SoftwareOne AG, Stans, Switzerland

SYSTEM AND ORGANIZATION CONTROLS REPORT (SOC3)

Cyber Security Practice

Relevant to Security, Availability and Confidentiality

For the period April 1, 2022 to March 31, 2023

Report of Independent Service Auditors issued by

JAY MARU CPA LLC

Contents

Report of Independent Service Auditor

Report of Independent Service Auditor

To

Management of SoftwareOne AG
Stans, Switzerland

Scope

We have examined management's assertion, contained with the accompanying "Assertion of SoftwareOne Management" (assertion) that, SoftwareOne controls over the Cyber Security Practice (system) were effective throughout the period from 1st April, 2022 to 31st March, 2023, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security (applicable trust services criteria) set forth in the AICPA's TSP Section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy.*

Service Organization's Responsibilities

SoftwareOne is responsible for its service commitments and system requirements for designing, implementing, and operating effective controls within the system to provide reasonable assurance that SoftwareOne service commitments and system requirements were achieved. SoftwareOne has provided the accompanying assertion titled "Assertion of SoftwareOne Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. SoftwareOne is also responsible for preparing 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 assertion, 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

management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion which includes:

a) Obtaining an understanding of SoftwareOne's relevant security policies, processes and controls
b) Testing and evaluating the operating effectiveness of the controls and
c) Performing such other procedures as we considered necessary in the circumstances.

The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Inherent limitations

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 SoftwareOne's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to future of any conclusions about the suitability of the design or 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, SoftwareOne's controls over the system were effective throughout the period April 01, 2022 to March 31, 2023, to provide reasonable assurance that its principal service commitments and system requirements were achieved on the applicable trust services criteria.

Jay Maru, CPA

Date: 07-August-2023

Assertion of SoftwareOne Management

28th July 2023

Assertion of SoftwareOne Management

We are responsible for designing, implementing, operating and maintaining effective controls within the ***SoftwareOne Cyber Security Practice*** (System) throughout the period April 01, 2022 to March 31, 2023, to provide reasonable assurance that SoftwareOne's service commitments and systems requirements relevant to security were achieved. Our description of the boundaries of the system is presented in the section of this report titled "SoftwareOne Description of the System", (description) and identifies the aspects of the system covered by our assertion.

SoftwareOne utilizes SOC 2 Type 2 compliant AWS and Azure infrastructure for hosting its service environment. The description includes only the controls of SoftwareOne and excludes controls of the subservice organizations. The description also indicates that certain trust services criteria specified therein can be met only if the subservice organization controls contemplated in the design of SoftwareOne controls are suitably designed and operating effectively along with related controls at the service organization. The description does not extend to controls of the subservice organizations.

The description also indicates that certain trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of SoftwareOne's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of user entities.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 01, 2022 to March 31, 2023, to provide reasonable assurance that SoftwareOne's service commitments and system commitments were achieved based on the rust services criteria relevant to Security (application 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).

SoftwareOne's objectives for the system in applying the applicable trust services criteria are embodies 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 the accompanying system description.

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 April 01, 2022 to March 31, 2023, to provide reasonable assurance that SoftwareOne's service commitments and system requirements were achieved based on the applicable trust services criteria relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, if subservice organizations applied the complementary subservice organizations controls assumed in the design of SoftwareOne's controls throughout the period April 01, 2022 to March 31, 2023.

Chief Executive Officer/ CISO Ravindar Bindra

Date : 28 July 2023

Description of SoftwareOne Systems

About the Organization

Company Background

SoftwareOne is a leading global provider of end-to-end software and cloud technology solutions, headquartered in Switzerland. With an IP and technology-driven services portfolio, it enables companies to holistically develop and implement their commercial, technology and digital transformation strategies. This is achieved by modernizing applications and migrating critical workloads on public clouds, while simultaneously managing and optimizing the related software and cloud assets and licensing. SoftwareOne's offerings are connected by PyraCloud, its proprietary digital platform and Cyber security practice which provides customers with data-driven, actionable intelligence. With around 9000 employees and sales and service delivery capabilities in 90 countries, SoftwareOne provides around 65,000 business customers with software and cloud solutions from over 7,500 publishers.

