b.1.	Controls and control enhancements under assessment;
CA-2b.2.	Assessment procedures to be used to determine control effectiveness; and
CA-2b.3.	Assessment environment, assessment team, and assessment roles and responsibilities;
CA-2c.	Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;
CA-2d.	Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;
CA-2e.	Produce a control assessment report that document the results of the assessment; and
CA-2f.	Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].
CA-2(1)	Employ independent assessors or assessment teams to conduct control assessments.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
CA-2(2)	Include as part of control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection (one or more): in-depth monitoring; security instrumentation; automated security test cases; vulnerability scanning; malicious user testing; insider threat assessment; performance and load testing; data leakage or data loss assessment; [Assignment: organization-defined other forms of assessment]].
CA-2(3)	Leverage the results of control assessments performed by [Assignment: organization-defined external organization] on [Assignment: organization-defined system] when the assessment meets [Assignment: organization-defined requirements].
CA-3a.	Approve and manage the exchange of information between the system and other systems using [Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements; user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]];
CA-3b.	Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated; and
CA-3c.	Review and update the agreements [Assignment: organization-defined frequency].
CA-3(6)	Verify that individuals or systems transferring data between interconnecting systems have the requisite authorizations (i.e., write permissions or privileges) prior to accepting such data.
CA-3(7)(a)	Identify transitive (downstream) information exchanges with other systems through the systems identified in CA-3a; and
CA-3(7)(b)	Take measures to ensure that transitive (downstream) information exchanges cease when the controls on identified transitive (downstream) systems cannot be verified or validated.
CA-5a.	Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
CA-5b.	Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.
CA-5(1)	Ensure the accuracy, currency, and availability of the plan of action and milestones for the system using [Assignment: organization-defined automated mechanisms].
CA-6a.	Assign a senior official as the authorizing official for the system;
CA-6b.	Assign a senior official as the authorizing official for common controls available for inheritance by organizational systems;
CA-6c.	Ensure that the authorizing official for the system, before commencing operations:
CA-6c.1.	Accepts the use of common controls inherited by the system; and

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
CA-6c.2.	Authorizes the system to operate;
CA-6d.	Ensure that the authorizing official for common controls authorizes the use of those controls for inheritance by organizational systems;
CA-6e.	Update the authorizations [Assignment: organization-defined frequency].
CA-6(1)	Employ a joint authorization process for the system that includes multiple authorizing officials from the same organization conducting the authorization.
CA-6(2)	Employ a joint authorization process for the system that includes multiple authorizing officials with at least one authorizing official from an organization external to the organization conducting the authorization.
CA-7	Develop a system-level continuous monitoring strategy and implement continuous monitoring in accordance with the organization-level continuous monitoring strategy that includes:
CA-7a.	Establishing the following system-level metrics to be monitored: [Assignment: organization-defined system-level metrics];
CA-7b.	Establishing [Assignment: organization-defined frequencies] for monitoring and [Assignment: organization-defined frequencies] for assessment of control effectiveness;
CA-7c.	Ongoing control assessments in accordance with the continuous monitoring strategy;
CA-7d.	Ongoing monitoring of system and organization-defined metrics in accordance with the continuous monitoring strategy;
CA-7e.	Correlation and analysis of information generated by control assessments and monitoring;
CA-7f.	Response actions to address results of the analysis of control assessment and monitoring information; and
CA-7g.	Reporting the security and privacy status of the system to [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency].
CA-7(1)	Employ independent assessors or assessment teams to monitor the controls in the system on an ongoing basis.
CA-7(3)	Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data.
CA-7(4)	Ensure risk monitoring is an integral part of the continuous monitoring strategy that includes the following: (a) Effectiveness monitoring; (b) Compliance monitoring; and (c) Change monitoring.
CA-7(5)	Employ the following actions to validate that policies are established and implemented controls are operating in a consistent manner: [Assignment: organization-defined actions].
CA-7(6)	Ensure the accuracy, currency, and availability of monitoring results for the system using [Assignment: organization-defined automated mechanisms].
CA-8	Conduct penetration testing [Assignment: organization-defined frequency] on [Assignment: organization-defined systems or system components].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
CA-8(1)	Employ an independent penetration testing agent or team to perform penetration testing on the system or system components.
CA-8(2)	Employ the following red-team exercises to simulate attempts by adversaries to compromise organizational systems in accordance with applicable rules of engagement: [Assignment: organization-defined red team exercises].
CA-8(3)	Employ a penetration testing process that includes [Assignment: organization-defined frequency] [Selection: announced; unannounced] attempts to bypass or circumvent controls associated with physical access points to the facility.
CA-9a.	Authorize internal connections of [Assignment: organization-defined system components or classes of components] to the system;
CA-9b.	Document, for each internal connection, the interface characteristics, security and privacy requirements, and the nature of the information communicated;
CA-9c.	Terminate internal system connections after [Assignment: organization-defined conditions]; and
CA-9d.	Review [Assignment: organization-defined frequency] the continued need for each internal connection.
CA-9(1)	Perform security and privacy compliance checks on constituent system components prior to the establishment of the internal connection.
CM-1a.	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
CM-1a.1.	[Selection (one or more): Organization-level; Mission/business process-level; System-level] configuration management policy that:
CM-1a.1.a	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
CM-1a.1.b	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
CM-1a.2.	Procedures to facilitate the implementation of the configuration management policy and the associated configuration management controls;
CM-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the configuration management policy and procedures; and
CM-1c.	Review and update the current configuration management:
CM-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
CM-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
CM-2	Develop, document, and maintain under configuration control, a current baseline configuration of the system; and
CM-2(2)	Maintain the currency, completeness, accuracy, and availability of the baseline configuration of the system using [Assignment: organization-defined automated mechanisms].
CM-2(3)	Retain [Assignment: organization-defined number] of previous versions of baseline configurations of the system to support rollback.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
CM-2(6)	Maintain a baseline configuration for system development and test environments that is managed separately from the operational baseline configuration.
CM-2(7)(a)	Issue [Assignment: organization-defined systems or system components] with [Assignment: organization-defined configurations] to individuals traveling to locations that the organization deems to be of significant risk; and
CM-2(7)(b)	Apply the following controls to the systems or components when the individuals return from travel: [Assignment: organization-defined controls].
CM-2.a.	Review and update the baseline configuration of the system:
CM-2.b.	[Assignment: organization-defined frequency];
CM-2.b.1.	When required due to [Assignment: organization-defined circumstances]; and
CM-2.b.2.	When system components are installed or upgraded.
CM-3a.	Determine and document the types of changes to the system that are configuration-controlled;
CM-3b.	Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses;
CM-3c.	Document configuration change decisions associated with the system;
CM-3d.	Implement approved configuration-controlled changes to the system;
CM-3e.	Retain records of configuration-controlled changes to the system for [Assignment: organization-defined time period];
CM-3f.	Monitor and review activities associated with configuration-controlled changes to the system; and
CM-3g.	Coordinate and provide oversight for configuration change control activities through [Assignment: organization-defined configuration change control element] that convenes [Selection (one or more): [Assignment: organization-defined frequency]; when [Assignment: organization-defined configuration change conditions]].
CM-3(1)	Use [Assignment: organization-defined automated mechanisms] to:
CM-3(1)(a)	Document proposed changes to the system;
CM-3(1)(b)	Notify [Assignment: organization-defined approval authorities] of proposed changes to the system and request change approval;
CM-3(1)(c)	Highlight proposed changes to the system that have not been approved or disapproved within [Assignment: organization-defined time period];
CM-3(1)(d)	Prohibit changes to the system until designated approvals are received;
CM-3(1)(e)	Document all changes to the system; and
CM-3(1)(f)	Notify [Assignment: organization-defined personnel] when approved changes to the system are completed.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
CM-3(2)	Test, validate, and document changes to the system before finalizing the implementation of the changes.
CM-3(3)	Implement changes to the current system baseline and deploy the updated baseline across the installed base using [Assignment: organization-defined automated mechanisms].
CM-3(4)	Require [Assignment: organization-defined security and privacy representatives] to be members of the [Assignment: organization-defined configuration change control element].
CM-3(5)	Implement the following security responses automatically if baseline configurations are changed in an unauthorized manner: [Assignment: organization-defined security responses].
CM-3(6)	Ensure that cryptographic mechanisms used to provide the following controls are under configuration management: [Assignment: organization-defined controls].
CM-3(7)	Review changes to the system [Assignment: organization-defined frequency] or when [Assignment: organization-defined circumstances] to determine whether unauthorized changes have occurred.
CM-3(8)	Prevent or restrict changes to the configuration of the system under the following circumstances: [Assignment: organization-defined circumstances].
CM-4	Analyze changes to the system to determine potential security and privacy impacts prior to change implementation.
CM-4(1)	Analyze changes to the system in a separate test environment before implementation in an operational environment, looking for security and privacy impacts due to flaws, weaknesses, incompatibility, or intentional malice.
CM-4(2)	After system changes, verify that the impacted controls are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security and privacy requirements for the system.
CM-5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to the system.
CM-5(1)(a)	Enforce access restrictions using [Assignment: organization-defined automated mechanisms]; and
CM-5(1)(b)	Automatically generate audit records of the enforcement actions.
CM-5(4)	Enforce dual authorization for implementing changes to [Assignment: organization-defined system components and system-level information].
CM-5(5)(a)	Limit privileges to change system components and system-related information within a production or operational environment; and
CM-5(5)(b)	Review and reevaluate privileges [Assignment: organization-defined frequency].
CM-5(6)	Limit privileges to change software resident within software libraries.
CM-6a.	Establish and document configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using [Assignment: organization-defined common secure configurations];
CM-6b.	Implement the configuration settings;

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
CM-6c.	Identify, document, and approve any deviations from established configuration settings for [Assignment: organization-defined system components] based on [Assignment: organization-defined operational requirements]; and
CM-6d.	Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.
CM-6(1)	Manage, apply, and verify configuration settings for [Assignment: organization-defined system components] using [Assignment: organization-defined automated mechanisms].
CM-6(2)	Take the following actions in response to unauthorized changes to [Assignment: organization-defined configuration settings]: [Assignment: organization-defined actions].
CM-7a.	Configure the system to provide only [Assignment: organization-defined mission essential capabilities]; and
CM-7b.	Prohibit or restrict the use of the following functions, ports, protocols, software, and/or services: [Assignment: organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services].
CM-7(1)(a)	Review the system [Assignment: organization-defined frequency] to identify unnecessary and/or nonsecure functions, ports, protocols, software, and services; and
CM-7(1)(b)	Disable or remove [Assignment: organization-defined functions, ports, protocols, software, and services within the system deemed to be unnecessary and/or nonsecure].
CM-7(2)	Prevent program execution in accordance with [Selection (one or more): [Assignment: organization-defined policies, rules of behavior, and/or access agreements regarding software program usage and restrictions]; rules authorizing the terms and conditions of software program usage].
CM-7(3)	Ensure compliance with [Assignment: organization-defined registration requirements for functions, ports, protocols, and services].
CM-7(4)(a)	Identify [Assignment: organization-defined software programs not authorized to execute on the system];
CM-7(4)(b)	Employ an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the system; and
CM-7(4)(c)	Review and update the list of unauthorized software programs [Assignment: organization-defined frequency].
CM-7(5)(a)	Identify [Assignment: organization-defined software programs authorized to execute on the system];
CM-7(5)(b)	Employ a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the system; and
CM-7(5)(c)	Review and update the list of authorized software programs [Assignment: organization-defined frequency].
CM-7(6)	Require that the following user-installed software execute in a confined physical or virtual machine environment with limited privileges: [Assignment: organization-defined user-installed software].
CM-7(7)	Allow execution of binary or machine-executable code only in confined physical or virtual machine environments and with the explicit approval of [Assignment: organization-defined personnel or roles] when such code is:
CM-7(7)(a)	Obtained from sources with limited or no warranty; and/or

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
CM-7(7)(b)	Without the provision of source code.
CM-7(8)(a)	Prohibit the use of binary or machine-executable code from sources with limited or no warranty or without the provision of source code; and
CM-7(8)(b)	Allow exceptions only for compelling mission or operational requirements and with the approval of the authorizing official.
CM-8a.	Develop and document an inventory of system components that:
CM-8a.1.	Accurately reflects the system;
CM-8a.2.	Includes all components within the system;
CM-8a.3.	Does not include duplicate accounting of components or components assigned to any other system;
CM-8a.4.	Is at the level of granularity deemed necessary for tracking and reporting; and
CM-8a.5.	Includes the following information to achieve system component accountability: [Assignment: organization-defined information deemed necessary to achieve effective system component accountability]; and
CM-8b.	Review and update the system component inventory [Assignment: organization-defined frequency].
CM-8(1)	Update the inventory of system components as part of component installations, removals, and system updates.
CM-8(2)	Maintain the currency, completeness, accuracy, and availability of the inventory of system components using [Assignment: organization-defined automated mechanisms].
CM-8(3)(a)	Detect the presence of unauthorized hardware, software, and firmware components within the system using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency]; and
CM-8(3)(b)	Take the following actions when unauthorized components are detected: [Selection (one or more): disable network access by such components; isolate the components; notify [Assignment: organization-defined personnel or roles]].
CM-8(4)	Include in the system component inventory information, a means for identifying by [Selection (one or more): name; position; role], individuals responsible and accountable for administering those components.
CM-8(6)	Include assessed component configurations and any approved deviations to current deployed configurations in the system component inventory.
CM-8(7)	Provide a centralized repository for the inventory of system components.
CM-8(8)	Support the tracking of system components by geographic location using [Assignment: organization-defined automated mechanisms].
CM-8(9)(a)	Assign system components to a system; and
CM-8(9)(b)	Receive an acknowledgement from [Assignment: organization-defined personnel or roles] of this assignment.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
CM-9	Develop, document, and implement a configuration management plan for the system that:
CM-9a.	Addresses roles, responsibilities, and configuration management processes and procedures;
CM-9b.	Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items;
CM-9c.	Defines the configuration items for the system and places the configuration items under configuration management;
CM-9d.	Is reviewed and approved by [Assignment: organization-defined personnel or roles]; and
CM-9e.	Protects the configuration management plan from unauthorized disclosure and modification.
CM-9(1)	Assign responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.
CM-10a.	Use software and associated documentation in accordance with contract agreements and copyright laws;
CM-10b.	Track the use of software and associated documentation protected by quantity licenses to control copying and distribution; and
CM-10c.	Control and document the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.
CM-10(1)	Establish the following restrictions on the use of open-source software: [Assignment: organization-defined restrictions].
CM-11a.	Establish [Assignment: organization-defined policies] governing the installation of software by users;
CM-11b.	Enforce software installation policies through the following methods: [Assignment: organization-defined methods]; and
CM-11c.	Monitor policy compliance [Assignment: organization-defined frequency].
CM-11(1)	Allow user installation of software only with explicit privileged status.
CM-11(2)	Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].
CM-11(3)	Enforce and monitor compliance with software installation policies using [Assignment: organization-defined automated mechanisms].
CP-1a.	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
CP-1a.1.	[Selection (one or more): Organization-level; Mission/business process-level; System-level] contingency planning policy that:
CP-1a.1.(a)	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
CP-1a.1.(b)	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
CP-1a.2.	Procedures to facilitate the implementation of the contingency planning policy and the associated contingency planning controls;

