Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B



System and Organization Controls (SOC) 3 Report on Workable's Description of its Hiring and HR management platform and on the Suitability of the Design and Operating Effectiveness of its Controls relevant to Security, Availability, and Confidentiality for the period 1 June 2024 to 31 May 2025.

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

Contents

SECTION A - WORKABLE MANAGEMENT ASSERTION 3

SECTION B - REPORT OF INDEPENDENT SERVICE AUDITORS 5

SECTION C - DESCRIPTION OF WORKABLE PRODUCT 8

1.1 Workable Company Overview 8

1.2 Product Overview and Services Provided 8

1.3 Scope and boundaries 9

1.4 Workable system components 9

1.4.1 Infrastructure 9

1.4.2 Network 10

1.4.3 Computing Services 10

1.4.4 Software 10

1.4.5 Data 11

1.5 People 11

1.6 Policies and Procedures 14

1.7 Principal Service Commitments and System Requirements 15

1.8 Description of the Control Environment, Information, Communication, Monitoring and Risk Assessment Processes 16

SECTION D - AICPA TRUST SERVICES CRITERIA 17

AICPA Trust Services Criteria 17

Categories 17

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

workable

SECTION A - WORKABLE MANAGEMENT ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within Workable Software Single Member Private Company (the “Service Organization" or “Workable”) related to internal controls related to operations, software development, delivery, and management of Workable Product throughout the period 01 June 2024 to 31 May 2025 (the “period”), to provide reasonable assurance that Workable’s service commitments and system requirements relevant to security, availability and confidentiality were achieved. Our description of the boundaries of the system is presented in Section C and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period 01 June 2024 to 31 May 2025 to provide reasonable assurance that Workable’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability 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).

Workable’s 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 D.

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.

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

We assert that the controls within the system were effective throughout the period 01 June 2024 to 31 May 2025, to provide reasonable assurance that Workable's service commitments and system requirements were achieved based on the applicable trust services criteria.

DocuSigned by:
Spyridon Magiatis
EC12145A1F364E4...

30/7/2025

Workable Software Single Member Private Company

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

SECTION B - REPORT OF INDEPENDENT SERVICE AUDITORS

To the Management of Workable Software Single Member Private Company

Scope

We have examined Workable Software Single Member Private Company (the "Service Organization" or "Workable") accompanying description of Workable's product (the "System") described in section C, throughout the period 01 June 2024 to 31 May 2025 (the "period") 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*) ("description criteria") and the suitability of the design of controls stated in the description throughout that period, to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability 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*).

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Service Organization, to achieve the Service Organization's service commitments and system requirements based on the applicable trust services criteria. The description presents the systems related to Workable Product, the Service Organization's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Service Organization's controls. Our examination did not extend to the services provided by the subservice organizations, and we have not evaluated whether the controls management assumes have been implemented at both subservice organizations have been implemented or whether such controls were suitably designed and operating effectively through the period 01 June 2024 to 31 May 2025.

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

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

Service Organization's responsibilities

The Service Organization 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 Service Organization's service commitments and system requirements were achieved. The Service Organization has provided the accompanying assertion titled "Workable Management Assertion", about the description and the suitability of the design of controls stated therein. The Service Organization 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 auditor's responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design 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 and with International Standard on Assurance Engagements 3000, Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. 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 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 of controls involves the following:

● Obtaining an understanding of the system and the service organization'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.

We are required to be independent and to meet our other ethical responsibilities in accordance with

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

relevant ethical requirements related to the engagement.

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 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.

Opinion

In our opinion, management's assertion that the controls within Workable's product were effective throughout the period June 1, 2024 to May 31, 2025, to provide reasonable assurance that Workable's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

PricewaterhouseCoopers SA

Athens, Greece

30/7/2025

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

workable

SECTION C - DESCRIPTION OF WORKABLE PRODUCT

1.1 Workable Company Overview

Workable offers a comprehensive suite for hiring and employee management, making HR tasks simpler and more efficient. It's designed to help companies of all types manage their recruitment and HR processes in one place.

Workable Recruiting is a leading Applicant Tracking System that's helped make more than 1.5 million hires. It's an advanced hiring process, a full sourcing suite, and top-tier integrations with major job boards. It speeds up hiring by automating routine tasks like scheduling, emailing, and texting – helping hiring teams focus on finding and hiring the best. A full recruitment reporting center makes for informed decision-making at every point of the hiring process.