Core Values

SoftwareOne's seven core values are the foundation of the company – they've been there from the start and really are the DNA of organization. They represent the way we behave towards each other, our colleagues and our customers, and drive our approach to work and business. They underpin the entire employee lifecycle and are a core part of both our recruitment process as well as employee development and growth.

The core values are: Humble, Customer Focused, Employee Satisfaction, Passionate, Speed, Integrity and Discipline.

Code of Conduct

The SoftwareOne Code of Conduct is for employees and Board members as well as for SoftwareOne Partners. The Codes serves to guide the actions of our staff and our partners, including customers, software licensors, sub-contractors and suppliers.

These Codes describe our values and assist our staff in doing the right thing and abiding by the rules wherever we operate around the world. The Codes also set out the expectations that we have for our partners, which we require to commit to the same standards of ethical conduct and integrity as we expect ourselves.

Control Environment

Executive Board

The Executive Board is the overall and final body responsible for all decision-making within SoftwareOne. The Board is composed of experienced executives, with a broad and diverse range of technology, financial, sales, and general business experience. Executive Leadership (Management) Team serves as the link between the Executive Board and Operational level management. The Management plays a critical role in the operations of the Company. The Management has representation from all business functions and serves as the multidisciplinary decision making body of the Company. The Management meets on a weekly basis to discuss operational matters for quick decision making and implementation, and monthly to discuss strategic aspects of the business. The mandate of the Management is to ensure the business is executing the defined strategy.

Information Security Team

The information security team is led by the Chief Information Security Officer (CISO). The team defines security policies and is responsible for security governance, training and awareness, product and platform security and security operations.

Business IT (BiT) Team

BiT Team is led by the Chief Information Officer (CIO) and is broadly divided into two sub-teams viz. infrastructure and product.

The infrastructure team is responsible for the architecture of the Services which exists across the Azure/ Amazon Web Service environment and for the design and implementation of adequate and appropriate measures for ensuring that security and confidentiality requirements are met.

Sales, Service, Support & Marketing

The sales, services, support and marketing functions are organized into the geographical segments in which they operate. These division spearhead the marketing, sales and service initiatives and are responsible for positioning SoftwareOne's services in the global market.

Finance

The Finance team is responsible for meeting financial reporting compliance requirements, as well as corporate compliance and risk management, and is led by the Chief Financial Officer.

Legal and Compliance

The legal team is responsible for ensuring compliance with the legal requirements across the organization.

Human Resources

The human resource team is led by the Director-HR and is responsible for identifying, on-boarding and retaining suitably qualified team members, overseeing ongoing training and education requirements and off-boarding terminated personnel.

Training and Awareness

An information security education and awareness program has been established that includes policy training and periodic security updates to SoftwareOne personnel. New hires and existing employees are required to undergo Information Security Awareness Training via training portal.

Information security related policies and procedures are communicated to the employees during the induction training and are made accessible to employees via the SharePoint. Personnel using mobile computing devices/teleworking are trained on the risks, the controls implemented, and their responsibilities.

SoftwareOne has developed, implemented, and maintained a comprehensive privacy protection awareness and training program to educate relevant personnel on their responsibilities of protecting PII and organizational procedures. Also, modules related to privacy protection and awareness are also covered during the Information Security training conducted for all employees.

The training focused on the technology domain, soft-skills, and behaviour are conducted periodically for employees as part of the learning and capabilities development initiatives of the organization.

Communication and Information

SoftwareOne utilizes various methods of communication to help ensure employees understand their roles and responsibilities and the entity's controls. SoftwareOne's knowledgebase is hosted on their intranet to disseminate information to employees. SoftwareOne has established various communication channels to communicate with external stakeholders. SoftwareOne provides periodic reporting on operations and other relevant reports as agreed with the clients.

Information Security

SoftwareOne has a formal information security protection program based on ISO 27001: 2013 framework and periodically certifies its compliance with the standards. The information security policy is formally documented, actively monitored, reviewed, and updated to ensure its objectives continue to be met.

An organizational structure is defined for information security which details the reporting lines, authorities, and responsibilities for business operations. The roles and responsibilities of the members of the information security organization are defined. Information Security Policy and information security-related procedural documents for processes are made available to the employees.