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
CP-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the contingency planning policy and procedures; and
CP-1c.	Review and update the current contingency planning:
CP-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
CP-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
CP-2a.	Develop a contingency plan for the system that:
CP-2a.1.	Identifies essential mission and business functions and associated contingency requirements;
CP-2a.2.	Provides recovery objectives, restoration priorities, and metrics;
CP-2a.3.	Addresses contingency roles, responsibilities, assigned individuals with contact information;
CP-2a.4.	Addresses maintaining essential mission and business functions despite a system disruption, compromise, or failure;
CP-2a.5.	Addresses eventual, full system restoration without deterioration of the controls originally planned and implemented;
CP-2a.6.	Addresses the sharing of contingency information; and
CP-2a.7.	Is reviewed and approved by [Assignment: organization-defined personnel or roles];
CP-2b.	Distribute copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
CP-2c.	Coordinate contingency planning activities with incident handling activities;
CP-2d.	Review the contingency plan for the system [Assignment: organization-defined frequency];
CP-2e.	Update the contingency plan to address changes to the organization, system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;
CP-2f.	Communicate contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];
CP-2g.	Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and
CP-2h.	Protect the contingency plan from unauthorized disclosure and modification.
CP-2(1)	Coordinate contingency plan development with organizational elements responsible for related plans.
CP-2(2)	Conduct capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.
CP-2(3)	Plan for the resumption of [Selection: all; essential] mission and business functions within [Assignment: organization-defined time period] of contingency plan activation.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
CP-2(5)	Plan for the continuance of [Selection: all; essential] mission and business functions with minimal or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites.
CP-2(6)	Plan for the transfer of [Selection: all; essential] mission and business functions to alternate processing and/or storage sites with minimal or no loss of operational continuity and sustain that continuity through system restoration to primary processing and/or storage sites.
CP-2(7)	Coordinate the contingency plan with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.
CP-2(8)	Identify critical system assets supporting [Selection: all; essential] mission and business functions.
CP-3a.	Provide contingency training to system users consistent with assigned roles and responsibilities:
CP-3a.1	Within [Assignment: organization-defined time period] of assuming a contingency role or responsibility;
CP-3a.2	When required by system changes; and
CP-3a.3	[Assignment: organization-defined frequency] thereafter; and
CP-3b.	Review and update contingency training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
CP-3(1)	Incorporate simulated events into contingency training to facilitate effective response by personnel in crisis situations.
CP-3(2)	Employ mechanisms used in operations to provide a more thorough and realistic contingency training environment.
CP-7a.	Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable;
CP-7b.	Make available at the alternate processing site, the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and
CP-7c.	Provide controls at the alternate processing site that are equivalent to those at the primary site.
CP-7(1)	Identify an alternate processing site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.
CP-7(2)	Identify potential accessibility problems to alternate processing sites in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.
CP-7(3)	Develop alternate processing site agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives).
CP-7(4)	Prepare the alternate processing site so that the site can serve as the operational site supporting essential mission and business functions.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
CP-7(6)	Plan and prepare for circumstances that preclude returning to the primary processing site.
CP-8	Establish alternate telecommunications services, including necessary agreements to permit the resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period] when the primary telecommunications capabilities are unavailable at either the primary or alternate processing or storage sites.
CP-8(1)(a)	Develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with availability requirements (including recovery time objectives); and
CP-8(1)(b)	Request Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness if the primary and/or alternate telecommunications services are provided by a common carrier.
CP-8(2)	Obtain alternate telecommunications services to reduce the likelihood of sharing a single point of failure with primary telecommunications services.
CP-8(3)	Obtain alternate telecommunications services from providers that are separated from primary service providers to reduce susceptibility to the same threats.
CP-8(4)(a)	Require primary and alternate telecommunications service providers to have contingency plans;
CP-8(4)(b)	Review provider contingency plans to ensure that the plans meet organizational contingency requirements; and
CP-8(4)(c)	Obtain evidence of contingency testing and training by providers [Assignment: organization-defined frequency].
CP-8(5)	Test alternate telecommunication services [Assignment: organization-defined frequency].
CP-10	Provide for the recovery and reconstitution of the system to a known state within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] after a disruption, compromise, or failure.
CP-10(2)	Implement transaction recovery for systems that are transaction-based.
CP-10(4)	Provide the capability to restore system components within [Assignment: organization-defined restoration time periods] from configuration-controlled and integrity-protected information representing a known, operational state for the components.
CP-10(6)	Protect system components used for recovery and reconstitution.
CP-11	Provide the capability to employ [Assignment: organization-defined alternative communications protocols] in support of maintaining continuity of operations.
CP-12	When [Assignment: organization-defined conditions] are detected, enter a safe mode of operation with [Assignment: organization-defined restrictions of safe mode of operation].
CP-13	Employ [Assignment: organization-defined alternative or supplemental security mechanisms] for satisfying [Assignment: organization-defined security functions] when the primary means of implementing the security function is unavailable or compromised.
IA-1a.	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
IA-1a.1.	[Selection (one or more): Organization-level; Mission/business process-level; System-level] identification and authentication policy that:
IA-1a.1.a	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
IA-1a.1.b	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
IA-1a.2.	Procedures to facilitate the implementation of the identification and authentication policy and the associated identification and authentication controls;
IA-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the identification and authentication policy and procedures; and
IA-1c.	Review and update the current identification and authentication:
IA-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
IA-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
IA-2	Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.
IA-2(1)	Implement multi-factor authentication for access to privileged accounts.
IA-2(2)	Implement multi-factor authentication for access to non-privileged accounts.
IA-2(5)	When shared accounts or authenticators are employed, require users to be individually authenticated before granting access to the shared accounts or resources.
IA-2(6)	Implement multi-factor authentication for [Selection (one or more): local; network; remote] access to [Selection (one or more): privileged accounts; non-privileged accounts] such that:
IA-2(6)(a)	One of the factors is provided by a device separate from the system gaining access; and
IA-2(6)(b)	The device meets [Assignment: organization-defined strength of mechanism requirements].
IA-2(8)	The information system implements replay-resistant authentication mechanisms for network access to privileged accounts.
IA-2(10)	Implement replay-resistant authentication mechanisms for access to [Selection (one or more): privileged accounts; non-privileged accounts].
IA-2(12)	Accept and electronically verify Personal Identity Verification-compliant credentials.
IA-2(13)	Implement the following out-of-band authentication mechanisms under [Assignment: organization-defined conditions]: [Assignment: organization-defined out-of-band authentication].
IA-3	Uniquely identify and authenticate [Assignment: organization-defined devices and/or types of devices] before establishing a [Selection (one or more): local; remote; network] connection.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
IA-3(1)	Authenticate [Assignment: organization-defined devices and/or types of devices] before establishing [Selection (one or more): local; remote; network] connection using bidirectional authentication that is cryptographically based.
IA-3(3)(a)	Where addresses are allocated dynamically, standardize dynamic address allocation lease information and the lease duration assigned to devices in accordance with [Assignment: organization-defined lease information and lease duration]; and
IA-3(3)(b)	Audit lease information when assigned to a device.
IA-3(4)	Handle device identification and authentication based on attestation by [Assignment: organization-defined configuration management process].
IA-4	Manage system identifiers by:
IA-4a.	Receiving authorization from [Assignment: organization-defined personnel or roles] to assign an individual, group, role, service, or device identifier;
IA-4b.	Selecting an identifier that identifies an individual, group, role, service, or device;
IA-4c.	Assigning the identifier to the intended individual, group, role, service, or device; and
IA-4d.	Preventing reuse of identifiers for [Assignment: organization-defined time period].
IA-4(1)	The organization prohibits the use of information system account identifiers that are the same as public identifiers for individual electronic mail accounts.
IA-4(4)	The organization manages individual identifiers by uniquely identifying each individual as [Assignment: organization-defined characteristic identifying individual status].
IA-4(5)	The information system dynamically manages identifiers.
IA-4(6)	The organization coordinates with [Assignment: organization-defined external organizations] for cross-organization management of identifiers.
IA-4(8)	Generate pairwise pseudonymous identifiers.
IA-4(9)	Maintain the attributes for each uniquely identified individual, device, or service in [Assignment: organization-defined protected central storage].
IA-5	Manage system authenticators by:
IA-5a.	Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, service, or device receiving the authenticator;
IA-5b.	Establishing initial authenticator content for any authenticators issued by the organization;
IA-5c.	Ensuring that authenticators have sufficient strength of mechanism for their intended use;
IA-5d.	Establishing and implementing administrative procedures for initial authenticator distribution, for lost or compromised or damaged authenticators, and for revoking authenticators;
IA-5e.	Changing default authenticators prior to first use;