Workable HR is a comprehensive workforce management solution that is designed to manage a dynamic workforce and for ease of use by the HR team and employees. It's highly customizable to handle personal data securely, track & manage employee time off, create reports, and connect with payroll systems with org charts, company directories, and mobile app.

In addition to Workable's HR Suite, Jobs by Workable connects millions of job seekers with opportunities in companies using Workable, and Workable's Branded Job Boards allow communities and networks to set up their job boards to attract specific talent.

Workable has helped over 27,000 companies hire all over the world, becoming one of the most reputable names in HR tech.

1.2 Product Overview and Services Provided

With Workable, users access advanced recruitment and HR tools via a web-based hiring platform to find and attract candidates, evaluate applicants with their hiring teams, automate manual hiring tasks and processes, and manage employees. Workable provides users with dozens of essential hiring and employee management tools, including AI-powered candidate recommendations, customizable pipelines, interview self-scheduling, advanced reporting, requisition and budget workflows, one-way video interviews, employee onboarding, time off management, payroll integrations, and many more.

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

In addition to providing native tools, Workable also integrates with 70+ third-party apps and services to extend what users are able to accomplish within Workable. Mobile apps for iOS and Android are also available, in addition to Workable's mobile-friendly browser-based web platform. Workable's global support team is available nearly 24/7. Workable is ISO/IEC 27001 and ISO/IEC 27017 certified and complies with applicable Data Protection Requirements (e.g. GDPR, UK-GDPR, CCPA).

Additional details are available on Workable's website.

1.3 Scope and boundaries

The system is designed, implemented and operated to achieve specific business objectives in accordance with management, client and legal requirements. The purpose of the system description is to present the boundaries of the system, which includes the provision of services as well as the main components described below: infrastructure, software, people, data, policies and procedures.

1.4 Workable system components

Workable is an all-in-one HR suite: redefining HR with intelligent tools to streamline hiring, employee data management, time tracking and payroll. They are referenced as a Workable Product within this document.

1.4.1 Infrastructure

The System production environment is hosted by infrastructure subprocessors; the two core ones that cover the biggest part of the Product being Amazon Web Services ("AWS") and Google Cloud Platform ("GCP"). We also use Microsoft Azure Cognitive services.

Customer data is processed by and stored in hosted infrastructure *Compute* services (such as Google Kubernetes Engine (GKE), Google Compute Engine (GCE), Amazon Elastic Compute Cloud (EC2) and AWS Lambda Functions) instances and hosted infrastructure *Storage* services (such as AWS Simple Storage Service (S3). Google Cloud Storage (GCS) is utilized to store backup copies of customer data and application logs. Moreover, customer data are present in hosted Data Stores (such as Mongo, Redis, Postgres (RDS)) services.

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

Development activities and quality assurance tests occur on systems in environments that are separate from the production environment; GCP and AWS use distinct organizations.

1.4.1.1 Request Flow

A typical HTTP request to the Workable applications connects to Cloudflare's Edge Servers that is closest to the user (acting as Web Application Firewall), and from there the request is forwarded to the corresponding application cluster in GKE. The application validates the user session and its authorization rights and responds accordingly either with the requested object (potentially via other internal redirects) or with an error message that redirects the user to the login page. Mobile applications' access follows the similar flows.

1.4.1.2 Static Assets Request Flow

For static assets (CSS, index.js, etc.) that are served to the user, we use mostly Cloudflare Workers or CloudFront, Amazon's Content Delivery Network and the content is served out of S3 buckets in AWS.

1.4.2 Network

For each environment, all network access to Workable products is split in two main domains; for Production this translates to:

- *.workable.com: reserved for user traffic.
- *.workableservices.com: reserved for server-to-server traffic and includes HTTP traffic from external third-party integrations.

All production and staging domains are proxied through Cloudflare. The traffic towards the Workable application is encrypted in transit (TLS and HSTS) and protected by WAF security controls such as bot-detection, rate limiting and firewall rules.

1.4.3 Computing Services

GCP provides infrastructure as a service; Workable application is hosted there.

1.4.4 Software

Workable follows a standardized sprint-based development process that includes all necessary steps from the design and requirement analysis phases to implementation, testing and release processes. Our stack contains multiple technologies such as Ruby, Java, NodeJS,

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

Go, Python, JavaScript, CSS/Sass and Swift.