Services Provided

SoftwareOne has 24*7 Security Operations Centre to cater to its own and their clients' information security requirements. The in-scope software and applications are as follows:

- Microsoft M365 Security and Compliance
- Email Security – Proof Point
- Endpoint Security – Microsoft Defender
- Server Security – Trendmicro, Microsoft Defender, Qualys and Cloud Raxak
- Security User Awareness- Knowbe4
- Threat Management – Splunk SIEM
- Authentication Services - CyberArk
- Internet Security - Zscaler

Principal Service Commitments and System Requirements

SoftwareOne designs its processes and procedures related to its platform to meet its objectives for Cyber Security Practice. Those objectives are based on the service commitments that SoftwareOne makes to user entities, the laws and regulations that govern the provision of its services, and the financial, operational and compliance requirements that SoftwareOne has established for the services. The Cyber Security Practice of SoftwareOne is subject to the security and privacy requirements of state and local privacy security laws and regulations in the jurisdictions in which SoftwareOne operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offerings provided online.

Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Cyber Security Practice that are designed to permit system users to access the information they need on their role in the system while restricting them accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

SoftwareOne establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in the SoftwareOne's 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, and 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 Cyber Security Practice.

Business Continuity Commitments:

The IT infrastructure of the organization is being managed and maintained in the Cloud with adequate redundancy. The critical success factor for effective business continuity is the

human resources. To tackle this, the human resources are spread across all locations with adequate cross function training. In addition, the employees can also access the cloud environment from their place of stay/ home through secure VPN.

The RTO for SoftwareONE critical servers is defined as 24 hours and RPO for services covered in BCP shall not exceed 8 hours.

The SLA, RTO and RPO for client services are defined in the respective client contracts.

System Components

Services provided by a Third Party

SoftwareOne's facilities do not host any systems that transmit, process, or store Restricted Information. SoftwareOne uses Azure / Amazon Web Service cloud platforms for its services. Azure's / Amazon's controls are reviewed annually via third party attestation reports to provide SoftwareOne with comfort the control environment deployed by both Azure/ Amazon on its behalf aligns with the SoftwareOne Security and Confidentiality governance framework.

Services offered by business partners

SoftwareOne has engaged business partners for offering services to its customers. However, all the system configuration and maintenance are managed by SoftwareOne and the business partners services are limited to customer service only.

Infrastructure

The primary infrastructure used to provide SoftwareOne's services system includes the following:

Platform	Type	Purpose
AWS	S3	Source code repository
	IAM/ AWS SSO	User Access Management
	EC2	Virtual Machine
	VPC	Virtual Network
	ELB – Elastic Load Balancing	Load Balancing
	RDS	Database Services
	Security groups / NACL	Firewall
	Cloud trail	Log Monitoring

Platform	Storage Account	Source code repository
AZURE	IAM / Identity Protection/ Privilege identity management	User Access Management
	VM	Virtual Machine
	V Net	Virtual Network
	Load Balancers	Load Balancing

Platform	Storage Account	Source code repository
	NSG	Firewall
	Log analytics	Log Monitoring
	Microsoft 365 Security	Endpoint/E-mail/office/ identity and cloud apps security
	Compliance and Data Protection	Data classification labelling and Microsoft 365 DLP, Microsoft Purview
	Microsoft Defender	Defender for endpoint, Defender for cloud, Defender for O365

Software

SoftwareOne has 24*7 Security Operations Centre to cater to its own and their clients' information security requirements.

The primary Software used to by SoftwareOne's Cyber Security Practice includes the following:

Primary Software			
Product	**Technology**	**Operating Systems**	**Remarks**
Proofpoint	Email security	OS not known	Vendor hosted SaaS.
Trend Micro CloudONE	Cloud workload security		
KnowB4	Security awareness training		
M365 Security and Compliance	Workplace security		
ZScalar	Secure web gateway		
Microsoft Defender	Endpoint security		
Cloud Raxak	Security configuration management	Ubuntu 18.04	SoftwareOne hosted infrastructure
Splunk SIEM	Security Incident & Event management	Ubuntu 16.04	
CyberArk	Privileged access management	Window Server	SoftwareOne hosted infrastructure

Cyber Security Practice

Cyber Security Practice is organized in the following functional areas.