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
IA-5f.	Changing or refreshing authenticators [Assignment: organization-defined time period by authenticator type] or when [Assignment: organization-defined events] occur;
IA-5g.	Protecting authenticator content from unauthorized disclosure and modification;
IA-5i.	Changing authenticators for group or role accounts when membership to those accounts changes.
IA-5(1)	For password-based authentication:
IA-5(1)(a)	Maintain a list of commonly-used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;
IA-5(1)(b)	Verify, when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5(1)(a);
IA-5(1)(c)	Transmit passwords only over cryptographically-protected channels;
IA-5(1)(d)	Store passwords using an approved salted key derivation function, preferably using a keyed hash;
IA-5(1)(e)	Require immediate selection of a new password upon account recovery;
IA-5(1)(f)	Allow user selection of long passwords and passphrases, including spaces and all printable characters;
IA-5(1)(g)	Employ automated tools to assist the user in selecting strong password authenticators; and
IA-5(1)(h)	Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].
IA-5(2)(a)	For public key-based authentication:
IA-5(2)(a)(1)	Enforce authorized access to the corresponding private key; and
IA-5(2)(a)(2)	Map the authenticated identity to the account of the individual or group; and
IA-5(2)(b)	When public key infrastructure (PKI) is used:
IA-5(2)(b)(1)	Validate certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; and
IA-5(2)(b)(2)	Implement a local cache of revocation data to support path discovery and validation.
IA-5(5)	Require developers and installers of system components to provide unique authenticators or change default authenticators prior to delivery and installation.
IA-5(6)	Protect authenticators commensurate with the security category of the information to which use of the authenticator permits access.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
IA-5(7)	Ensure that unencrypted static authenticators are not embedded in applications or other forms of static storage.
IA-5(8)	Implement [Assignment: organization-defined security controls] to manage the risk of compromise due to individuals having accounts on multiple systems.
IA-5(9)	Use the following external organizations to federate credentials: [Assignment: organization-defined external organizations].
IA-5(10)	Bind identities and authenticators dynamically using the following rules: [Assignment: organization-defined binding rules].
IA-5(12)	For biometric-based authentication, employ mechanisms that satisfy the following biometric quality requirements [Assignment: organization-defined biometric quality requirements].
IA-5(13)	Prohibit the use of cached authenticators after [Assignment: organization-defined time period].
IA-5(14)	For PKI-based authentication, employ an organization-wide methodology for managing the content of PKI trust stores installed across all platforms, including networks, operating systems, browsers, and applications.
IA-5(15)	Use only General Services Administration-approved products and services for identity, credential, and access management.
IA-6	Obscure feedback of authentication information during the authentication process to protect the information from possible exploitation and use by unauthorized individuals.
IA-7	Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, executive orders, directives, policies, regulations, standards, and guidelines for such authentication.
IA-8	Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.
IA-8(1)	Accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies.
IA-8(2)(a)	Accept only external authenticators that are NIST-compliant; and
IA-8(2)(b)	Document and maintain a list of accepted external authenticators.
IA-8(4)	The information system conforms to FICAM-issued profiles.
IA-8(5)	The information system accepts and electronically verifies Personal Identity Verification-I (PIV-I) credentials.
IA-8(6)	Implement the following measures to disassociate user attributes or identifier assertion relationships among individuals, credential service providers, and relying parties: [Assignment: organization-defined measures].
IA-9	Uniquely identify and authenticate [Assignment: organization-defined system services and applications] before establishing communications with devices, users, or other services or applications.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
IA-10	Require individuals accessing the system to employ [Assignment: organization-defined supplemental authentication techniques or mechanisms] under specific [Assignment: organization-defined circumstances or situations].
IA-11	Require users to re-authenticate when [Assignment: organization-defined circumstances or situations requiring re-authentication].
IA-12(1)	Require that the registration process to receive an account for logical access includes supervisor or sponsor authorization.
IA-12(2)	Require evidence of individual identification be presented to the registration authority.
IA-12(4)	Require that the validation and verification of identity evidence be conducted in person before a designated registration authority.
IR-1a.	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
IR-1a.1(a)	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
IR-1a.1(b)	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
IR-1a.1.	[Selection (one or more): Organization-level; Mission/business process-level; System-level] incident response policy that:
IR-1a.2.	Procedures to facilitate the implementation of the incident response policy and the associated incident response controls;
IR-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the incident response policy and procedures; and
IR-1c.	Reviews and updates the current:
IR-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
IR-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
IR-2a.	Provide incident response training to system users consistent with assigned roles and responsibilities:
IR-2a.1.	Within [Assignment: organization-defined time period] of assuming an incident response role or responsibility or acquiring system access;
IR-2a.2.	When required by system changes; and
IR-2a.3.	[Assignment: organization-defined frequency] thereafter; and
IR-2b.	Review and update incident response training content [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
IR-2(1)	Incorporate simulated events into incident response training to facilitate the required response by personnel in crisis situations.
IR-2(2)	Provide an incident response training environment using [Assignment: organization-defined automated mechanisms].
IR-2(3)	Provide incident response training on how to identify and respond to a breach, including the organization's process for reporting a breach.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
IR-3	Test the effectiveness of the incident response capability for the system [Assignment: organization-defined frequency] using the following tests: [Assignment: organization-defined tests].
IR-3(1)	Test the incident response capability using [Assignment: organization-defined automated mechanisms].
IR-3(2)	Coordinate incident response testing with organizational elements responsible for related plans.
IR-4a.	Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery;
IR-4b.	Coordinate incident handling activities with contingency planning activities;
IR-4c.	Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly; and
IR-4d.	Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.
IR-4(1)	Support the incident handling process using [Assignment: organization-defined automated mechanisms].
IR-4(2)	Include the following types of dynamic reconfiguration for [Assignment: organization-defined system components] as part of the incident response capability: [Assignment: organization-defined types of dynamic reconfiguration].
IR-4(3)	Identify [Assignment: organization-defined classes of incidents] and take the following actions in response to those incidents to ensure continuation of organizational mission and business functions: [Assignment: organization-defined actions to take in response to classes of incidents].
IR-4(4)	Correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.
IR-4(5)	Implement a configurable capability to automatically disable the system if [Assignment: organization-defined security violations] are detected.
IR-4(6)	Implement an incident handling capability for incidents involving insider threats.
IR-4(7)	Coordinate an incident handling capability for insider threats that includes the following organizational entities [Assignment: organization-defined entities].
IR-4(8)	Coordinate with [Assignment: organization-defined external organizations] to correlate and share [Assignment: organization-defined incident information] to achieve a cross-organization perspective on incident awareness and more effective incident responses.
IR-4(9)	Employ [Assignment: organization-defined dynamic response capabilities] to respond to incidents.
IR-4(10)	Coordinate incident handling activities involving supply chain events with other organizations involved in the supply chain.
IR-5	Track and document incidents.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
IR-5(1)	Track incidents and collect and analyze incident information using [Assignment: organization-defined automated mechanisms].
IR-6a.	Require personnel to report suspected incidents to the organizational incident response capability within [Assignment: organization-defined time period]; and
IR-6b.	Report incident information to [Assignment: organization-defined authorities].
IR-6(1)	Report incidents using [Assignment: organization-defined automated mechanisms].
IR-6(2)	Report system vulnerabilities associated with reported incidents to [Assignment: organization-defined personnel or roles].
IR-6(3)	Provide incident information to the provider of the product or service and other organizations involved in the supply chain or supply chain governance for systems or system components related to the incident.
IR-7	Provide an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the system for the handling and reporting of incidents.
IR-7(1)	Increase the availability of incident response information and support using [Assignment: organization-defined automated mechanisms].
IR-7(2)(a)	Establish a direct, cooperative relationship between its incident response capability and external providers of system protection capability; and
IR-7(2)(b)	Identify organizational incident response team members to the external providers.
IR-8a.	Develop an incident response plan that:
IR-8a.1.	Provides the organization with a roadmap for implementing its incident response capability;
IR-8a.2.	Describes the structure and organization of the incident response capability;
IR-8a.3.	Provides a high-level approach for how the incident response capability fits into the overall organization;
IR-8a.4.	Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;
IR-8a.5.	Defines reportable incidents;
IR-8a.6.	Provides metrics for measuring the incident response capability within the organization;
IR-8a.7.	Defines the resources and management support needed to effectively maintain and mature an incident response capability;
IR-8a.8.	Addresses the sharing of incident information;
IR-8a.9.	Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and
IR-8a.10.	Explicitly designates responsibility for incident response to [Assignment: organization-defined entities, personnel, or roles].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
IR-8b.	Distribute copies of the incident response plan to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements];
IR-8c.	Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing;
IR-8d.	Communicate incident response plan changes to [Assignment: organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and
IR-8e.	Protect the incident response plan from unauthorized disclosure and modification.
IR-8(1)	Include the following in the Incident Response Plan for breaches involving personally identifiable information:
IR-8(1)a.	A process to determine if notice to individuals or other organizations, including oversight organizations, is needed;
IR-8(1)b.	An assessment process to determine the extent of the harm, embarrassment, inconvenience, or unfairness to affected individuals and any mechanisms to mitigate such harms; and
IR-8(1)c.	Identification of applicable privacy requirements.
IR-9	Respond to information spills by:
IR-9a.	Assigning [Assignment: organization-defined personnel or roles] with responsibility for responding to information spills;
IR-9b.	Identifying the specific information involved in the system contamination;
IR-9c.	Alerting [Assignment: organization-defined personnel or roles] of the information spill using a method of communication not associated with the spill;
IR-9d.	Isolating the contaminated system or system component;
IR-9e.	Eradicating the information from the contaminated system or component;
IR-9f.	Identifying other systems or system components that may have been subsequently contaminated; and
IR-9g.	Performing the following additional actions: [Assignment: organization-defined actions].
IR-9(2)	Provide information spillage response training [Assignment: organization-defined frequency].
IR-9(3)	Implement the following procedures to ensure that organizational personnel impacted by information spills can continue to carry out assigned tasks while contaminated systems are undergoing corrective actions: [Assignment: organization-defined procedures].
IR-9(4)	Employ the following controls for personnel exposed to information not within assigned access authorizations: [Assignment: organization-defined controls].
MA-1a.	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
MA-1a.1(a)	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
MA-1a.1(b)	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
MA-1a.2.	Procedures to facilitate the implementation of the maintenance policy and the associated maintenance controls;
MA-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the maintenance policy and procedures; and
MA-1c.	Review and update the current maintenance:
MA-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
MA-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
MA-2a.	Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements;
MA-2b.	Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location;
MA-2c.	Require that [Assignment: organization-defined personnel or roles] explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement;
MA-2d.	Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: [Assignment: organization-defined information];
MA-2e.	Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions; and
MA-2f.	Include the following information in organizational maintenance records: [Assignment: organization-defined information].
MA-2(2)(a)	Schedule, conduct, and document maintenance, repair, and replacement actions for the system using [Assignment: organization-defined automated mechanisms]; and
MA-2(2)(b)	Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.
MA-3a.	Approve, control, and monitor the use of system maintenance tools; and
MA-3b.	Review previously approved system maintenance tools [Assignment: organization-defined frequency].
MA-3(1)	Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.
MA-3(2)	Check media containing diagnostic and test programs for malicious code before the media are used in the system.
MA-3(3)	Prevent the removal of maintenance equipment containing organizational information by:

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
MA-3(3)(a)	Verifying that there is no organizational information contained on the equipment;
MA-3(3)(b)	Sanitizing or destroying the equipment;
MA-3(3)(c)	Retaining the equipment within the facility; or
MA-3(3)(d)	Obtaining an exemption from [Assignment: organization-defined personnel or roles] explicitly authorizing removal of the equipment from the facility.
MA-3(4)	Restrict the use of maintenance tools to authorized personnel only.
MA-3(5)	Monitor the use of maintenance tools that execute with increased privilege.
MA-3(6)	Inspect maintenance tools to ensure the latest software updates and patches are installed.
MA-4a.	Approve and monitor nonlocal maintenance and diagnostic activities;
MA-4b.	Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;
MA-4c.	Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;
MA-4d.	Maintain records for nonlocal maintenance and diagnostic activities; and
MA-4e.	Terminate session and network connections when nonlocal maintenance is completed.
MA-4(1)(a)	Log [Assignment: organization-defined audit events] for nonlocal maintenance and diagnostic sessions; and
MA-4(1)(b)	Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.
MA-4(3)(a)	Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or
MA-4(3)(b)	Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.
MA-4(4)	Protect nonlocal maintenance sessions by:
MA-4(4)(a)	Employing [Assignment: organization-defined authenticators that are replay resistant]; and
MA-4(4)(b)	Separating the maintenance sessions from other network sessions with the system by either:
MA-4(4)(b)(1)	Physically separated communications paths; or
MA-4(4)(b)(2)	Logically separated communications paths.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
MA-4(5)	The organization:
MA-4(5)(a)	Require the approval of each nonlocal maintenance session by [Assignment: organization-defined personnel or roles]; and
MA-4(5)(b)	Notify the following personnel or roles of the date and time of planned nonlocal maintenance: [Assignment: organization-defined personnel or roles].
MA-4(6)	Implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: [Assignment: organization-defined cryptographic mechanisms].
MA-4(7)	Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.
MA-5a.	Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;
MA-5b.	Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and
MA-5c.	Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.
MA-5(1)(a)	Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:
MA-5(1)(a)(1)	Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and
MA-5(1)(a)(2)	Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and
MA-5(1)(b)	Develop and implement [Assignment: organization-defined alternate controls] in the event a system component cannot be sanitized, removed, or disconnected from the system.
MA-5(2)	Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information possess security clearances and formal access approvals for at least the highest classification level and for compartments of information on the system.
MA-5(3)	Verify that personnel performing maintenance and diagnostic activities on a system processing, storing, or transmitting classified information are U.S. citizens.
MA-5(4)	Ensure that:
MA-5(4)(a)	Foreign nationals with appropriate security clearances are used to conduct maintenance and diagnostic activities on classified systems only when the systems are jointly owned and operated by the United States and foreign allied governments, or owned and operated solely by foreign allied governments; and

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
MA-5(4)(b)	Approvals, consents, and detailed operational conditions regarding the use of foreign nationals to conduct maintenance and diagnostic activities on classified systems are fully documented within Memoranda of Agreements.
MA-5(5)	Ensure that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.
MA-6	Obtain maintenance support and/or spare parts for [Assignment: organization-defined system components] within [Assignment: organization-defined time period] of failure.
MP-1a.	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
MP-1a.1.	[Selection (one or more): Organization-level; Mission/business process-level; System-level] media protection policy that:
MP-1a.1(a)	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
MP-1a.1(b)	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
MP-1a.2.	Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;
MP-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the media protection policy and procedures; and
MP-1c.	Review and update the current media protection:
MP-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
MP-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
MP-2	Restrict access to [Assignment: organization-defined types of digital and/or non-digital media] to [Assignment: organization-defined personnel or roles].
MP-3a.	Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
MP-3b.	Exempt [Assignment: organization-defined types of system media] from marking if the media remain within [Assignment: organization-defined controlled areas].
MP-4a.	Physically control and securely store [Assignment: organization-defined types of digital and/or non-digital media] within [Assignment: organization-defined controlled areas]; and
MP-4b.	Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
MP-4(2)	Restrict access to media storage areas and log access attempts and access granted using [Assignment: organization-defined automated mechanisms].
MP-5a.	Protect and control [Assignment: organization-defined types of system media] during transport outside of controlled areas using [Assignment: organization-defined controls];
MP-5b.	Maintain accountability for system media during transport outside of controlled areas;