1.4.5 Data

Workable uses multiple relational and non-relational databases for its applications. Each database server has an independent synchronous replica in a different availability zone within the same AWS or GCP region to mitigate the risk of data lost due to hardware failure. Data and log backups are kept redundantly on a regular basis in order to allow restoration of data within a reasonable point in time, if needed. Moreover, we have read-only replicas for our main databases which can be promoted to master if needed at any point in time.

Customer related objects are stored in AWS S3 or GCS buckets and for the most essential ones a backup is kept in GCP as well.

Workable application ensures that customer data is encrypted in transit and our data store configuration ensures that the data is encrypted at rest. Production data is stored in the US.

Workable Product processes the following categories of data:

- Customer data: customer details such as email, name, address, job role, company billing info etc.
- Candidate data: candidate information such as email, name, address, role, employer, photo, resume, emails, video interview, interview feedback, assessments, offer letter, etc.
- Employee data: employee profile data such as email, home address, job role, seniority level, salary, etc.

1.5 People

The Workable control environment is implemented, maintained and supported by the following teams:

Top management: Executives, Senior Vice Presidents, Vice Presidents are responsible for ensuring that:

- The communication of the security objectives across the company,
- Business requirements and client needs are considered during the SDL of the Workable Product,

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

- Appropriate resources are in place and allocated to each team, based on the strategic product priorities,
- All involved teams are aware of the technical priorities.

Human Resources & Recruitment teams is responsible for:

- The hiring process,
- The employee onboarding, awareness and training plan,
- The employee performance evaluation and career development,
- Spreading the company culture and values.

Finance team is responsible for:

- The financial and management reporting process,
- The Accounts payable cycle (vendor payments),
- The Order-to-cash cycle (billing to customer collections),
- The payroll process for four jurisdictions (US, UK, GR, Australia) and various contractors,
- Tax and statutory reporting compliance.

Operations: IT, Support, Tech-Ops, Implementation Managers, Account management, Data Management teams are responsible for:

- Providing technical support to clients, ensuring that all client requests are handled based on the provided services and internal procedures,
- Assisting clients to the implementation of any professional service (such as integration with existing systems, etc.),
- Assisting clients during the mitigation of any potential data breach, where appropriate.

Product: Development, Site Reliability Engineers, Quality Assurance, Data Science teams are responsible for:

- Ensuring that Secure Development process is implemented based on the Workable policies,
- Ensuring that backup policy is implemented to all workable components based on the criticality of the service and Workable Backup policy,
- Implement logical isolation of environments between clients,
- Security configuration and Systems monitoring (availability issues, resource capacity, etc.),

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

- Ensuring that all changes affecting the production environment are logged, traceable, approved and performed through structured methodology and tools (i.e.: gitops),
- Fixing on time any identified issues derived from the security assessments,
- Cooperating with Legal and Security Teams during security incident investigations.

Marketing: Content, Analytics, Ops teams are responsible for:

- Designing all marketing materials,
- Coordinate any marketing events / campaigns,
- Managing the content of Workable social media and websites.

Sales: Account Executive, Sales Development, Researchers, Sales-Ops teams are responsible for:

- Finding potential sales opportunities, arrange meetings with potential clients, present the features of the Workable Product and identify any custom requirement,
- Communicating with existing clients in order to discuss any issues or custom needs (i.e. new features, tailor-made reports, etc.).

Legal team is responsible for:

- Interacting with the Security team and DPO, as required in order to ensure Workable's compliance with applicable legislation,
- Monitoring any new regulations on data protection and updating the company's policies as applicable,
- Assessing any new vendors - customers in regard to legal terms and data protection.

Security team is responsible for:

- Contributing to the definition of security mechanisms for the Workable cloud infrastructure,
- Reviewing the cloud providers security controls (e.g. ISO certifications, SOC reports, etc.), where appropriate (i.e. during the selection of the provider- prior the contract phase),
- Security monitoring and maintenance of Workable Perimeter (WAF, etc.),
- Conducting Security Assessments,
- Communicating internal audits and security assessments results to the appropriate teams,
- Cooperating with Legal, DPO and SRE (or other teams) during the investigation phase of an incident.

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

1.6 Policies and Procedures

Workable has developed, documented and communicated to interested parties information security policies and procedures that contain rules and requirements that are met by Workable staff in the delivery and operations of the Workable Product. The Security Policies and Procedures are derived from the ISO/IEC 27001:2022 and ISO/IEC 27017:2015 standards and are augmented to address relevant regulatory and industry requirements for the Workable Product.