- Global Security Practice
- Cyber Security Leadership Team (CSLT)
- Cyber Security Incident Response Team (CSIRT) – Cyber Defence Centre (CDC) & Security Operations Centre (SOC)
- Security Engineering
- Global Service Delivery Lead
- Security Assurance, Audit & Compliance

Procedures

SoftwareOne has developed the Information Security Management System (ISMS) policies and procedures. The policies and procedures are reviewed and changes if any, are authorized by the Information Security Steering Committee.

Policy documents cover the following key areas –

- Asset Management
- Change Management
- Information Classification
- Information Security Continuity
- Acceptable Data Collection and Usage
- Bring Your Own Device
- Work From Home
- Network Management
- Monitoring
- Encryption
- Information Access Control Management
- Data Protection and Privacy
- Data Retention and Disposal
- Security Incident Management

- Information Security
- Information Security Risk Management
- Intellectual Property Rights
- Malicious Code Protection
- Password
- Personnel Security
- Remote Access Security
- User Account Management
- Email, Internet Usage
- Removable Media Usage
- Software Usage
- Backup & Restoration
- System Acquisition, Development and Maintenance
- Social Media
- Supplier Information Security
- Open Source Software
- Patch Management
- Physical Security
- Information Security Awareness and Training

Separate policies and procedures are defined for Business Continuity and Disaster Recovery, which are tested on a periodic basis.

All policies are kept up to date and reviewed and approved by the Management on an annual basis, or more frequently as necessary (for example, based on an updated risk assessment).

Data

SoftwareOne has defined and documented the Asset Management Policy to ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

SoftwareOne's data is classified as:

- Public Information
- Internal Information
- Confidential Information
- Private
- Customer confidential
- Customer Private

Processes and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the SoftwareOne policies and procedures that define how services should be delivered. These are located on the Company's SharePoint and can be accessed by any SoftwareOne team member. They are reviewed annually and modified as soon as required to maintain relevance to current operational requirements

Physical Security

Production Environment Physical Access:

All restricted data is stored at a SoftwareOne secured facility, which is hosted within Microsoft Azure / Amazon. Controls for ensuring physical and environmental security are implemented and managed by Azure / Amazon and are therefore out of scope for this report.

The Physical Security Policy sets out the minimum-security standards for an acceptable secured facility. SoftwareOne relies on third party attestation reports provided by Azure / Amazon for ascertaining the design and operating effectiveness of physical and environmental security controls.

Identity & Access Management

User Account Management:

Access to in-scope systems is granted on a "need to know" and "least privilege" basis. Role based access privileges are enforced by access control systems, where configurable. General access to in-scope systems is authorized by respective managers. The initial setting of, and subsequent changes to, access privileges is approved by respective managers. Revocation of access for terminated personnel is performed by BiT Team in a timely manner via a process managed by the HR Team.

Access Review:

Half Yearly review of privileged user access rights and annual review of normal user access rights are carried out to ensure the level of access is appropriate. Any access, which is deemed to be no longer required, is identified and disabled.

Customer Portal Access Management:

Administrative access to the Customer Portal (Tenant Portal) is provisioned for an authorized customer representative following execution of an Addendum/ Statement of Work (SoW). The customer administrator is responsible for managing and monitoring access to the customer portal, including optional enforcement of dual factor authentication. All customer accounts and administrative access to the Customer Portal will be revoked following termination of an Addendum / SoW. The customer portal enforces minimum required password settings including the disabling of user accounts after a limited number of unsuccessful logons for a specified duration.

Password Management

There is a defined password policy configured on the domain controller specifying minimum password length, maximum password age, password complexity requirement, and account lockout. The organization's password requirements are documented in Password Policy published, communicated, and made available to all employees via SharePoint. In-scope system components require a unique username and password before authenticating users. Before deploying any new devices in a network environment, the organization changes all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.

Backups

SoftwareOne has a Backup and Restoration policy that governs the performance of data and data restoration. Azure / Amazon services are utilized to maintain a rolling backup of all Restricted Information. Alerts for failed backups are raised for resolution via log monitoring processes.

Restorability and integrity of backups is periodically assessed and provides confirmation of Disaster Recovery capabilities.

Security Incident Management

Security Incidents:

The SoftwareOne team follows documented incident response plans for specific scenarios, which could impact a service. All security incidents are notified to the relevant stakeholders in SoftwareOne based upon identification. The Incident Manager will involve adequate

resources to assess and resolve the incident based on severity and impact. Incidents are recorded in "ServiceNow" ticketing tool. Appropriate communication is updated to the relevant stakeholders about the incident.

