

**SYSTEM AND ORGANIZATION
CONTROLS 3 (SOC 3) REPORT**

Report on Bitwarden Inc. Password Management System

For the Period **July 1, 2020** to **June 30, 2021**

SYSTEM AND ORGANIZATION CONTROLS 3 (SOC 3) REPORT

Report on Bitwarden Inc. Description of Its Password Management System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security and Confidentiality Throughout the Period July 1, 2020, to June 30, 2021



Bitwarden Inc.
1 N. Calle Cesar Chavez, Suite 102
Santa Barbara, CA 93103

Tel: +1.904.337.9364

www.bitwarden.com



Table of Contents

Section I – Assertion of Bitwarden Inc. Management.....	1
Section II – Independent Service Auditor’s Report	4
Section III – Bitwarden Inc. Description of its Password Management System Throughout the Period July 1, 2020, to June 30, 2021.....	8
Company Background	9
Services Provided.....	11
Components of the System.....	13
Principal Service Commitments	17
Attachment A – AICPA Trust Services Criteria	18

Section I – Assertion of Bitwarden Inc. Management

Assertion of Bitwarden Inc. Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Bitwarden Inc. (Bitwarden) Password Management System (system) throughout the period July 1, 2020, to June 30, 2021, to provide reasonable assurance that Bitwarden service commitments and system requirements relevant to security and confidentiality were achieved. Our description of the boundaries of the system is presented in Section III and identifies the aspects of the system covered by our assertion.

Bitwarden utilizes two nationally known cloud service providers, and a cloud-based performance and reliability service, as subservice organization providers. The Description (Section III) included only the controls of Bitwarden and excludes controls of these subservice providers. The Description also indicates that certain trust service criteria specific therein can be met only if these subservice provider's controls assumed in the design of Bitwarden controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls at the subservice providers. However, we perform annual due diligence procedures for third party subservice providers and based on the procedures performed nothing has been identified that prevents the subservice providers from achieving its specified commitments. The subservice organizations used by Bitwarden have met SOC certification standards.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period July 1, 2020, to June 30, 2021, to provide reasonable assurance that Bitwarden service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality, (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)*. Bitwarden objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period July 1, 2020, to June 30, 2021, to provide reasonable assurance that Bitwarden service commitments and system requirements were achieved based on the applicable trust services criteria.

A handwritten signature in blue ink, appearing to read "Michael Crandell".

Mr. Michael Crandell, CEO

Bitwarden Inc.

August 16, 2021

Section II – Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Bitwarden Inc.

Scope

We have examined Bitwarden Inc. (Bitwarden) accompanying assertion titled "Assertion of Bitwarden Inc. Management" (assertion) that the controls within the Bitwarden Password Management System (system) were effective throughout the period July 1, 2020, to June 30, 2021, to provide reasonable assurance that Bitwarden service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (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*).

Bitwarden utilizes two nationally known cloud service providers, and a cloud-based performance and reliability service, as subservice organization providers. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Bitwarden, to achieve Bitwarden service commitments and system requirements based on the applicable trust services criteria. The description presents Bitwarden controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Bitwarden controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, 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 Bitwarden, to achieve Bitwarden service commitments and system requirements based on the applicable trust services criteria. The description presents Bitwarden controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Bitwarden 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.

Service Organization's Responsibilities

Bitwarden 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 Bitwarden service commitments and system requirements were achieved. Bitwarden has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Bitwarden is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Bitwarden service commitments and system requirements based on the applicable trust services criteria
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Bitwarden service commitments and system requirements based the applicable trust services criteria

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

Inherent Limitations

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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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.

Opinion

In our opinion, management's assertion that the controls within the Bitwarden Password Management System were effective throughout the period July 1, 2020, to June 30, 2021, to provide reasonable assurance that Bitwarden service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.



San Jose, California

August 16, 2021

**Section III – Bitwarden Inc. Description of its
Password Management System Throughout the
Period July 1, 2020, to June 30, 2021**

Bitwarden Inc. Description of its Password Management System Throughout the Period July 1, 2020, to June 30, 2021

Company Background

Bitwarden Inc. (Bitwarden) is an open source password management solution for individuals, teams, and business organizations available in both free and paid plans. Bitwarden was created by Kyle Spearrin in 2016.

Today the company is headquartered in Santa Barbara, California with a global distributed team. Bitwarden serves large and small companies around the world as well as our base of individual users.

Company Management

Michael Crandell, Chief Executive Officer

Michael is the chief executive officer at Bitwarden driving overall company strategy and growth.

Before Bitwarden, Michael was the CEO and co-founder of RightScale where he led the vision and direction for the company as a cloud management platform during the first decade of cloud computing. He grew the company to 250 employees and a successful exit to Flexera in 2018.