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
MP-5c.	Document activities associated with the transport of system media; and
MP-5d.	Restrict the activities associated with the transport of system media to authorized personnel.
MP-5(3)	Employ an identified custodian during transport of system media outside of controlled areas.
MP-6a.	Sanitize [Assignment: organization-defined system media] prior to disposal, release out of organizational control, or release for reuse using [Assignment: organization-defined sanitization techniques and procedures]; and
MP-6b.	Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
MP-6(1)	Review, approve, track, document, and verify media sanitization and disposal actions.
MP-6(2)	Test sanitization equipment and procedures [Assignment: organization-defined frequency] to ensure that the intended sanitization is being achieved.
MP-6(3)	Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [Assignment: organization-defined circumstances requiring sanitization of portable storage devices].
MP-6(7)	Enforce dual authorization for the sanitization of [Assignment: organization-defined system media].
MP-6(8)	Provide the capability to purge or wipe information from [Assignment: organization-defined systems or system components] [Selection: remotely; under the following conditions: [Assignment: organization-defined conditions]].
MP-7(a)	[Selection: Restrict; Prohibit] the use of [Assignment: organization-defined types of system media] on [Assignment: organization-defined systems or system components] using [Assignment: organization-defined controls]; and
MP-7(b)	Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.
MP-7(2)	Prohibit the use of sanitization-resistant media in organizational systems.
MP-8a.	Establish [Assignment: organization-defined system media downgrading process] that includes employing downgrading mechanisms with strength and integrity commensurate with the security category or classification of the information;
MP-8b.	Verify that the system media downgrading process is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information;
MP-8c.	Identify [Assignment: organization-defined system media requiring downgrading]; and
MP-8d.	Downgrade the identified system media using the established process.
MP-8(1)	Document system media downgrading actions.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
MP-8(2)	Test downgrading equipment and procedures [Assignment: organization-defined frequency] to ensure that downgrading actions are being achieved.
MP-8(3)	Downgrade system media containing controlled unclassified information prior to public release.
MP-8(4)	Downgrade system media containing classified information prior to release to individuals without required access authorizations.
PE-1a.	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
PE-1a.1(a)	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
PE-1a.1(b)	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
PE-1a.1.	[Selection (one or more): Organization-level; Mission/business process-level; System-level] physical and environmental protection policy that:
PE-1a.2.	Procedures to facilitate the implementation of the physical and environmental protection policy and the associated physical and environmental protection controls;
PE-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the physical and environmental protection policy and procedures; and
PE-1c.	Review and update the current physical and environmental protection:
PE-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
PE-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
PE-2a.	Develop, approve, and maintain a list of individuals with authorized access to the facility where the system resides;
PE-2b.	Issue authorization credentials for facility access;
PE-2c.	Review the access list detailing authorized facility access by individuals [Assignment: organization-defined frequency]; and
PE-2d.	Remove individuals from the facility access list when access is no longer required.
PE-2(1)	Authorize physical access to the facility where the system resides based on position or role.
PE-2(2)	Require two forms of identification from the following forms of identification for visitor access to the facility where the system resides: [Assignment: organization-defined list of acceptable forms of identification].
PE-2(3)	Restrict unescorted access to the facility where the system resides to personnel with [Selection (one or more): security clearances for all information contained within the system; formal access authorizations for all information contained within the system; need for access to all information contained within the system; [Assignment: organization-defined physical access authorizations]].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
PE-3a.	Enforce physical access authorizations at [Assignment: organization-defined entry and exit points to the facility where the system resides] by:
PE-3a.1.	Verifying individual access authorizations before granting access to the facility; and
PE-3a.2.	Controlling ingress and egress to the facility using [Selection (one or more): [Assignment: organization-defined physical access control systems or devices]; guards];
PE-3b.	Maintain physical access audit logs for [Assignment: organization-defined entry or exit points];
PE-3c.	Control access to areas within the facility designated as publicly accessible by implementing the following controls: [Assignment: organization-defined physical access controls];
PE-3d.	Escort visitors and control visitor activity [Assignment: organization-defined circumstances requiring visitor escorts and control of visitor activity];
PE-3e.	Secure keys, combinations, and other physical access devices;
PE-3f.	Inventory [Assignment: organization-defined physical access devices] every [Assignment: organization-defined frequency]; and
PE-3g.	Change combinations and keys [Assignment: organization-defined frequency] and/or when keys are lost, combinations are compromised, or when individuals possessing the keys or combinations are transferred or terminated.
PE-3(1)	Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].
PE-3(2)	Perform security checks [Assignment: organization-defined frequency] at the physical perimeter of the facility or system for exfiltration of information or removal of system components.
PE-3(3)	Employ guards to control [Assignment: organization-defined physical access points] to the facility where the system resides 24 hours per day, 7 days per week.
PE-3(4)	Use lockable physical casings to protect [Assignment: organization-defined system components] from unauthorized physical access.
PE-3(5)	Employ [Assignment: organization-defined anti-tamper technologies] to [Selection (one or more): detect; prevent] physical tampering or alteration of [Assignment: organization-defined hardware components] within the system.
PE-3(7)	Limit access using physical barriers.
PE-3(8)	Employ access control vestibules at [Assignment: organization-defined locations within the facility].
PE-4	Control physical access to [Assignment: organization-defined system distribution and transmission lines] within organizational facilities using [Assignment: organization-defined security controls].
PE-5	Control physical access to output from [Assignment: organization-defined output devices] to prevent unauthorized individuals from obtaining the output.
PE-5(2)	Link individual identity to receipt of output from output devices.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
PE-6a.	Monitor physical access to the facility where the system resides to detect and respond to physical security incidents;
PE-6b.	Review physical access logs [Assignment: organization-defined frequency] and upon occurrence of [Assignment: organization-defined events or potential indications of events]; and
PE-6c.	Coordinate results of reviews and investigations with the organizational incident response capability.
PE-6(1)	Monitor physical access to the facility where the system resides using physical intrusion alarms and surveillance equipment.
PE-6(2)	Recognize [Assignment: organization-defined classes or types of intrusions] and initiate [Assignment: organization-defined response actions] using [Assignment: organization-defined automated mechanisms].
PE-6(3)(a)	Employ video surveillance of [Assignment: organization-defined operational areas];
PE-6(3)(b)	Review video recordings [Assignment: organization-defined frequency]; and
PE-6(3)(c)	Retain video recordings for [Assignment: organization-defined time period].
PE-6(4)	Monitor physical access to the system in addition to the physical access monitoring of the facility at [Assignment: organization-defined physical spaces containing one or more components of the system].
PE-8a.	Maintain visitor access records to the facility where the system resides for [Assignment: organization-defined time period];
PE-8b.	Review visitor access records [Assignment: organization-defined frequency]; and
PE-8c.	Report anomalies in visitor access records to [Assignment: organization-defined personnel].
PE-8(1)	Maintain and review visitor access records using [Assignment: organization-defined automated mechanisms].
PE-8(3)	Limit personally identifiable information contained in visitor access records to the following elements identified in the privacy risk assessment: [Assignment: organization-defined elements].
PE-16a.	Authorize and control [Assignment: organization-defined types of system components] entering and exiting the facility; and
PE-16b.	Maintain records of the system components.
PE-17a.	Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees;
PE-17b.	Employ the following controls at alternate work sites: [Assignment: organization-defined controls];
PE-17c.	Assess the effectiveness of controls at alternate work sites; and
PE-17d.	Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
PE-19	Protect the system from information leakage due to electromagnetic signals emanations.
PE-19(1)	Protect system components, associated data communications, and networks in accordance with national Emissions Security policies and procedures based on the security category or classification of the information.
PE-20	Employ [Assignment: organization-defined asset location technologies] to track and monitor the location and movement of [Assignment: organization-defined assets] within [Assignment: organization-defined controlled areas].
PE-22	Mark [Assignment: organization-defined system hardware components] indicating the impact level or classification level of the information permitted to be processed, stored, or transmitted by the hardware component.
PL-1a.	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
PL-1a.1.	[Selection (one or more): Organization-level; Mission/business process-level; System-level] planning policy that:
PL-1a.1.(a)	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
PL-1a.1.(b)	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
PL-1a.2.	Procedures to facilitate the implementation of the planning policy and the associated planning controls;
PL-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the planning policy and procedures; and
PL-1c.	Reviews and updates the current:
PL-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
PL-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
PL-2a.	Develop security and privacy plans for the system that:
PL-2a.1.	Are consistent with the organization’s enterprise architecture;
PL-2a.2.	Explicitly define the constituent system components;
PL-2a.3.	Describe the operational context of the system in terms of mission and business processes;
PL-2a.4.	Identify the individuals that fulfill system roles and responsibilities;
PL-2a.5.	Identify the information types processed, stored, and transmitted by the system;
PL-2a.6.	Provide the security categorization of the system, including supporting rationale;
PL-2a.7.	Describe any specific threats to the system that are of concern to the organization;

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
PL-2a.8.	Provide the results of a privacy risk assessment for systems processing personally identifiable information;
PL-2a.9.	Describe the operational environment for the system and any dependencies on or connections to other systems or system components;
PL-2a.10.	Provide an overview of the security and privacy requirements for the system;
PL-2a.11.	Identify any relevant control baselines or overlays, if applicable;
PL-2a.12.	Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
PL-2a.13.	Include risk determinations for security and privacy architecture and design decisions;
PL-2a.14.	Include security- and privacy-related activities affecting the system that require planning and coordination with [Assignment: organization-defined individuals or groups]; and
PL-2a.15.	Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.
PL-2b.	Distribute copies of the plans and communicate subsequent changes to the plans to [Assignment: organization-defined personnel or roles];
PL-2c.	Review the plans [Assignment: organization-defined frequency];
PL-2d.	Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments; and
PL-2e.	Protect the plans from unauthorized disclosure and modification.
PL-4a.	Establish and provide to individuals requiring access to the system, the rules that describe their responsibilities and expected behavior for information and system usage, security, and privacy;
PL-4b.	Receive a documented acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the system;
PL-4c.	Review and update the rules of behavior [Assignment: organization-defined frequency]; and
PL-4d.	Require individuals who have acknowledged a previous version of the rules of behavior to read and re-acknowledge [Selection (one or more): [Assignment: organization-defined frequency]; when the rules are revised or updated].
PL-4 (1)	Include in the rules of behavior, restrictions on: (a) Use of social media, social networking sites, and external sites/applications; (b) Posting organizational information on public websites; and (c) Use of organization-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.
PL-7a.	Develop a Concept of Operations (CONOPS) for the system describing how the organization intends to operate the system from the perspective of information security and privacy; and
PL-7b.	Review and update the CONOPS [Assignment: organization-defined frequency].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
PL-8a.	Develop security and privacy architectures for the system that:
PL-8a.1.	Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information;
PL-8a.2.	Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals;
PL-8a.3.	Describe how the architectures are integrated into and support the enterprise architecture; and
PL-8a.4.	Describe any assumptions about, and dependencies on, external systems and services;
PL-8b.	Review and update the architectures [Assignment: organization-defined frequency] to reflect changes in the enterprise architecture; and
PL-8c.	Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions.
PL-8(1)	Design the security and privacy architectures for the system using a defense-in-depth approach that:
PL-8(1)(a)	Allocates [Assignment: organization-defined controls] to [Assignment: organization-defined locations and architectural layers]; and
PL-8(1)(b)	Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.
PL-8(2)	Require that [Assignment: organization-defined controls] allocated to [Assignment: organization-defined locations and architectural layers] are obtained from different suppliers.
PL-9	Centrally manage [Assignment: organization-defined controls and related processes].
PM-1a.	Develop and disseminate an organization-wide information security program plan that:
PM-1a.1.	Provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements;
PM-1a.2.	Includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance;
PM-1a.3.	Reflects the coordination among organizational entities responsible for information security; and
PM-1a.4.	Is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;
PM-1b.	Review and update the organization-wide information security program plan [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
PM-1c.	Protect the information security program plan from unauthorized disclosure and modification.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
PM-2	Appoint a senior agency information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program.
PM-3a.	Include the resources needed to implement the information security and privacy programs in capital planning and investment requests and document all exceptions to this requirement;
PM-3b.	Prepare documentation required for addressing information security and privacy programs in capital planning and investment requests in accordance with applicable laws, executive orders, directives, policies, regulations, standards; and
PM-3c.	Make available for expenditure, the planned information security and privacy resources.
PM-4a.	Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems:
PM-4a.1.	Are developed and maintained;
PM-4a.2.	Document the remedial information security, privacy, and supply chain risk management actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and
PM-4a.3.	Are reported in accordance with established reporting requirements.
PM-4b.	Review plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
PM-5	Develop and update [Assignment: organization-defined frequency] an inventory of organizational systems.
PM-5(1)	Establish, maintain, and update [Assignment: organization-defined frequency] an inventory of all systems, applications, and projects that process personally identifiable information.
PM-6	Develop, monitor, and report on the results of information security and privacy measures of performance.
PM-7	Develop and maintain an enterprise architecture with consideration for information security, privacy, and the resulting risk to organizational operations and assets, individuals, other organizations, and the Nation.
PM-7(1)	Offload [Assignment: organization-defined non-essential functions or services] to other systems, system components, or an external provider.
PM-8	Address information security and privacy issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.
PM-9a.	Develops a comprehensive strategy to manage:
PM-9a.1	Security risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of organizational systems; and
PM-9a.2	Privacy risk to individuals resulting from the authorized processing of personally identifiable information;

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
PM-9b.	Implements the risk management strategy consistently across the organization; and
PM-9c.	Reviews and updates the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes.
PM-10a.	Manage the security and privacy state of organizational systems and the environments in which those systems operate through authorization processes;
PM-10b.	Designate individuals to fulfill specific roles and responsibilities within the organizational risk management process; and
PM-10c.	Integrate the authorization processes into an organization-wide risk management program.
PM-11a.	Define organizational mission and business processes with consideration for information security and privacy and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and
PM-11b.	Determine information protection and personally identifiable information processing needs arising from the defined mission and business processes; and
PM-11c.	Review and revise the mission and business processes [Assignment: organization-defined frequency].
PM-12	Implement an insider threat program that includes a cross-discipline insider threat incident handling team.
PM-13	Establish a security and privacy workforce development and improvement program.
PM-14a.	Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems:
PM-14a.1.	Are developed and maintained; and
PM-14a.2.	Continue to be executed; and
PM-14b.	Review testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.
PM-15	The organization establishes and institutionalizes contact with selected groups and associations within the security community:
PM-15a.	To facilitate ongoing security education and training for organizational personnel;
PM-15b.	To maintain currency with recommended security practices, techniques, and technologies; and
PM-15c.	To share current security-related information including threats, vulnerabilities, and incidents.
PM-16	Implement a threat awareness program that includes a cross-organization information-sharing capability for threat intelligence.
PS-1a.	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
PS-1a.1.	[Selection (one or more): Organization-level; Mission/business process-level; System-level] personnel security policy that:
PS-1a.1.(a)	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
PS-1a.1.(b)	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
PS-1a.2.	Procedures to facilitate the implementation of the personnel security policy and the associated personnel security controls;
PS-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the personnel security policy and procedures; and
PS-1c.	Review and update the current personnel security:
PS-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
PS-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
PS-2a.	Assign a risk designation to all organizational positions;
PS-2b.	Establish screening criteria for individuals filling those positions; and
PS-2c.	Review and update position risk designations [Assignment: organization-defined frequency].
PS-3a.	Screen individuals prior to authorizing access to the system; and
PS-3b.	Rescreen individuals in accordance with [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of rescreening].
PS-3(1)	Verify that individuals accessing a system processing, storing, or transmitting classified information are cleared and indoctrinated to the highest classification level of the information to which they have access on the system.
PS-3(2)	Verify that individuals accessing a system processing, storing, or transmitting types of classified information that require formal indoctrination, are formally indoctrinated for all the relevant types of information to which they have access on the system.
PS-3(3)	Verify that individuals accessing a system processing, storing, or transmitting information requiring special protection:
PS-3(3)(a)	Have valid access authorizations that are demonstrated by assigned official government duties; and
PS-3(3)(b)	Satisfy [Assignment: organization-defined additional personnel screening criteria].
PS-3(4)	Verify that individuals accessing a system processing, storing, or transmitting [Assignment: organization-defined information types] meet [Assignment: organization-defined citizenship requirements].
PS-4	Upon termination of individual employment:
PS-4a.	Disable system access within [Assignment: organization-defined time period];
PS-4b.	Upon Termination of individual employment: Terminate or revoke any authenticators and credentials associated with the individual;