Post Incident Reviews:

If the incident was categorized as a major security incident, the CISO will conduct a Post Incident Review. The main purpose of the Post Incident Review is to evaluate the response to an incident and derive learnings from it. Any major security incidents are raised and discussed with the Management.

Audit Logging & Monitoring

Logging and monitoring tools are used to collect data from in-scope systems to monitor system performance, potential security threats and vulnerabilities, and resource utilization; and to detect unusual system activity or service requests. Logs are reviewed as required to investigate issues, as also part of a formalized weekly health check. Any issues identified are logged and tracked to find resolution. Logs collected are aggregated, analyzed and investigated using the tool.

Ongoing Monitoring

Automated Monitoring Systems:

SoftwareOne uses a wide variety of automated monitoring systems, which cover security, service performance and availability. Monitoring tools are implemented to detect and protect against external and internal threats. System performance including availability is also continuously monitored through a specific set of tools and control procedures.

Client Services:

A dedicated Client Services team is in place to service customer requests and monitor customer feedback for performance, which makes its way back to the respective teams to action for resolution. External customers communicate with Client Services through the SoftwareOne application and email.

Patch Management

An immutable infrastructure is in place comprised of immutable components that are replaced at each redeployment, rather than updated. Controls for ensuring patching of environments are implemented and managed by Azure / Amazon and are therefore out of scope for this report.

Change Management

SoftwareOne follows an agile development process that includes being able to iteratively roll out functional and non-functional changes (standard, normal and emergency changes) while targeting both high quality and high applicability. Management has documented change management policy and processes to communicate management's expectations in regard to performing changes to the production environment. This policy and processes apply to all changes to the production environment and convey the change control process including assessing the impact of changes, testing, rollback procedures, approval requirements, and change communication to relevant stakeholders. In addition, change management team (support team) will prioritize / categorize the change request based on the impact and risk. Depending on the type of change the support team will create the ticket in the automated tool and will prepare the implementation, test and roll-back plans. The Change Advisory Board (CAB) will assess the change and once approved the change will be implemented.

Change Request Initiation and Control Infrastructure Changes:

Infrastructure changes (such as new servers, server patches, firewall rule changes, configuration changes, global changes to the hypervisor, network or storage components etc.) are raised through the ServiceNow. The CAB will assess the change and once approved the change will be implemented.

System Boundaries

The scope of this report includes the Services performed by SoftwareOne. This report does not include the datacentre hosting services provided by AWS or Azure.

Common Criteria (to the Security, Availability, and Confidentiality Categories)

Security refers to the protection of

a) information during its collection or creation, use, processing, transmission, and storage

b) systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removals of information or system resources, misuse of software licenses, and improper access to or use of, alteration, destruction, or disclosure of information.

Risk Management

Oversight of information security risk at a corporate level is undertaken by the Management and is managed by the CISO. Information security is a standing item on the agenda of the Management meetings, and the Management considers key risks for which high level governance and management decisions are required.

SoftwareOne has a formalized risk management process and maintains a Risk Register which tracks key risks to the organization, including information security risks. Risk assessments include a review of internal and external factors that threaten the achievement of business objectives. Mitigating controls are identified for all risks and risks with residual scores above the acceptable risk threshold have mitigating actions agreed that are then tracked by the Information Security team.

Risk Assessment

SoftwareOne generates information on information security risks from the following sources:

- Risk assessment by the CISO and third-party contractors in relation to business assets.
- Risk assessment by internal business and software development teams during the development of new or updated product features.
- Regular penetration testing by third party specialists.
- Regular vulnerability assessments of the systems.
- Alerting services providing real-time information on security trends and threats.
- Operational data and alerts from application and infrastructure log analysis.
    a) Ongoing monitoring of compliance activities and trends by the CISO and CIO
    b) Review of user logs of privileged users, showing system login attempts and failures
    c) Subscription to relevant newsletters and attendance at relevant forums

Information security risks are managed through a number of processes:

- Service level controls for risks that have been identified by risk and threat assessment, penetration or vulnerability testing are managed by the respective teams.