Prior to RightScale, Michael served as chief executive officer at several Internet software-as-a-service (SaaS) companies and as vice president of software and executive vice president at eFax.com, where he was part of the executive team that took the company public.

Michael received his bachelor's degree from Stanford University and completed graduate studies at Harvard University. He began his career as a software engineer, self-taught, coding in assembly language.

Kyle Spearrin, Founder and Chief Technology Officer

Kyle is the founder and chief technology officer of Bitwarden and currently leads all engineering and product efforts.

Before Bitwarden, Kyle was a software architect and engineering lead at iMobile3, a payment solutions company, where he focused on cloud infrastructure, mobile applications, and security for credit card processing.

Kyle previously founded companies in hosting and web services and has been a builder of online tools since he started organizing gaming communities in high school.

Kyle holds a bachelor's degree in Computer Science from the University of Florida.

Gary Orenstein, Chief Customer Officer

Gary is the chief customer officer at Bitwarden leading the go to market efforts across customer success, marketing, and sales.

Before Bitwarden, Gary served in executive marketing and product roles at enterprise infrastructure companies Yellowbrick Data and MemSQL, and flash memory pioneer Fusion-io which went public during his tenure there. Earlier in his career he led marketing at Compellent which after its IPO was acquired by Dell.

Gary holds a bachelor's degree from Dartmouth College and a master's in business administration from The Wharton School at the University of Pennsylvania.

Stephen Morrison, Chief Financial Officer

Steve joined Bitwarden in 2019 and leads the accounting, finance, legal and human resources functions.

Previously, Steve was CFO at RightScale, Inc. where he led the strategic sale of the company to Flexera, Inc. Before that, Steve was CFO at Butler America, LLC, a leading outsourcing firm, where he led the strategic sale of the aerospace engineering and defense division and the financial sale of the company's healthcare unit. He has held CFO roles at several other technology firms including ValenTx in medical technology, SmartReceipt in SaaS marketing, and 724 Solutions focused on mobile technology.

Originally from Canada, Steve moved to Santa Barbara 2003 after spending two years in Hong Kong while at 724 Solutions. He holds a BA from Western University in London, Ontario and an MBA from the Richard Ivey School of Business at Western.

Services Provided

Bitwarden provides a comprehensive solution for password management.

User view

Users primarily interact with Bitwarden through our client applications. In order to access Bitwarden client applications, users must create a login and master password. This information is used both for authenticating into Bitwarden, as well as to create a unique encryption key for each individual user. The encryption key is used to encrypt passwords, files, and other sensitive data the user selects to store in the Bitwarden Vault.

When interacting with Bitwarden applications, all Vault data is encrypted locally as it is stored, and Vault data remains encrypted for syncing. Thus, Bitwarden utilizes end-to-end encryption in the transmission and storage of all sensitive user data.

Bitwarden Client Applications

Bitwarden client applications span virtually all endpoint devices:

- Mobile for iOS and Android devices
- Desktop for Windows, MacOS, and Linux operating systems
- Browser Extensions for Chrome, Safari, Firefox, Edge, Brave, Opera and other web browsers
- Command Line Interface
- Web Application

All Vault data is encrypted and decrypted in the client applications with access granted via the user email and master password. Bitwarden as a company has no access to unencrypted Vault user data.

Bitwarden Extensions

Bitwarden also includes extensions such as

- Directory Sync with a range of directory services such as
- Active Directory
- Any LDAP-based directory
- Azure Active Directory
- G Suite (Google)
- Okta
- A RESTful API is available at docs.bitwarden.com

Bitwarden Cloud

Bitwarden Cloud is available to all Bitwarden users as a means to synchronize devices. Bitwarden Cloud runs on Microsoft Azure.

Self-hosted Installation

Bitwarden is also available for self-hosted installation through a simplified Docker deployment.

Company Differentiators

Bitwarden is the only password management solution that is available as open source software and can be deployed as a service in the cloud, or self-hosted wherever customers choose, such as behind their firewall.

Components of the System

Management Controls

Control Environment

Board of Directors and Executive Oversight: The Company's board of directors conducts quarterly meetings. In addition, processes are in place to ensure that any sensitive information, investigations, and improper acts by or within the Company are reported to the board of directors in a timely manner.

Organizational Structure: The responsibilities of key positions within the Company are clearly defined and communicated. The Company has a hierarchical organizational structure that supports the open and continuous communication of information between leadership and its support staff. The hierarchy allows for clear direction to be communicated from executive management throughout the Company to support the overall objectives and direction of the Company.

Management Philosophy: Management's policies and communications are directed at ensuring that the company's personnel (i) understand the company's objectives; (ii) know how their individual actions interrelate and contribute to those objectives; and (iii) recognize how and for what they will be held accountable.