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
PS-4c.	Conduct exit interviews that include a discussion of [Assignment: organization-defined information security topics];
PS-4d.	Retrieve all security-related organizational system-related property; and
PS-4e.	Retain access to organizational information and systems formerly controlled by terminated individual.
PS-4(1)(a)	Notify terminated individuals of applicable, legally binding post-employment requirements for the protection of organizational information; and
PS-4(1)(b)	Require terminated individuals to sign an acknowledgment of post-employment requirements as part of the organizational termination process.
PS-4(2)	Use [Assignment: organization-defined automated mechanisms] to [Selection (one or more): notify [Assignment: organization-defined personnel or roles] of individual termination actions; disable access to system resources].
PS-5a.	Review and confirm ongoing operational need for current logical and physical access authorizations to systems and facilities when individuals are reassigned or transferred to other positions within the organization;
PS-5b.	Initiate [Assignment: organization-defined transfer or reassignment actions] within [Assignment: organization-defined time period following the formal transfer action];
PS-5c.	Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer; and
PS-5d.	Notify [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period].
PS-6a.	Develop and document access agreements for organizational systems;
PS-6b.	Review and update the access agreements [Assignment: organization-defined frequency]; and
PS-6c.	Verify that individuals requiring access to organizational information and systems:
PS-6c.1.	Sign appropriate access agreements prior to being granted access; and
PS-6c.2.	Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [Assignment: organization-defined frequency].
PS-6(2)	Verify that access to classified information requiring special protection is granted only to individuals who:
PS-6(2)(a)	Have a valid access authorization that is demonstrated by assigned official government duties;
PS-6(2)(b)	Satisfy associated personnel security criteria; and
PS-6(2)(c)	Have read, understood, and signed a nondisclosure agreement.
PS-6(3)(a)	Notify individuals of applicable, legally binding post-employment requirements for protection of organizational information; and
PS-6(3)(b)	Require individuals to sign an acknowledgment of these requirements, if applicable, as part of granting initial access to covered information.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
PS-7a.	Establish personnel security requirements, including security roles and responsibilities for external providers;
PS-7b.	Require external providers to comply with personnel security policies and procedures established by the organization;
PS-7c.	Document personnel security requirements;
PS-7d.	Require external providers to notify [Assignment: organization-defined personnel or roles] of any personnel transfers or terminations of external personnel who possess organizational credentials and/or badges, or who have system privileges within [Assignment: organization-defined time period]; and
PS-7e.	Monitor provider compliance with personnel security requirements.
PS-8a.	Employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and
PS-8b.	Notifies [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction.
RA-1a	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
RA-1a.1.	[Selection (one or more): Organization-level; Mission/business process-level; System-level] risk assessment policy that:
RA-1a.1.a.	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
RA-1a.1.b.	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
RA-1a.2	Procedures to facilitate the implementation of the risk assessment policy and the associated risk assessment controls;
RA-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the risk assessment policy and procedures; and
RA-1c.	Review and update the current risk assessment:
RA-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
RA-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
RA-2a.	Categorize the system and information it processes, stores, and transmits;
RA-2b.	Document the security categorization results, including supporting rationale, in the security plan for the system; and
RA-2c.	Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.
RA-2(1)	Conduct an impact-level prioritization of organizational systems to obtain additional granularity on system impact levels.
RA-3a.	Conduct a risk assessment, including:

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
RA-3a.1	Identifying threats to and vulnerabilities in the system;
RA-3a.2	Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and
RA-3a.3	Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information;
RA-3b.	Integrate risk assessment results and risk management decisions from the organization and mission or business process perspectives with system-level risk assessments;
RA-3c.	Document risk assessment results in [Selection: security and privacy plans; risk assessment report; [Assignment: organization-defined document]];
RA-3d.	Review risk assessment results [Assignment: organization-defined frequency];
RA-3e.	Disseminate risk assessment results to [Assignment: organization-defined personnel or roles]; and
RA-3f.	Update the risk assessment [Assignment: organization-defined frequency] or when there are significant changes to the system, its environment of operation, or other conditions that may impact the security or privacy state of the system.
RA-3(2)	Use all-source intelligence to assist in the analysis of risk.
RA-5a.	Monitor and scan for vulnerabilities in the system and hosted applications [Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process] and when new vulnerabilities potentially affecting the system are identified and reported;
RA-5b.	Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
RA-5b.1.	Enumerating platforms, software flaws, and improper configurations;
RA-5b.2.	Formatting checklists and test procedures; and
RA-5b.3.	Measuring vulnerability impact;
RA-5c.	Analyze vulnerability scan reports and results from vulnerability monitoring;
RA-5d.	Remediate legitimate vulnerabilities [Assignment: organization-defined response times] in accordance with an organizational assessment of risk;
RA-5e.	Share information obtained from the vulnerability monitoring process and control assessments with [Assignment: organization-defined personnel or roles] to help eliminate similar vulnerabilities in other systems; and
RA-5f.	Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.
RA-5(2)	Update the system vulnerabilities to be scanned [Selection (one or more): [Assignment: organization-defined frequency]; prior to a new scan; when new vulnerabilities are identified and reported].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
RA-5(3)	Define the breadth and depth of vulnerability scanning coverage.
RA-5(4)	Determine information about the system that is discoverable and take [Assignment: organization-defined corrective actions].
RA-5(5)	Implement privileged access authorization to [Assignment: organization-defined system components] for [Assignment: organization-defined vulnerability scanning activities].
RA-5(6)	Compare the results of multiple vulnerability scans using [Assignment: organization-defined automated mechanisms].
RA-5(8)	Review historic audit logs to determine if a vulnerability identified in a [Assignment: organization-defined system] has been previously exploited within an [Assignment: organization-defined time period].
RA-5(10)	Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors.
RA-5(11)	Establish a public reporting channel for receiving reports of vulnerabilities in organizational systems and system components.
RA-6	Employ a technical surveillance countermeasures survey at [Assignment: organization-defined locations] [Selection (one or more): [Assignment: organization-defined frequency]; when the following events or indicators occur: [Assignment: organization-defined events or indicators]].
RA-9	Identify critical system components and functions by performing a criticality analysis for [Assignment: organization-defined systems, system components, or system services] at [Assignment: organization-defined decision points in the system development life cycle].
SA-1a.	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
SA-1a.1.	[Selection (one or more): Organization-level; Mission/business process-level; System-level] system and services acquisition policy that:
SA-1a.1.(a)	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
SA-1a.1.(b)	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
SA-1a.2.	Procedures to facilitate the implementation of the system and services acquisition policy and the associated system and services acquisition controls;
SA-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures; and
SA-1c.	Review and update the current system and services acquisition:
SA-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
SA-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
SA-2a.	Determine the high-level information security and privacy requirements for the system or system service in mission and business process planning;

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SA-2b.	Determine, document, and allocate the resources required to protect the system or system service as part of the organizational capital planning and investment control process; and
SA-2c.	Establish a discrete line item for information security and privacy in organizational programming and budgeting documentation.
SA-3a.	Acquire, develop, and manage the system using [Assignment: organization-defined system development life cycle] that incorporates information security and privacy considerations;
SA-3b.	Define and document information security and privacy roles and responsibilities throughout the system development life cycle;
SA-3c.	Identify individuals having information security and privacy roles and responsibilities; and
SA-3d.	Integrate the organizational information security and privacy risk management process into system development life cycle activities.
SA-3(1)	Protect system preproduction environments commensurate with risk throughout the system development life cycle for the system, system component, or system service.
SA-3(2)(a)	Approve, document, and control the use of live data in preproduction environments for the system, system component, or system service; and
SA-3(2)(b)	Protect preproduction environments for the system, system component, or system service at the same impact or classification level as any live data in use within the preproduction environments.
SA-3(3)	Plan for and implement a technology refresh schedule for the system throughout the system development life cycle.
SA-4	Include the following requirements, descriptions, and criteria, explicitly or by reference, using [Selection (one or more): standardized contract language; [Assignment: organization-defined contract language]] in the acquisition contract for the system, system component, or system service:
SA-4a.	Security and privacy functional requirements;
SA-4b.	Strength of mechanism requirements;
SA-4c.	Security and privacy assurance requirements;
SA-4d.	Controls needed to satisfy the security and privacy requirements.
SA-4e.	Security and privacy documentation requirements;
SA-4f.	Requirements for protecting security and privacy documentation;
SA-4g.	Description of the system development environment and environment in which the system is intended to operate;
SA-4h.	Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management; and
SA-4i.	Acceptance criteria.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SA-4(1)	Require the developer of the system, system component, or system service to provide a description of the functional properties of the controls to be implemented.
SA-4(2)	Require the developer of the system, system component, or system service to provide design and implementation information for the controls that includes: [Selection (one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [Assignment: organization-defined design and implementation information]] at [Assignment: organization-defined level of detail].
SA-4(3)	Require the developer of the system, system component, or system service to demonstrate the use of a system development life cycle process that includes:
SA-4(3)(a)	[Assignment: organization-defined systems engineering methods];
SA-4(3)(b)	<assign:#>organization-defined [Selection (one or more): systems security; privacy<#:assign> engineering methods]; and
SA-4(3)(c)	[Assignment: organization-defined software development methods; testing, evaluation, assessment, verification, and validation methods; and quality control processes].
SA-4(5)	Require the developer of the system, system component, or system service to:
SA-4(5)(a)	Deliver the system, component, or service with [Assignment: organization-defined security configurations] implemented; and
SA-4(5)(b)	Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.
SA-4(6)(a)	Employ only government off-the-shelf or commercial off-the-shelf information assurance and information assurance-enabled information technology products that compose an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and
SA-4(6)(b)	Ensure that these products have been evaluated and/or validated by NSA or in accordance with NSA-approved procedures.
SA-4(7)(a)	Limit the use of commercially provided information assurance and information assurance-enabled information technology products to those products that have been successfully evaluated against a National Information Assurance partnership (NIAP)-approved Protection Profile for a specific technology type, if such a profile exists; and
SA-4(7)(b)	Require, if no NIAP-approved Protection Profile exists for a specific technology type but a commercially provided information technology product relies on cryptographic functionality to enforce its security policy, that the cryptographic module is FIPS-validated or NSA-approved.
SA-4(8)	Require the developer of the system, system component, or system service to produce a plan for continuous monitoring of control effectiveness that is consistent with the continuous monitoring program of the organization.
SA-4(9)	Require the developer of the system, system component, or system service to identify the functions, ports, protocols, and services intended for organizational use.
SA-4(10)	Employ only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational systems.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SA-5a.	Obtain or develop administrator documentation for the system, system component, or system service that describes:
SA-5a.1.	Secure configuration, installation, and operation of the system, component, or service;
SA-5a.2.	Effective use and maintenance of security and privacy functions and mechanisms; and
SA-5a.3.	Known vulnerabilities regarding configuration and use of administrative or privileged functions;
SA-5b.	Obtain or develop user documentation for the system, system component, or system service that describes:
SA-5b.1.	User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms;
SA-5b.2.	Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and
SA-5b.3.	User responsibilities in maintaining the security of the system, component, or service and privacy of individuals;
SA-5c.	Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take [Assignment: organization-defined actions] in response; and
SA-5d.	Distribute documentation to [Assignment: organization-defined personnel or roles].
SA-8	Apply the following systems security and privacy engineering principles in the specification, design, development, implementation, and modification of the system and system components: [Assignment: organization-defined systems security and privacy engineering principles].
SA-8(1)	Implement the security design principle of clear abstractions.
SA-8(2)	Implement the security design principle of least common mechanism in [Assignment: organization-defined systems or system components].
SA-8(3)	Implement the security design principles of modularity and layering in [Assignment: organization-defined systems or system components].
SA-8(4)	Implement the security design principle of partially ordered dependencies in [Assignment: organization-defined systems or system components].
SA-8(5)	Implement the security design principle of efficiently mediated access in [Assignment: organization-defined systems or system components].
SA-8(6)	Implement the security design principle of minimized sharing in [Assignment: organization-defined systems or system components].
SA-8(7)	Implement the security design principle of reduced complexity in [Assignment: organization-defined systems or system components].
SA-8(8)	Implement the security design principle of secure evolvability in [Assignment: organization-defined systems or system components].
SA-8(9)	Implement the security design principle of trusted components in [Assignment: organization-defined systems or system components].
SA-8(10)	Implement the security design principle of hierarchical trust in [Assignment: organization-defined systems or system components].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SA-8(11)	Implement the security design principle of inverse modification threshold in [Assignment: organization-defined systems or system components].
SA-8(12)	Implement the security design principle of hierarchical protection in [Assignment: organization-defined systems or system components].
SA-8(13)	Implement the security design principle of minimized security elements in [Assignment: organization-defined systems or system components].
SA-8(14)	Implement the security design principle of least privilege in [Assignment: organization-defined systems or system components].
SA-8(15)	Implement the security design principle of predicate permission in [Assignment: organization-defined systems or system components].
SA-8(16)	Implement the security design principle of self-reliant trustworthiness in [Assignment: organization-defined systems or system components].
SA-8(17)	Implement the security design principle of secure distributed composition in [Assignment: organization-defined systems or system components].
SA-8(18)	Implement the security design principle of trusted communications channels in [Assignment: organization-defined systems or system components].
SA-8(19)	Implement the security design principle of continuous protection in [Assignment: organization-defined systems or system components].
SA-8(20)	Implement the security design principle of secure metadata management in [Assignment: organization-defined systems or system components].
SA-8(21)	Implement the security design principle of self-analysis in [Assignment: organization-defined systems or system components].
SA-8(22)	Implement the security design principle of accountability and traceability in [Assignment: organization-defined systems or system components].
SA-8(23)	Implement the security design principle of secure defaults in [Assignment: organization-defined systems or system components].
SA-8(24)	Implement the security design principle of secure failure and recovery in [Assignment: organization-defined systems or system components].
SA-8(25)	Implement the security design principle of economic security in [Assignment: organization-defined systems or system components].
SA-8(26)	Implement the security design principle of performance security in [Assignment: organization-defined systems or system components].
SA-8(27)	Implement the security design principle of human factored security in [Assignment: organization-defined systems or system components].
SA-8(28)	Implement the security design principle of acceptable security in [Assignment: organization-defined systems or system components].
SA-8(29)	Implement the security design principle of repeatable and documented procedures in [Assignment: organization-defined systems or system components].
SA-8(30)	Implement the security design principle of procedural rigor in [Assignment: organization-defined systems or system components].
SA-8(31)	Implement the security design principle of secure system modification in [Assignment: organization-defined systems or system components].
SA-8(32)	Implement the security design principle of sufficient documentation in [Assignment: organization-defined systems or system components].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SA-8(33)	Implement the privacy principle of minimization using [Assignment: organization-defined processes].
SA-9a.	Require that providers of external system services comply with organizational security and privacy requirements and employ the following controls: [Assignment: organization-defined controls];
SA-9b.	Define and document organizational oversight and user roles and responsibilities with regard to external system services; and
SA-9c.	Employ the following processes, methods, and techniques to monitor control compliance by external service providers on an ongoing basis: [Assignment: organization-defined processes, methods, and techniques].
SA-9(1)(a)	Conduct an organizational assessment of risk prior to the acquisition or outsourcing of information security services; and
SA-9(1)(b)	Verify that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined personnel or roles].
SA-9(2)	Require providers of the following external system services to identify the functions, ports, protocols, and other services required for the use of such services: [Assignment: organization-defined external system services].
SA-9(3)	Establish, document, and maintain trust relationships with external service providers based on the following requirements, properties, factors, or conditions: [Assignment: organization-defined security and privacy requirements, properties, factors, or conditions defining acceptable trust relationships].
SA-9(4)	Take the following actions to verify that the interests of [Assignment: organization-defined external service providers] are consistent with and reflect organizational interests: [Assignment: organization-defined actions].
SA-9(5)	Restrict the location of [Selection (one or more): information processing; information or data; system services] to [Assignment: organization-defined locations] based on [Assignment: organization-defined requirements or conditions].
SA-9(6)	Maintain exclusive control of cryptographic keys for encrypted material stored or transmitted through an external system.
SA-9(7)	Provide the capability to check the integrity of information while it resides in the external system.
SA-9(8)	Restrict the geographic location of information processing and data storage to facilities located within in the legal jurisdictional boundary of the United States.
SA-10	Require the developer of the system, system component, or system service to:
SA-10a.	Perform configuration management during system, component, or service [Selection (one or more): design; development; implementation; operation; disposal];
SA-10b.	Document, manage, and control the integrity of changes to [Assignment: organization-defined configuration items under configuration management];
SA-10c.	Implement only organization-approved changes to the system, component, or service;
SA-10d.	Document approved changes to the system, component, or service and the potential security and privacy impacts of such changes; and