- Infrastructure risks, including infrastructure patching and configuration, are managed as an integral part of operational management processes by the BiT team, who are also responsible for infrastructure security monitoring.
- Application security monitoring, including anomalous application behaviour detection and response, is managed by the respective teams.

Controls at Subservice Organizations

SoftwareOne uses Azure / Amazon as a subservice organization to provide services, which form part of the SoftwareOne Identify service to be used by SoftwareOne's customers, including: Identity and Access Management (IAM), cloud computing (EC2), Elastic Block Storage (EBS) and electronic storage (S3).

As the controls related to the following Control Objectives are fully outsourced to Azure/Amazon the following Control Objectives have been carved-out of scope:

- Physical access to cloud facilities housing the system (for example, data centres, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and confidentiality.

SoftwareOne has an established monitoring program over controls which have been outsourced to subservice organizations.

Common criteria to all in-scope trust service principles

The following controls were evaluated during the SOC2 Type2 audit to determine the effectiveness of controls implemented, for the given selected samples and **NO EXCEPTIONS** were found.

CC1.0 Control Environment

Control Point	Criteria and controls specified by the Service Organization
CC1.1	***COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.***
	The Company has developed a clearly articulated statements of core values that is understood at all levels of the organization. The entity has code of conduct within the Employee Handbook that establishes standards and guidelines for personnel ethical behavior. Personnel are required to read and accept the entity's code of conduct All new employees have to read and sign the Confidentiality Agreement/NDA upon joining. As part of employee orientation, new hires are required to acknowledge their understanding and acceptance of the Acceptable Use Policy (AUP). Agreements are established with third parties/ partners/ subcontractors that include clearly defined terms, conditions, and responsibilities for third parties and subcontractors. Customer can provide their issues, complaints or feedback through email or Delivery Team. Employees can raise their complaints and grievances to HR. Cyber Security Practice of the company has the following certifications. 1. ISO 27001
CC1.2	***COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.***
	CISO conduct meetings at monthly intervals to discuss the security level, changes, technology trends, occurrence of incidents, and Cyber Security initiatives. The Management team meets weekly and discuss the business as well as operational issues

Control Point	Criteria and controls specified by the Service Organization
CC1.3	***COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.***
	Organization charts are established that depicts authority, reporting lines and responsibilities for management of its information systems. These charts are communicated to employees and are updated as needed Organization has Information security related policies and procedures that describes information security processes, practices and organization. Information Security Policy & Procedures related to HR policies are reviewed and approved by the Management at least annually. The responsibility of managing Information Security is assigned to the Chief Information Security Officer (CISO). Allocation of information security responsibility is documented in ISMS Document. Company has Information security related policies and procedures that describes information security processes, practices and organization. Authority limits, delegation of powers and other responsibilities are in place for significant roles in Cyber Security Practice. Vendor SLA breaches are reported to Director, Cyber Security Practice.
CC1.4	***COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.***
	The company has documented HR Policies and procedures including recruitment, training and exit procedures. Job requirements are documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring and transfer process. New employees sign offer letter as their agreement and acceptance of broad terms of employment including a brief description of position and other terms. Management evaluates the need for additional resources in order to achieve business objectives as part of its periodic management meetings All critical roles within Cyber Security Practice have adequate succession planning to ensure that there is no business disruption.

Control Point	Criteria and controls specified by the Service Organization
	Internal HR Reference checks are conducted by HR team or the hiring manager through document verification and references checks with the former colleagues or managers provided in the resume. External third-party background verification checks are carried out for selected employees based on organization's policy. This includes education qualification verification, employment verification, address check and where necessary criminal checks. Negative BGV reports require further management action. Newly hired personnel are provided sufficient functional training before they assume the responsibilities of their new position The induction training given by HR includes information security training. In this training the HR, physical access and security policies are explained. An ISMS awareness refresher training is provided to all employees at least on annual basis. Compliance with training requirements is monitored in the form of periodic training calendar
CC1.5	***COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.***
	Roles and responsibilities are defined in written job descriptions and communicated to employees and their managers Grievance escalation mechanism for critical roles within CSP is established. Job descriptions are reviewed on an annual basis as part of performance appraisals. All Employees acknowledge the Code of Conduct annually. Performance appraisals are performed annually.