Management instills a philosophy that enables employees to share in the success and growth of the Company. A highly skilled and diverse group of employees comprises the organization's management team, individuals who are ultimately responsible for the vision and direction of the Company. Management members meet on a structured, routine basis to discuss a range of topics and are also responsible for establishing policies and addressing operational, financial, and social aspects of the organization.

Human Resource Management: The Company's management understands that a secure, quality operation requires an ethical, responsible, and competent staff. The Company maintains a thorough set of policies and practices to meet this objective including:

- Comprehensive employee background checks
- Hiring standards are established with emphasis on prior work experience, qualifications, and past accomplishments
- New hire orientation with training sessions addressing all essential organizational elements and department level orientation specific to respective roles
- Employee performance management process includes periodic assessments and real-time feedback
- Annual compliance training

Company policies and standards are clearly communicated to employees through formal documentation, close supervision and training. Employees are provided a comprehensive employee handbook that covers a wide range of control considerations, clearly stated disciplinary procedures, and grounds for termination. Documented policies include:

- At-will employment policy
- Code of ethics
- Acceptable use
- Information/data security
- Confidentiality/non-disclosure of Company and client information
- Possession and use of company property
- Internet, email, and phone use
- Safety standards

Business Development: The sales staff is responsible for actively pursuing new business opportunities to help grow the organization. The team communicates openly and frequently with other members of the management team regarding business development and market penetration, and also discusses labor, capacity, productivity measures, and short-term and long-term planning when applicable. The Company actively assesses the risks of a potential decline or growth in sales and how it may affect the organization as a whole.

Financial Management: Finance and accounting employees are responsible for payments of organizational fixed and variable costs, tracking and reporting on key financial metrics, building cash flow projection models, budgeting and financial regulatory compliance, collecting payments from clients, and maintaining all other financial activities. This team continually monitors and evaluates risk assessment concerning cash flows and the ability to meet mandatory expenses. Senior management also routinely addresses issues such as lines of credit, cash reserves, and other financial requirements. Annual budgets are created each fiscal year and reviewed on an ongoing basis.

Budgetary Process: The budgetary process encompasses all aspects of the financial reporting, including the creation of a budget book that details each division's budgeted monthly client revenue; a headcount report, including additions and deletions; balance sheet; cash flow; capital expenditures; roll-forward from prior year, including explanations of variances; and comparison to prior year actual, budget, and forecast. The Finance team works with each individual department manager to develop their respective budget then completes a review with the department manager to finalize the plan. The budget is then reviewed at the senior management level with the CEO. Upon completion, the budget is presented to the executive board by the leadership team for final approval.

Communication: The Company conducts recurring meetings to identify and address significant issues affecting the Company's operations. As business and development plans are established, meetings are held throughout the Company to report results achieved and communicate defined goals. Informal meetings provide the vehicle for management to communicate and respond to operational tasks and issues. At all corporate levels, the Company has established communication channels to promote and distribute information up and down the defined management structure. The Company embraces a belief that information should flow in an open environment, allowing discussion on a wide range of topics and subject matter by all employees.

Mission and Values: The Company has engaged in a Company-wide process of defining the mission and values statements of the Company and reviews those statements on a regular basis with existing and new employees.

Policy Management: Policy and procedure documents inform employees of their responsibility within the workplace environment and professional conduct expectations. Each department has access to work instruction documents pertaining to their respective roles and duties and how they should be performed. Revisions to corporate policies and procedures are readily available through the Company Google Docs, and are distributed to relevant employees in a timely manner. Each policy and procedure is subject to an annual review and must be approved by respective managers.

Monitoring Controls: The Company maintains internal reporting, monitoring, and evaluation procedures to identify deviations from internal controls; and maintains a process to effectively report these deficiencies to the appropriate departments. The Company's monitoring procedures include:

- Goal setting and periodic review meetings with all employees
- Analysis of and appropriate follow-up on operating reports or metrics that might identify anomalies indicative of a control failure
- Supervisory reviews of controls, such as reconciliation reviews, as a normal part of processing

The assessment of compliance risk and ongoing corrective actions established by an: 1) annual risk assessment; and 2) ongoing quality control, quality assurance, and departmental monitoring.