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SA-10e.	Track security flaws and flaw resolution within the system, component, or service and report findings to [Assignment: organization-defined personnel].
SA-10(1)	Require the developer of the system, system component, or system service to enable integrity verification of software and firmware components.
SA-10(2)	Provide an alternate configuration management process using organizational personnel in the absence of a dedicated developer configuration management team.
SA-10(3)	Require the developer of the system, system component, or system service to enable integrity verification of hardware components.
SA-10(4)	Require the developer of the system, system component, or system service to employ tools for comparing newly generated versions of security-relevant hardware descriptions, source code, and object code with previous versions.
SA-10(5)	Require the developer of the system, system component, or system service to maintain the integrity of the mapping between the master build data describing the current version of security-relevant hardware, software, and firmware and the on-site master copy of the data for the current version.
SA-10(6)	Require the developer of the system, system component, or system service to execute procedures for ensuring that security-relevant hardware, software, and firmware updates distributed to the organization are exactly as specified by the master copies.
SA-10(7)	Require [Assignment: organization-defined security and privacy representatives] to be included in the [Assignment: organization-defined configuration change management and control process].
SA-11	Require the developer of the system, system component, or system service, at all post-design stages of the system development life cycle, to:
SA-11a.	Develop and implement a plan for ongoing security and privacy control assessments;
SA-11b.	Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation [Assignment: organization-defined frequency] at [Assignment: organization-defined depth and coverage];
SA-11c.	Produce evidence of the execution of the assessment plan and the results of the testing and evaluation;
SA-11d.	Implement a verifiable flaw remediation process; and
SA-11e.	Correct flaws identified during testing and evaluation.
SA-11(1)	Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis.
SA-11(2)	Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that:
SA-11(2)(a)	Uses the following contextual information: [Assignment: organization-defined information concerning impact, environment of operations, known or assumed threats, and acceptable risk levels];

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SA-11(2)(b)	Employs the following tools and methods: [Assignment: organization-defined tools and methods];
SA-11(2)(c)	Conducts the modeling and analyses at the following level of rigor: [Assignment: organization-defined breadth and depth of modeling and analyses]; and
SA-11(2)(d)	Produces evidence that meets the following acceptance criteria: [Assignment: organization-defined acceptance criteria].
SA-11(3)(a)	Require an independent agent satisfying [Assignment: organization-defined independence criteria] to verify the correct implementation of the developer security and privacy assessment plans and the evidence produced during testing and evaluation; and
SA-11(3)(b)	Verify that the independent agent is provided with sufficient information to complete the verification process or granted the authority to obtain such information.
SA-11(4)	Require the developer of the system, system component, or system service to perform a manual code review of [Assignment: organization-defined specific code] using the following processes, procedures, and/or techniques: [Assignment: organization-defined processes, procedures, and/or techniques].
SA-11(5)	Require the developer of the system, system component, or system service to perform penetration testing:
SA-11(5)(a)	At the following level of rigor: [Assignment: organization-defined breadth and depth of testing]; and
SA-11(5)(b)	Under the following constraints: [Assignment: organization-defined constraints].
SA-11(6)	Require the developer of the system, system component, or system service to perform attack surface reviews.
SA-11(7)	Require the developer of the system, system component, or system service to verify that the scope of testing and evaluation provides complete coverage of the required controls at the following level of rigor: [Assignment: organization-defined breadth and depth of testing and evaluation].
SA-11(8)	Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis.
SA-11(9)	Require the developer of the system, system component, or system service to employ interactive application security testing tools to identify flaws and document the results.
SA-15a.	Require the developer of the system, system component, or system service to follow a documented development process that:
SA-15a.1.	Explicitly addresses security and privacy requirements;
SA-15a.2.	Identifies the standards and tools used in the development process;
SA-15a.3.	Documents the specific tool options and tool configurations used in the development process; and
SA-15a.4.	Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SA-15b.	Review the development process, standards, tools, tool options, and tool configurations [Assignment: organization-defined frequency] to determine if the process, standards, tools, tool options and tool configurations selected and employed can satisfy the following security and privacy requirements: [Assignment: organization-defined security and privacy requirements].
SA-15(1)	Require the developer of the system, system component, or system service to:
SA-15(1)(a)	(a) Define quality metrics at the beginning of the development process; and
SA-15(1)(b)	(b) Provide evidence of meeting the quality metrics [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined program review milestones]; upon delivery].
SA-15(2)	Require the developer of the system, system component, or system service to select and employ security and privacy tracking tools for use during the development process.
SA-15(3)	Require the developer of the system, system component, or system service to:
SA-15(3)(a)	Define quality metrics at the beginning of the development process; and
SA-15(3)(b)	Provide evidence of meeting the quality metrics [Selection (one or more): [Assignment: organization-defined frequency]; [Assignment: organization-defined program review milestones]; upon delivery].
SA-15(5)	Require the developer of the system, system component, or system service to reduce attack surfaces to [Assignment: organization-defined thresholds].
SA-15(6)	Require the developer of the system, system component, or system service to implement an explicit process to continuously improve the development process.
SA-15(7)	Require the developer of the system, system component, or system service [Assignment: organization-defined frequency] to:
SA-15(7)(a)	Perform an automated vulnerability analysis using [Assignment: organization-defined tools];
SA-15(7)(b)	Determine the exploitation potential for discovered vulnerabilities;
SA-15(7)(c)	Determine potential risk mitigations for delivered vulnerabilities; and
SA-15(7)(d)	Deliver the outputs of the tools and results of the analysis to [Assignment: organization-defined personnel or roles].
SA-15 (8)	Require the developer of the system, system component, or system service to use threat modeling and vulnerability analyses from similar systems, components, or services to inform the current development process.
SA-15(10)	Require the developer of the system, system component, or system service to provide, implement, and test an incident response plan.
SA-15(11)	Require the developer of the system or system component to archive the system or component to be released or delivered together with the corresponding evidence supporting the final security and privacy review.
SA-15(12)	Require the developer of the system or system component to minimize the use of personally identifiable information in development and test environments.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SA-16	Require the developer of the system, system component, or system service to provide the following training on the correct use and operation of the implemented security and privacy functions, controls, and/or mechanisms: [Assignment: organization-defined training].
SA-17	Require the developer of the system, system component, or system service to produce a design specification and security and privacy architecture that:
SA-17a.	Is consistent with the organization's security and privacy architecture that is an integral part the organization's enterprise architecture;
SA-17b.	Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components; and
SA-17c.	Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities and a unified approach to protection.
SA-17(1)	Require the developer of the system, system component, or system service to:
SA-17(1)(a)	Produce, as an integral part of the development process, a formal policy model describing the [Assignment: organization-defined elements of organizational security and privacy policy] to be enforced; and
SA-17(1)(b)	Prove that the formal policy model is internally consistent and sufficient to enforce the defined elements of the organizational security and privacy policy when implemented.
SA-17(2)	Require the developer of the system, system component, or system service to:
SA-17(2)(a)	Define security-relevant hardware, software, and firmware; and
SA-17(2)(b)	Provide a rationale that the definition for security-relevant hardware, software, and firmware is complete.
SA-17(3)	Require the developer of the system, system component, or system service to:
SA-17(3)(a)	Produce, as an integral part of the development process, a formal top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;
SA-17(3)(b)	Show via proof to the extent feasible with additional informal demonstration as necessary, that the formal top-level specification is consistent with the formal policy model;
SA-17(3)(c)	Show via informal demonstration, that the formal top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;
SA-17(3)(d)	Show that the formal top-level specification is an accurate description of the implemented security-relevant hardware, software, and firmware; and
SA-17(3)(e)	Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the formal top-level specification but strictly internal to the security-relevant hardware, software, and firmware.
SA-17(4)	Require the developer of the system, system component, or system service to:
SA-17(4)(a)	(Produce, as an integral part of the development process, an informal descriptive top-level specification that specifies the interfaces to security-relevant hardware, software, and firmware in terms of exceptions, error messages, and effects;

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SA-17(4)(b)	Show via [Selection: informal demonstration; convincing argument with formal methods as feasible] that the descriptive top-level specification is consistent with the formal policy model;
SA-17(4)(c)	Show via informal demonstration, that the descriptive top-level specification completely covers the interfaces to security-relevant hardware, software, and firmware;
SA-17(4)(d)	Show that the descriptive top-level specification is an accurate description of the interfaces to security-relevant hardware, software, and firmware; and
SA-17(4)(e)	Describe the security-relevant hardware, software, and firmware mechanisms not addressed in the descriptive top-level specification but strictly internal to the security-relevant hardware, software, and firmware.
SA-17(5)	Require the developer of the system, system component, or system service to:
SA-17(5)(a)	Design and structure the security-relevant hardware, software, and firmware to use a complete, conceptually simple protection mechanism with precisely defined semantics; and
SA-17(5)(b)	Internally structure the security-relevant hardware, software, and firmware with specific regard for this mechanism.
SA-17(6)	Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate testing.
SA-17(7)	Require the developer of the system, system component, or system service to structure security-relevant hardware, software, and firmware to facilitate controlling access with least privilege.
SA-21	Require that the developer of [Assignment: organization-defined system, system component, or system service]:
SA-21a.	Has appropriate access authorizations as determined by assigned [Assignment: organization-defined official government duties]; and
SA-21b.	Satisfies the following additional personnel screening criteria: [Assignment: organization-defined additional personnel screening criteria].
SA-22a.	Replace system components when support for the components is no longer available from the developer, vendor, or manufacturer; or
SA-22b.	Provide the following options for alternative sources for continued support for unsupported components [Selection (one or more): in-house support; [Assignment: organization-defined support from external providers]].
SC-1a.	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
SC-1a.1.	[Selection (one or more): Organization-level; Mission/business process-level; System-level] system and communications protection policy that:
SC-1a.1.(a)	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
SC-1a.1.(b)	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
SC-1a.2.	Procedures to facilitate the implementation of the system and communications protection policy and the associated system and communications protection controls;