CC2.0 Communication and Information

Control Point	Criteria and controls specified by the Service Organization
CC2.1	***COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.***
	Adequate business MIS is generated on a monthly basis for information requirements. A standing meeting is carried out weekly to hold department discussion and status updates. Timely reporting to CISO is carried out internally by all teams of Cyber Security Practice.
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.***
	System boundaries in terms of logical and physical boundaries are documented. Network diagrams are in place. Customer responsibilities and system descriptions are provided in client contracts. Security policies are published on intranet / SharePoint. An organizational wide incident management process is in place Entity communicates its commitment to security as a top priority for its customers via contracts and website pages. System changes that impact internal and external users are communicated in a timely manner CSP Team communicates to external clients as per the client escalation process Maintenance/ downtime banners are displayed on client facing applications during maintenance window. Decisions regarding changes in confidentiality practices and commitments will be on need basis. CSP teams communicate these changes to the customers. New employees hired at senior levels are communicated to stakeholders through email.

Control Point	Criteria and controls specified by the Service Organization
CC2.3	***COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.***
	Company's security, availability and confidentiality commitments regarding the system are included in the client contracts / SOW Customer specific SLA are monitored as per the contractual terms. The reports are shared with customers as per their requirement. The induction training given by HR includes information security training. In this training the HR, physical access and security policies are explained. Customer responsibilities are described in client contracts / Master Service Agreement / Service Level Agreement Users are informed of the incident management/ security breaches reporting process during Induction (ISMS Training). Customer can provide their issues, complaints or feedback through email to Business Heads. Employees can raise their complaints and grievances to Management Changes to system boundaries, network systems are communicated to clients, if required. Incidents impacting external users are communicated to them through emails along with root cause analysis, if applicable.

CC3.0 Risk Assessment

Control Point	Criteria and controls specified by the Service Organization
CC3.1	***COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.***
	Business strategies and goals are set as part of the business planning process. Risk Assessment Scales (Risk Rating scales) are defined to evaluate and assess the significance of Risk. This is part of the Risk Management Framework. Need for additional resources are discussed during periodic management meetings
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.***
	Policies and procedures related to risk management are developed, implemented, and communicated to personnel. A risk assessment is performed annually or whenever there are changes in security posture. As part of this process, threats to information assets are identified and the risk from these threats are assessed. Identified risks are rated and prioritized based on their likelihood and impact. Risk Mitigation Plans and action trackers are in place to respond to risks.
CC3.3	***COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.***
	Patch Management for SOC devices are vendor initiated. Hardware inventory is maintained as part of the asset register. Company has defined a risk management process for evaluating risks based on identified vulnerabilities, threats, business impact and mitigating controls. Adequate access reviews are performed regularly to detect fraud with respect to data within applications and other information assets of CSP. Company's risk assessment covers privacy related risks.
CC3.4	***COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.***

Control Point	Criteria and controls specified by the Service Organization
	Controls are designed and mitigation strategies adopted in treating identified risks. Also changes to existing controls are recommended if warranted. Whenever new products or services are added or its business model changes, a risk assessment is carried out for the new service. Emerging technology and system changes are considered when performing risk assessment Vendor agreements, including any security, availability and confidentiality commitments, are reviewed by appropriate senior management during the procurement process.

CC4.0 Monitoring Activities

Control Point	Criteria and controls specified by the Service Organization
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.***
	The internal audit function conducts system security reviews half yearly. Results and recommendations for improvement are reported to management. Internal audit team is staffed with competent professionals with technical expertise. Approved internal audit calendar for the year 2022 is established. The audit calendar covers internal audit of Cyber Security Practice. System access is reviewed on a monthly basis. Vulnerability Assessment (VA) is done on demand basis, at least on a quarterly basis & Penetration Tests (PT) are performed annually.
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.***
	The internal audit function conducts system security reviews half yearly. Results and recommendations for improvement are reported to management. Firewall is configured to log events that are reviewed on an ongoing basis. In bound and outbound network traffic are being monitored on a continuous basis. Vulnerability Assessment (VA) is done on demand basis, at least on a quarterly basis & Penetration Tests (PT) are performed annually. Critical vulnerabilities reported during vulnerability assessment/ penetration testing are reviewed by Management.