These Policies and Procedures cover (but are not limited to) the following security domains:

- Infrastructure and device hardening,
- Network segregation and filtering,
- Logging, monitoring and alerting,
- Business continuity,
- Incident management,
- Internal audit,
- Security Awareness,
- Risk assessment,
- Operational procedures (account request, change management, etc.),
- Teams' procedures (customer support, tech ops, legal, IT, HR, security etc.).

And the following IT policies and procedures:

- User Account Management,
- Change Management,
- Entitlement Review,
- Testing,
- Logging and Monitoring,
- Backup Policy,
- Roles and Responsibilities.

These policies and procedures are reviewed and updated, as necessary, at least annually, or more frequently, in case of a significant security event, or upon significant changes to the service or business model, legal requirements, organization of the Workable Product.

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

1.7 Principal Service Commitments and System Requirements

Workable designs its processes and procedures to meet its objectives for the Workable Product. Those objectives are based on the service commitments that Workable makes to user entities, the laws and regulations that govern the provision of the Workable Product, and the financial, operational, business and compliance requirements that Workable has established for the system.

Security commitments to user entities are documented and communicated in the terms of Services Workable Product through the Standard Service Agreements with other vendors and enterprise customers.

The security, availability, and confidentiality commitments include, but are not limited to, the following:

- Security and confidentiality principles inherent to the fundamental design of the Workable Product are designed to appropriately restrict unauthorized internal and external access to data and customer data and ensure such data is appropriately segregated from other customers.
- Workable data is encrypted in transit using security best practices (e.g.: HSTS) and the latest recommended secure cipher suites and protocols. All data stored within the production services utilized are encrypted at rest based on latest security best practices (e.g.: AES). Sensitive data - such as employee information - is encrypted in-use using data keys unique per customer.
- Production cloud infrastructure is hosted in a high-availability architecture in order to ensure service availability and performance with redundancy and failover.
- Appropriate tools and monitoring procedures are in place in order to ensure that all systems are functioning properly.
- Disaster Recovery and Business Continuity plans are in place and tested at least once per year.

Workable establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Workable system policies and procedures, system design documentation, and contracts with customers. These include policies around how the system 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

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

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 Workable Product.

1.8 Description of the Control Environment, Information, Communication, Monitoring and Risk Assessment Processes

This section provides information about the five interrelated components of internal control at Workable:

- Control Environment – sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
- Control Activities – include policies and procedures that help make sure that management's directives are carried out.
- Information and Communication – are systems, both automated and manual, that support the identification, capture and exchange of information in a form and time frame that enable people to carry out their responsibilities.
- Monitoring – is a process that assesses the quality of internal control performance over time and compliance with relevant laws and regulations.
- Risk Assessment – is the entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks can be managed.

Workable's internal control components include controls that may have a pervasive effect on the organization, an effect on specific processes, and security controls intended to effectively protect client data and provide a stable environment for availability of Workable's client-facing services. Some of the components of internal control include controls that have more of an effect at the entity level, while other components include controls that are primarily related to specific processes or applications.

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

workable

SECTION D - AICPA TRUST SERVICES CRITERIA

AICPA Trust Services Criteria

The AICPA trust services criteria, included in the scope, relevant to security, availability and confidentiality set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (AICPA, Trust Services Criteria).

Categories

Security - Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives.

Availability - Information and systems are available for operation and use to meet the entity's objectives.

Confidentiality - Information designated as confidential is protected to meet the entity's objectives.

Category	Criteria
CC1.0 Control Environment	CC1.1 The entity demonstrates a commitment to integrity and ethical values.
	CC1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
	CC1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
	CC1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
	CC1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
CC2.0 Communication	CC2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

and Information	CC2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
	CC2.3 The entity communicates with external parties regarding matters affecting the functioning of internal control.
CC3.0 Risk Assessment	CC3.1 The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
	CC3.2 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 The entity considers the potential for fraud in assessing risks to the achievement of objectives.
	CC3.4 The entity identifies and assesses changes that could significantly impact the system of internal control.
CC4.0 Monitoring Activities	CC4.1 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 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.
CC5.0 Control Activities	CC5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
	CC5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives
	CC5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
CC6.0 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.

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

	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, considering 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
CC7.0 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.

Docusign Envelope ID: A5E5253C-37D1-441C-8075-68234CC83F9B

	CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.
CC8.0 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.
CC9.0 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.
A1.0 Additional Criteria for Availability	A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
	A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.
	A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.
C1.0 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.