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SC-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and communications protection policy and procedures; and
SC-1c.	Review and update the current system and communications protection:
SC-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
SC-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].
SC-2	Separate user functionality, including user interface services, from system management functionality.
SC-2(1)	Prevent the presentation of system management functionality at interfaces to non-privileged users.
SC-2(2)	Store state information from applications and software separately.
SC-3	Isolate security functions from nonsecurity functions.
SC-3(1)	Employ hardware separation mechanisms to implement security function isolation.
SC-3(2)	Isolate security functions enforcing access and information flow control from nonsecurity functions and from other security functions.
SC-3(3)	Minimize the number of nonsecurity functions included within the isolation boundary containing security functions.
SC-3(4)	Implement security functions as largely independent modules that maximize internal cohesiveness within modules and minimize coupling between modules.
SC-3(5)	Implement security functions as a layered structure minimizing interactions between layers of the design and avoiding any dependence by lower layers on the functionality or correctness of higher layers.
SC-4	Prevent unauthorized and unintended information transfer via shared system resources.
SC-4(2)	Prevent unauthorized information transfer via shared resources in accordance with [Assignment: organization-defined procedures] when system processing explicitly switches between different information classification levels or security categories.
SC-5a.	[Selection: Protect against; Limit] the effects of the following types of denial-of-service events: [Assignment: organization-defined types of denial-of-service events]; and
SC-5b.	Employ the following controls to achieve the denial-of-service objective: [Assignment: organization-defined controls by type of denial-of-service event].
SC-5(1)	Restrict the ability of individuals to launch the following denial-of-service attacks against other systems: [Assignment: organization-defined denial-of-service attacks].
SC-5(3)(a)	Employ the following monitoring tools to detect indicators of denial-of-service attacks against, or launched from, the system: [Assignment: organization-defined monitoring tools]; and
SC-5(3)(b)	Monitor the following system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks: [Assignment: organization-defined system resources].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SC-7a.	Monitor and control communications at the external managed interfaces to the system and at key internal managed interfaces within the system;
SC-7b.	Implement subnetworks for publicly accessible system components that are [Selection: physically; logically] separated from internal organizational networks; and
SC-7c.	Connect to external networks or systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security and privacy architecture.
SC-7(3)	Limit the number of external network connections to the system.
SC-7(4)(a)	Implement a managed interface for each external telecommunication service;
SC-7(4)(b)	Establish a traffic flow policy for each managed interface;
SC-7(4)(c)	Protect the confidentiality and integrity of the information being transmitted across each interface;
SC-7(4)(d)	Document each exception to the traffic flow policy with a supporting mission or business need and duration of that need;
SC-7(4)(e)	Review exceptions to the traffic flow policy [Assignment: organization-defined frequency] and remove exceptions that are no longer supported by an explicit mission or business need;
SC-7(4)(h)	Filter unauthorized control plane traffic from external networks.
SC-7(5)	Deny network communications traffic by default and allow network communications traffic by exception [Selection (one or more): at managed interfaces; for [Assignment: organization-defined systems]].
SC-7(7)	Prevent split tunneling for remote devices connecting to organizational systems unless the split tunnel is securely provisioned using [Assignment: organization-defined safeguards].
SC-7(8)	Route [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers at managed interfaces.
SC-7(9)(a)	Detect and deny outgoing communications traffic posing a threat to external systems; and
SC-7(9)(b)	Audit the identity of internal users associated with denied communications.
SC-7(10)(a)	Prevent the exfiltration of information; and
SC-7(10)(b)	Conduct exfiltration tests [Assignment: organization-defined frequency].
SC-7(11)	Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].
SC-7(12)	Implement [Assignment: organization-defined host-based boundary protection mechanisms] at [Assignment: organization-defined system components].
SC-7(13)	Isolate [Assignment: organization-defined information security tools, mechanisms, and support components] from other internal system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SC-7(14)	Protect against unauthorized physical connections at [Assignment: organization-defined managed interfaces].
SC-7(15)	Route networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.
SC-7(16)	Prevent the discovery of specific system components that represent a managed interface.
SC-7(17)	Enforce adherence to protocol formats.
SC-7(18)	Prevent systems from entering unsecure states in the event of an operational failure of a boundary protection device.
SC-7(19)	Block inbound and outbound communications traffic between [Assignment: organization-defined communication clients] that are independently configured by end users and external service providers.
SC-7(20)	Provide the capability to dynamically isolate [Assignment: organization-defined system components] from other system components.
SC-7(21)	Employ boundary protection mechanisms to isolate [Assignment: organization-defined system components] supporting [Assignment: organization-defined missions and/or business functions].
SC-7(22)	Implement separate network addresses to connect to systems in different security domains.
SC-7(23)	Disable feedback to senders on protocol format validation failure.
SC-7(24)	For systems that process personally identifiable information:
SC-7(24)(a)	Apply the following processing rules to data elements of personally identifiable information: [Assignment: organization-defined processing rules];
SC-7(24)(b)	Monitor for permitted processing at the external interfaces to the system and at key internal boundaries within the system;
SC-7(24)(c)	Document each processing exception; and
SC-7(24)(d)	Review and remove exceptions that are no longer supported.
SC-7(25)	Prohibit the direct connection of [Assignment: organization-defined unclassified national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].
SC-7(26)	Prohibit the direct connection of a classified national security system to an external network without the use of [Assignment: organization-defined boundary protection device].
SC-7(27)	Prohibit the direct connection of [Assignment: organization-defined unclassified non-national security system] to an external network without the use of [Assignment: organization-defined boundary protection device].
SC-7(28)	Prohibit the direct connection of [Assignment: organization-defined system] to a public network.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SC-7(29)	Implement [Selection: physically; logically] separate subnetworks to isolate the following critical system components and functions: [Assignment: organization-defined critical system components and functions].
SC-8	Protect the [Selection (one or more): confidentiality; integrity] of transmitted information.
SC-8(1)	Implement cryptographic mechanisms to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.
SC-8(2)	Maintain the [Selection (one or more): confidentiality; integrity] of information during preparation for transmission and during reception.
SC-8(3)	Implement cryptographic mechanisms to protect message externals unless otherwise protected by [Assignment: organization-defined alternative physical controls].
SC-8(4)	Implement cryptographic mechanisms to conceal or randomize communication patterns unless otherwise protected by [Assignment: organization-defined alternative physical controls].
SC-8(5)	Implement [Assignment: organization-defined protected distribution system] to [Selection (one or more): prevent unauthorized disclosure of information; detect changes to information] during transmission.
SC-10	Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.
SC-11(1)(a)	Provide a trusted communications path that is irrefutably distinguishable from other communications paths; and
SC-11(1)(b)	Initiate the trusted communications path for communications between the [Assignment: organization-defined security functions] of the system and the user.
SC-11a.	Provide a [Selection: physically; logically] isolated trusted communications path for communications between the user and the trusted components of the system; and
SC-11b.	Permit users to invoke the trusted communications path for communications between the user and the following security functions of the system, including at a minimum, authentication and re-authentication: [Assignment: organization-defined security functions].
SC-12	Establish and manage cryptographic keys when cryptography is employed within the system in accordance with the following key management requirements: [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction].
SC-12(1)	Maintain availability of information in the event of the loss of cryptographic keys by users.
SC-12(2)	Produce, control, and distribute symmetric cryptographic keys using [Selection: NIST FIPS-validated; NSA-approved] key management technology and processes.
SC-12(3)	Produce, control, and distribute asymmetric cryptographic keys using [Selection: NSA-approved key management technology and processes; prepositioned keying material; DoD-approved or DoD-issued Medium Assurance PKI certificates; DoD-approved or DoD-issued Medium Hardware Assurance PKI certificates and hardware security tokens that protect the user's private key; certificates issued in accordance with organization-defined requirements].
SC-13(a)	Determine the [Assignment: organization-defined cryptographic uses]; and

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SC-13(b)	Implement the following types of cryptography required for each specified cryptographic use: [Assignment: organization-defined types of cryptography for each specified cryptographic use].
SC-15a.	Prohibit remote activation of collaborative computing devices and applications with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and
SC-15b.	Provide an explicit indication of use to users physically present at the devices.
SC-15(1)	Provide [Selection (one or more): physical; logical] disconnect of collaborative computing devices in a manner that supports ease of use.
SC-15(3)	Disable or remove collaborative computing devices and applications from [Assignment: organization-defined systems or system components] in [Assignment: organization-defined secure work areas].
SC-15(4)	Provide an explicit indication of current participants in [Assignment: organization-defined online meetings and teleconferences].
SC-16	Associate [Assignment: organization-defined security and privacy attributes] with information exchanged between systems and between system components.
SC-16(1)	Verify the integrity of transmitted security and privacy attributes.
SC-16(2)	Implement anti-spoofing mechanisms to prevent adversaries from falsifying the security attributes indicating the successful application of the security process.
SC-16(3)	Implement [Assignment: organization-defined mechanisms or techniques] to bind security and privacy attributes to transmitted information.
SC-17a.	Issue public key certificates under an [Assignment: organization-defined certificate policy] or obtain public key certificates from an approved service provider; and
SC-17b.	Include only approved trust anchors in trust stores or certificate stores managed by the organization.
SC-18a.	Define acceptable and unacceptable mobile code and mobile code technologies; and
SC-18b.	Authorize, monitor, and control the use of mobile code within the system.
SC-18(1)	Identify [Assignment: organization-defined unacceptable mobile code] and take [Assignment: organization-defined corrective actions].
SC-18(2)	Verify that the acquisition, development, and use of mobile code to be deployed in the system meets [Assignment: organization-defined mobile code requirements].
SC-18(3)	Prevent the download and execution of [Assignment: organization-defined unacceptable mobile code].
SC-18(4)	Prevent the automatic execution of mobile code in [Assignment: organization-defined software applications] and enforce [Assignment: organization-defined actions] prior to executing the code.
SC-18(5)	Allow execution of permitted mobile code only in confined virtual machine environments.
SC-20a.	Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SC-20b.	Provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace.
SC-20(2)	Provide data origin and integrity protection artifacts for internal name/address resolution queries.
SC-21	Request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources.
SC-23	Protect the authenticity of communications sessions.
SC-23(1)	Invalidate session identifiers upon user logout or other session termination.
SC-23(3)	Generate a unique session identifier for each session with [Assignment: organization-defined randomness requirements] and recognize only session identifiers that are system-generated.
SC-23(5)	Only allow the use of [Assignment: organization-defined certificate authorities] for verification of the establishment of protected sessions.
SC-24	Fail to a [Assignment: organization-defined known system state] for the following failures on the indicated components while preserving [Assignment: organization-defined system state information] in failure: [Assignment: list of organization-defined types of system failures on organization-defined system components].
SC-25	Employ minimal functionality and information storage on the following system components: [Assignment: organization-defined system components].
SC-26	Include components within organizational systems specifically designed to be the target of malicious attacks for detecting, deflecting, and analyzing such attacks.
SC-27	Include within organizational systems the following platform independent applications: [Assignment: organization-defined platform-independent applications].
SC-28	Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].
SC-28(1)	Implement cryptographic mechanisms to prevent unauthorized disclosure and modification of the following information at rest on [Assignment: organization-defined system components or media]: [Assignment: organization-defined information].
SC-28(2)	Remove the following information from online storage and store offline in a secure location: [Assignment: organization-defined information].
SC-28(3)	Provide protected storage for cryptographic keys [Selection: [Assignment: organization-defined safeguards]; hardware-protected key store].
SC-29	Employ a diverse set of information technologies for the following system components in the implementation of the system: [Assignment: organization-defined system components].
SC-29(1)	Employ virtualization techniques to support the deployment of a diversity of operating systems and applications that are changed [Assignment: organization-defined frequency].
SC-30	Employ the following concealment and misdirection techniques for [Assignment: organization-defined systems] at [Assignment: organization-defined time periods] to confuse and mislead adversaries: [Assignment: organization-defined concealment and misdirection techniques].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SC-30(2)	Employ [Assignment: organization-defined techniques] to introduce randomness into organizational operations and assets.
SC-30(3)	Change the location of [Assignment: organization-defined processing and/or storage] [Selection: [Assignment: organization-defined time frequency]; at random time intervals]].
SC-30(4)	Employ realistic, but misleading information in [Assignment: organization-defined system components] about its security state or posture.
SC-30(5)	Employ the following techniques to hide or conceal [Assignment: organization-defined system components]: [Assignment: organization-defined techniques].
SC-31a.	Perform a covert channel analysis to identify those aspects of communications within the system that are potential avenues for covert [Selection (one or more): storage; timing] channels; and
SC-31b.	Estimate the maximum bandwidth of those channels.
SC-31(1)	Test a subset of the identified covert channels to determine the channels that are exploitable.
SC-31(2)	Reduce the maximum bandwidth for identified covert [Selection (one or more): storage; timing] channels to [Assignment: organization-defined values].
SC-31(3)	Measure the bandwidth of [Assignment: organization-defined subset of identified covert channels] in the operational environment of the system.
SC-32	Partition the system into [Assignment: organization-defined system components] residing in separate [Selection: physical; logical] domains or environments based on [Assignment: organization-defined circumstances for physical or logical separation of components].
SC-32(1)	Partition privileged functions into separate physical domains.
SC-34	For [Assignment: organization-defined system components], load and execute:
SC-34a.	The operating environment from hardware-enforced, read-only media; and
SC-34b.	The following applications from hardware-enforced, read-only media: [Assignment: organization-defined applications].
SC-34(1)	Employ [Assignment: organization-defined system components] with no writeable storage that is persistent across component restart or power on/off.
SC-34(2)	Protect the integrity of information prior to storage on read-only media and control the media after such information has been recorded onto the media.
SC-35	Include system components that proactively seek to identify network-based malicious code or malicious websites.
SC-36(1)(a)	Employ polling techniques to identify potential faults, errors, or compromises to the following processing and storage components: [Assignment: organization-defined distributed processing and storage components]; and
SC-36(1)(b)	Take the following actions in response to identified faults, errors, or compromises: [Assignment: organization-defined actions].
SC-37	Employ the following out-of-band channels for the physical delivery or electronic transmission of [Assignment: organization-defined information, system components, or devices] to [Assignment: organization-defined individuals or systems]: [Assignment: organization-defined out-of-band channels].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SC-37(1)	Employ [Assignment: organization-defined controls] to ensure that only [Assignment: organization-defined individuals or systems] receive the following information, system components, or devices: [Assignment: organization-defined information, system components, or devices].
SC-38	Employ the following operations security controls to protect key organizational information throughout the system development life cycle: [Assignment: organization-defined operations security controls].
SC-39	Maintain a separate execution domain for each executing system process.
SC-39(1)	Implement hardware separation mechanisms to facilitate process isolation.
SC-39(2)	Maintain a separate execution domain for each thread in [Assignment: organization-defined multi-threaded processing].
SC-40	Protect external and internal [Assignment: organization-defined wireless links] from the following signal parameter attacks: [Assignment: organization-defined types of signal parameter attacks or references to sources for such attacks].
SC-40(1)	Implement cryptographic mechanisms that achieve [Assignment: organization-defined level of protection] against the effects of intentional electromagnetic interference.
SC-40(2)	Implement cryptographic mechanisms to reduce the detection potential of wireless links to [Assignment: organization-defined level of reduction].
SC-40(3)	Implement cryptographic mechanisms to identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.
SC-40(4)	Implement cryptographic mechanisms to prevent the identification of [Assignment: organization-defined wireless transmitters] by using the transmitter signal parameters.
SC-41	[Selection: Physically; Logically] disable or remove [Assignment: organization-defined connection ports or input/output devices] on the following systems or system components: [Assignment: organization-defined systems or system components].
SC-42a.	Prohibit [Selection (one or more): the use of devices possessing [Assignment: organization-defined environmental sensing capabilities] in [Assignment: organization-defined facilities, areas, or systems]; the remote activation of environmental sensing capabilities on organizational systems or system components with the following exceptions: [Assignment: organization-defined exceptions where remote activation of sensors is allowed]]; and
SC-42b.	Provide an explicit indication of sensor use to [Assignment: organization-defined group of users].
SC-42(1)	Verify that the system is configured so that data or information collected by the [Assignment: organization-defined sensors] is only reported to authorized individuals or roles.
SC-42(2)	Employ the following measures so that data or information collected by [Assignment: organization-defined sensors] is only used for authorized purposes: [Assignment: organization-defined measures].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SC-42(4)	Employ the following measures to facilitate an individual's awareness that personally identifiable information is being collected by [Assignment: organization-defined sensors]: [Assignment: organization-defined measures].
SC-42(5)	Employ [Assignment: organization-defined sensors] that are configured to minimize the collection of information about individuals that is not needed.
SC-43a.	Establish usage restrictions and implementation guidelines for the following system components: [Assignment: organization-defined system components]; and
SC-43b.	Authorize, monitor, and control the use of such components within the system.
SC-44	Employ a detonation chamber capability within [Assignment: organization-defined system, system component, or location].
SC-45	Synchronize system clocks within and between systems and system components.
SC-45(1)(a)	Compare the internal system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]; and
SC-45(1)(b)	Synchronize the internal system clocks to the authoritative time source when the time difference is greater than [Assignment: organization-defined time period].
SC-45(2)(a)	Identify a secondary authoritative time source that is in a different geographic region than the primary authoritative time source; and
SC-45(2)(b)	Synchronize the internal system clocks to the secondary authoritative time source if the primary authoritative time source is unavailable.
SI-1a.	Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]:
SI-1a.1.	[Selection (one or more): Organization-level; Mission/business process-level; System-level] system and information integrity policy that:
SI-1a.1.(a)	Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
SI-1a.1.(b)	Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
SI-1a.2.	Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;
SI-1b.	Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and
SI-1c.	Review and update the current system and information integrity:
SI-1c.1.	Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and
SI-1c.2.	Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SI-2a.	Identify, report, and correct system flaws;
SI-2b.	Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
SI-2c.	Install security-relevant software and firmware updates within [Assignment: organization-defined time period] of the release of the updates; and
SI-2d.	Incorporate flaw remediation into the organizational configuration management process.
SI-2(2)	Determine if system components have applicable security-relevant software and firmware updates installed using [Assignment: organization-defined automated mechanisms] [Assignment: organization-defined frequency].
SI-2(3)(a)	Measure the time between flaw identification and flaw remediation; and
SI-2(3)(b)	Establish the following benchmarks for taking corrective actions: [Assignment: organization-defined benchmarks].
SI-2(4)	Employ automated patch management tools to facilitate flaw remediation to the following system components: [Assignment: organization-defined system components].
SI-2(5)	Install [Assignment: organization-defined security-relevant software and firmware updates] automatically to [Assignment: organization-defined system components].
SI-2(6)	Remove previous versions of [Assignment: organization-defined software and firmware components] after updated versions have been installed.
SI-3a.	Implement [Selection (one or more): signature based; non-signature based] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;
SI-3b.	Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
SI-3c.	Configure malicious code protection mechanisms to:
SI-3c.1.	Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and
SI-3c.2.	[Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organization-defined personnel or roles] in response to malicious code detection; and
SI-3d.	Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.
SI-3(4)	Update malicious code protection mechanisms only when directed by a privileged user.
SI-3(6)(a)	Test malicious code protection mechanisms [Assignment: organization-defined frequency] by introducing known benign code into the system; and
SI-3(6)(b)	Verify that the detection of the code and the associated incident reporting occur.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SI-3(8)(a)	Employ the following tools and techniques to analyze the characteristics and behavior of malicious code: [Assignment: organization-defined tools and techniques]; and
SI-3(8)(b)	Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.
SI-3(10)(a)	Employ the following tools and techniques to analyze the characteristics and behavior of malicious code: [Assignment: organization-defined tools and techniques]; and
SI-3(10)(b)	Incorporate the results from malicious code analysis into organizational incident response and flaw remediation processes.
SI-4a.	Monitor the system to detect:
SI-4a.1.	Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [Assignment: organization-defined monitoring objectives]; and
SI-4a.2.	Unauthorized local, network, and remote connections;
SI-4b.	Identify unauthorized use of the system through the following techniques and methods: [Assignment: organization-defined techniques and methods];
SI-4c.	Invoke internal monitoring capabilities or deploy monitoring devices:
SI-4c.1.	Strategically within the system to collect organization-determined essential information; and
SI-4c.2.	At ad hoc locations within the system to track specific types of transactions of interest to the organization;
SI-4d.	Analyze detected events and anomalies;
SI-4e.	Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;
SI-4f.	Obtain legal opinion regarding system monitoring activities; and
SI-4g.	Provide [Assignment: organization-defined system monitoring information] to [Assignment: organization-defined personnel or roles] [Selection (one or more): as needed; [Assignment: organization-defined frequency]].
SI-4(1)	Connect and configure individual intrusion detection tools into a system-wide intrusion detection system.
SI-4(2)	Employ automated tools and mechanisms to support near real-time analysis of events.
SI-4(3)	Employ automated tools and mechanisms to integrate intrusion detection tools and mechanisms into access control and flow control mechanisms.
SI-4(4)(a)	Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
SI-4(4)(b)	Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].
SI-4(5)	Alert [Assignment: organization-defined personnel or roles] when the following system-generated indications of compromise or potential compromise occur: [Assignment: organization-defined compromise indicators].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SI-4(7)(a)	Notify [Assignment: organization-defined incident response personnel (identified by name and/or by role)] of detected suspicious events; and
SI-4(7)(b)	Take the following actions upon detection: [Assignment: organization-defined least-disruptive actions to terminate suspicious events].
SI-4(9)	Test intrusion-monitoring tools and mechanisms [Assignment: organization-defined frequency].
SI-4(10)	Make provisions so that [Assignment: organization-defined encrypted communications traffic] is visible to [Assignment: organization-defined system monitoring tools and mechanisms].
SI-4(11)	Analyze outbound communications traffic at the external interfaces to the system and selected [Assignment: organization-defined interior points within the system] to discover anomalies.
SI-4(12)	Alert [Assignment: organization-defined personnel or roles] using [Assignment: organization-defined automated mechanisms] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [Assignment: organization-defined activities that trigger alerts].
SI-4(13)(a)	Analyze communications traffic and event patterns for the system;
SI-4(13)(b)	Develop profiles representing common traffic and event patterns; and
SI-4(13)(c)	Use the traffic and event profiles in tuning system-monitoring devices.
SI-4(14)	Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.
SI-4(15)	Employ an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.
SI-4(16)	Correlate information from monitoring tools and mechanisms employed throughout the system.
SI-4(17)	Correlate information from monitoring physical, cyber, and supply chain activities to achieve integrated, organization-wide situational awareness.
SI-4(18)	Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [Assignment: organization-defined interior points within the system].
SI-4(19)	Implement [Assignment: organization-defined additional monitoring] of individuals who have been identified by [Assignment: organization-defined sources] as posing an increased level of risk.
SI-4(20)	Implement the following additional monitoring of privileged users: [Assignment: organization-defined additional monitoring].
SI-4(21)	Implement the following additional monitoring of individuals during [Assignment: organization-defined probationary period]: [Assignment: organization-defined additional monitoring].
SI-4(22)(a)	Detect network services that have not been authorized or approved by [Assignment: organization-defined authorization or approval processes]; and