The Company monitors internal control systems by conducting monitoring activities across the organization. Internal control deficiencies are immediately reported upstream to management where corrective action is applied. More serious matters are escalated to top-level management and immediate action is taken. Monitoring activities over internal controls are included in the following functional areas:

- Sales and Marketing
- Information Technology
- Finance and Accounting
- Daily Operations and Transaction Processing Environment

Security Controls:

Bitwarden security controls include but are not limited to:

- Logical access controls
- Data Security / Data Encryption
- Data Protection / Data Privacy
- Data Protection in Transit
- Data Protection at Rest
- Password hashing / Key derivation / Key Management and Key Storage

Please refer to the Bitwarden Security page for additional information

<https://bitwarden.com/help/security/>

Business Continuity and Disaster Recovery Program

Bitwarden employs a full range of disaster recovery and business continuity practices from Microsoft Azure that are built into the Bitwarden Cloud. This includes high availability and backup services for our application and database tiers. A combination of manual and automated monitoring of the Bitwarden Cloud infrastructure provides a comprehensive and detailed view of system health as well as proactive alerts on areas of concern. Issues are surfaced quickly so that our infrastructure team can effectively respond and mitigate problems with minimal disruption.

Customer / Client Support

Escalation Procedures are invoked to address any production processing issues. Clients are contacted if there are any quality issues or production delays that may affect agreed upon service levels.

Service Level Management: The Customer Support Manager monitors and reports on the achievement of specified performance criteria and takes corrective action when needed.

Principal Service Commitments and System Requirements

Bitwarden designs its processes and procedures related to the system to meet its objectives for its password management services. Those objectives are based on the service commitments that Bitwarden makes to user entities, the laws and regulations that govern the provision of the password management services, and the financial, operational, and compliance requirements that Bitwarden has established for the services. The password management services of Bitwarden are subject to the relevant regulatory and industry information and data security requirements in which Bitwarden operates

The security and confidentiality commitments to user entities are documented and communicated in customer agreements, sales and website documentation, and company policies. The principal security and confidentiality commitments are standardized and include, but are not limited to, the following:

- Security: Bitwarden maintains a robust information security program that includes:
 - Background checks conducted as part of the hiring process for employees and contractors
 - Security awareness training, and relevant compliance training provided at time of hire and renewed annually for all employees and contractors
 - Policies and procedures governing the security program reviewed and updated on an annual basis
 - Operational and technical controls in place to ensure confidential data is protected from unauthorized disclosure, use, modification, or destruction.
 - Independent third party security risk assessments performed on an annual basis
- Confidentiality: Bitwarden considers and classifies all personally identifiable customer/client data that is processed on its production information systems as Confidential.

Bitwarden establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Bitwarden system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the password management system.

Attachment A - AICPA Trust Services Criteria

Attachment A – AICPA Trust Services Criteria

Trust Services Criteria

Trust Services are a set of professional attestation and advisory services based on a core set of criteria that address the risks and opportunities of IT-enabled systems and privacy programs. The following criteria are being used in the performance of this trust services engagement:

- Security. The system is protected against unauthorized access (both physical and logical)
- Confidentiality. Information designated as confidential is protected as committed or agreed

Security

The system is protected against unauthorized access (both physical and logical).

The security criteria refers to the protection of the system components from unauthorized access, both logical and physical. In e-commerce and other systems, the respective parties wish to ensure that information provided is available only to those individuals who need access to complete the transaction or services or follow up on questions or issues that may arise. Information provided through these systems is susceptible to unauthorized access during transmission and while it is stored on the other party's systems. Limiting access to the system components helps prevent potential abuse of system components, theft of resources, misuse of software, and improper access to, use, alteration, destruction, or disclosure of information. Key elements for the protection of system components include permitting authorized access and preventing unauthorized access to those components.

Confidentiality

Information designated as confidential is protected as committed or agreed.

The confidentiality criteria focuses on information designated as confidential. Unlike personal information, which is being defined by regulation in a number of countries worldwide and is subject to the privacy criteria, there is no widely recognized definition of confidential information. In the course of communicating and transacting business, partners often exchange information they require to be maintained on a confidential basis. In most instances, the respective parties wish to ensure that the information they provide is available only to those individuals who need access to complete the transaction or resolution on any questions that arise. To enhance business partner confidence, it is important that the business partner is informed about the entity's confidentiality practices. The entity needs to disclose its practices relating to the manner in which it provides for authorized access to and uses and shares information designated as confidential.

The following table presents the trust services criteria for security and confidentiality, which are applicable to a SOC 2 examination. The table includes the criteria that originates directly from the Committee of Sponsoring Organizations of the Treadway Commission's 2013 Internal Control—Integrated Framework (COSO framework).

The trust services criteria for security, and confidentiality below have been extracted from TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, issued in April 2017 by the AICPA's Assurance Services Executive Committee.

TSP Ref. #	TRUST SERVICES CRITERIA
	CONTROL ENVIRONMENT
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
	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.

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.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.
	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.
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.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.
	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.
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 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.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
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.

	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.
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.
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.
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.

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

	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.
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.
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.

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.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.
	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.
	Risk Mitigation
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.

	ADDITIONAL CRITERIA FOR CONFIDENTIALITY
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.