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SI-4(22)(b)	[Selection (one or more): Audit; Alert [Assignment: organization-defined personnel or roles]] when detected.
SI-4(23)	Implement the following host-based monitoring mechanisms at [Assignment: organization-defined system components]: [Assignment: organization-defined host-based monitoring mechanisms].
SI-4(24)	Discover, collect, and distribute to [Assignment: organization-defined personnel or roles], indicators of compromise provided by [Assignment: organization-defined sources].
SI-4(25)	Provide visibility into network traffic at external and key internal system interfaces to optimize the effectiveness of monitoring devices.
SI-5a.	Receive system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis;
SI-5b.	Generate internal security alerts, advisories, and directives as deemed necessary;
SI-5c.	Disseminate security alerts, advisories, and directives to: [Selection (one or more): [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined elements within the organization]; [Assignment: organization-defined external organizations]]; and
SI-5d.	Implement security directives in accordance with established time frames, or notify the issuing organization of the degree of noncompliance.
SI-5(1)	Broadcast security alert and advisory information throughout the organization using [Assignment: organization-defined automated mechanisms].
SI-6a.	Verify the correct operation of [Assignment: organization-defined security and privacy functions];
SI-6b.	Perform the verification of the functions specified in SI-6a [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; [Assignment: organization-defined frequency]];
SI-6c.	Alert [Assignment: organization-defined personnel or roles] to failed security and privacy verification tests; and
SI-6d.	[Selection (one or more): Shut the system down; Restart the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered.
SI-6(2)	Implement automated mechanisms to support the management of distributed security and privacy function testing.
SI-6(3)	Report the results of security and privacy function verification to [Assignment: organization-defined personnel or roles].
SI-7a.	Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [Assignment: organization-defined software, firmware, and information]; and
SI-7b.	Take the following actions when unauthorized changes to the software, firmware, and information are detected: [Assignment: organization-defined actions].
SI-7(1)	Perform an integrity check of [Assignment: organization-defined software, firmware, and information] [Selection (one or more): at startup; at [Assignment: organization-defined transitional states or security-relevant events]; [Assignment: organization-defined frequency]].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SI-7(2)	Employ automated tools that provide notification to [Assignment: organization-defined personnel or roles] upon discovering discrepancies during integrity verification.
SI-7(3)	Employ centrally managed integrity verification tools.
SI-7(5)	Automatically [Selection (one or more): shut the system down; restart the system; implement [Assignment: organization-defined controls]] when integrity violations are discovered.
SI-7(6)	Implement cryptographic mechanisms to detect unauthorized changes to software, firmware, and information.
SI-7(7)	Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [Assignment: organization-defined security-relevant changes to the system].
SI-7(8)	Upon detection of a potential integrity violation, provide the capability to audit the event and initiate the following actions: [Selection (one or more): generate an audit record; alert current user; alert [Assignment: organization-defined personnel or roles]; [Assignment: organization-defined other actions]].
SI-7(9)	Verify the integrity of the boot process of the following system components: [Assignment: organization-defined system components].
SI-7(10)	Implement the following mechanisms to protect the integrity of boot firmware in [Assignment: organization-defined system components]: [Assignment: organization-defined mechanisms].
SI-7(12)	Require that the integrity of the following user-installed software be verified prior to execution: [Assignment: organization-defined user-installed software].
SI-7(15)	Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [Assignment: organization-defined software or firmware components].
SI-7(16)	Prohibit processes from executing without supervision for more than [Assignment: organization-defined time period].
SI-8a.	Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and
SI-8b.	Update spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures.
SI-8(2)	Automatically update spam protection mechanisms [Assignment: organization-defined frequency].
SI-8(3)	Implement spam protection mechanisms with a learning capability to more effectively identify legitimate communications traffic.
SI-10	Check the validity of the following information inputs: [Assignment: organization-defined information inputs to the system].
SI-10(1)(a)	Provide a manual override capability for input validation of the following information inputs: [Assignment: organization-defined inputs defined in the base control (SI-10)];
SI-10(1)(b)	Restrict the use of the manual override capability to only [Assignment: organization-defined authorized individuals]; and
SI-10(1)(c)	Audit the use of the manual override capability.

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SI-10(2)	Review and resolve input validation errors within [Assignment: organization-defined time period].
SI-10(3)	Verify that the system behaves in a predictable and documented manner when invalid inputs are received.
SI-10(4)	Account for timing interactions among system components in determining appropriate responses for invalid inputs.
SI-10(5)	Restrict the use of information inputs to [Assignment: organization-defined trusted sources] and/or [Assignment: organization-defined formats].
SI-10(6)	Prevent untrusted data injections.
SI-11a.	Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and
SI-11b.	Reveal error messages only to [Assignment: organization-defined personnel or roles].
SI-12	Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines and operational requirements.
SI-12(1)	Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [Assignment: organization-defined elements of personally identifiable information].
SI-12(2)	Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [Assignment: organization-defined techniques].
SI-12(3)	Use the following techniques to dispose of, destroy, or erase information following the retention period: [Assignment: organization-defined techniques].
SI-14	Implement non-persistent [Assignment: organization-defined system components and services] that are initiated in a known state and terminated [Selection (one or more): upon end of session of use; periodically at [Assignment: organization-defined frequency]].
SI-14(1)	Obtain software and data employed during system component and service refreshes from the following trusted sources: [Assignment: organization-defined trusted sources].
SI-15	Validate information output from the following software programs and/or applications to ensure that the information is consistent with the expected content: [Assignment: organization-defined software programs and/or applications].
SI-16	Implement the following controls to protect the system memory from unauthorized code execution: [Assignment: organization-defined controls].
SI-17	Implement the indicated fail-safe procedures when the indicated failures occur: [Assignment: organization-defined list of failure conditions and associated fail-safe procedures].
SR-3a.	Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel];
SR-3b.	Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain-related events: [Assignment: organization-defined supply chain controls]; and

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SR-3c.	Document the selected and implemented supply chain processes and controls in [Selection: security and privacy plans; supply chain risk management plan; [Assignment: organization-defined document]].
SR-3(1)	Employ a diverse set of sources for the following system components and services: [Assignment: organization-defined system components and services].
SR-3(2)	Employ the following controls to limit harm from potential adversaries identifying and targeting the organizational supply chain: [Assignment: organization-defined controls].
SR-4(1)	Establish and maintain unique identification of the following supply chain elements, processes, and personnel associated with the identified system and critical system components: [Assignment: organization-defined supply chain elements, processes, and
SR-4(2)	Establish and maintain unique identification of the following systems and critical system components for tracking through the supply chain: [Assignment: organization-defined systems and critical system components].
SR-4(3)	Employ the following controls to validate that the system or system component received is genuine and has not been altered: [Assignment: organization-defined controls].
SR-5	Employ the following acquisition strategies, contract tools, and procurement methods to protect against, identify, and mitigate supply chain risks: [Assignment: organization-defined acquisition strategies, contract tools, and procurement methods].
SR-5(1)	Employ the following controls to ensure an adequate supply of [Assignment: organization-defined critical system components]: [Assignment: organization-defined controls].
SR-5(2)	Assess the system, system component, or system service prior to selection, acceptance, modification, or update.
SR-6	Assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide [Assignment: organization-defined frequency].
SR-6(1)	Employ [Selection (one or more): organizational analysis; independent third-party analysis; organizational testing; independent third-party testing] of the following supply chain elements, processes, and actors associated with the system, system component, or system service: [Assignment: organization-defined supply chain elements, processes, and actors].
SR-7	Employ the following Operations Security (OPSEC) controls to protect supply chain-related information for the system, system component, or system service: [Assignment: organization-defined Operations Security (OPSEC) controls].
SR-8	Establish agreements and procedures with entities involved in the supply chain for the system, system component, or system service for the [Selection (one or more): notification of supply chain compromises; results of assessments or audits; [Assignment: organization-defined information]].
SR-11(1)	Train [Assignment: organization-defined personnel or roles] to detect counterfeit system components (including hardware, software, and firmware).
SR-11(2)	Maintain configuration control over the following system components awaiting service or repair and serviced or repaired components awaiting return to service: [Assignment: organization-defined system components].
SR-11(3)	Scan for counterfeit system components [Assignment: organization-defined frequency].

NIST 800-53 Definitions (continued)

NIST 800-53	NIST 800-53 Description
SR-11(a)	Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system; and
SR-11(b)	Report counterfeit system components to [Selection (one or more): source of counterfeit component; [Assignment: organization-defined external reporting organizations]; [Assignment: organization-defined personnel or roles]].

LWBJ®

CPA | Consulting | M&A

4200 University Avenue, Suite 410
West Des Moines, IA 50266
515-222-5680

1530 South Duff, Suite 2
Ames, IA 50010
515-233-1975

lwbj.com