CC5.0 Control Activities

Control Point	Criteria and controls specified by the Service Organization
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.***
	The internal audit function conducts system security reviews Half Yearly. Results and recommendations for improvement are reported to management. Segregation of duties is in place for Cyber Security Practice
CC5.2	***COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.***
	Vulnerability Assessment (VA) is done on demand basis, at least on a quarterly basis & Penetration Tests (PT) are performed annually. Internal audits including access reviews are performed every Half yearly. Results and recommendations for improvement are reported to management. Policies and procedures related to risk management are developed, implemented, and communicated to personnel. Azure Config tool is used for maintaining Azure Infrastructure. Azure Config tool records configurations of Relational Database services (RDS), Identity and Access Management (IAM), Simple Storage Service (S3), Elastic Compute Cloud (EC2), Virtual Private Cloud (VPC) and load balancer. Cloud Infrastructure is managed and maintained by the Business IT Team (BiT)
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.***
	The Company has implemented major policies and SOPs across the cyber security practice. Procedures are documented using various formats, such as narratives, flowcharts, and control matrices Significant policies and procedures are uploaded to the intranet and available for all employees that require access to these policies/procedures. All policies and procedures clearly define the roles & responsibilities for executing policies and procedures.

Control Point	Criteria and controls specified by the Service Organization
	The internal audit department assesses adequacy and relevance of policy and procedures during internal audits.

CC6.0 Logical and Physical Access Controls

Control Point	Criteria and controls specified by the Service Organization
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.***
	Company has documented policies for logical access controls Access is granted on least privileges basis as default and any additional access needs to be approved. Company has established hardening standards for production infrastructure that include implementation of security groups, access control, configuration settings, and standardized policies. Production hosts and Security Groups of Security Operations Centre (which are the equivalent of Firewalls) are hardened according to Industry best practices. Only the required ports are opened for inbound access at the load balancer level. Physical and logical diagrams of networking devices for office networks include routers, firewalls, switches and servers, including wireless, are documented. Vulnerability assessment is done on demand basis, at least on a quarterly basis & penetration tests are performed annually. Company does not allow customers or external users to access its systems. Infrastructure components and software are configured to use the Windows security using group policies & active directory. User credentials for employees are set up by the IT team against a request from HR. User access to applications hosted on Azure is granted as per the role. Access to application instances hosted on cloud for the clients is restricted to SOC support team and select client project team members based on the role and need. SOC Support team have admin rights and can add additional Entity's users on the client instances as per business requirements. Direct access to cloud infrastructure is possible only through encrypted SSH access by the BiT team. For Azure console access, Multi Factor Authentication is implemented for privileged users of CSP.

Control Point	Criteria and controls specified by the Service Organization
	The Company has a remote working policy that requires that external access is granted on a need basis. CSP maintains an up-to-date listing of all software. All Assets are assigned owners who are responsible for evaluating access based on job roles. The owners define access rights when assets are acquired or changed. Privileged access to sensitive resources is restricted to defined user roles and access to these roles must be approved by Management. Privileged access is authorized by the business owner based on the requirement and reviewed by CPS on a Monthly basis. Account sharing is prohibited and the same is controlled through Active Directory The following password parameters are in place for active directory: 1. length of 12 characters 2. complexity is enabled 3. password expires in 180 days 4. Password history is set at 5 Access to data is restricted to authorized applications through Active directory. User access to Company systems is given only against authorization. Access given to new employees is one of least privileges. Access to client systems is permitted by client on case-to-case basis. Such access is authorized and managed by the client. Company sends emails to clients regarding access request for new user on client projects. All confidential data is classified as per the Information Classification Policy
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.***
	On the day of joining, HR will send a mail to IT Helpdesk providing the details of the new joiners. The IT then provides necessary access as per request.

Control Point	Criteria and controls specified by the Service Organization
	Employee user accounts are removed from various application and network system as of the last date of employment manually based on access revocation request sent by HR department. Access on client systems is removed by sending an email to the client manager informing them about the exiting employee. When an employee leaves the organization, the employee's manager initiates the 'Exit Process'. HR informs respective teams / IT team within 24 hours to deactivate/delete the user ID from the email system and all applications. An exit checklist is used to ensure compliance with termination procedures. HR team sends the user deactivation list to IT team within 24 hours from the time an employee is terminated or the last working day. Privilege access to sensitive resources is restricted to defined user roles and access to these roles must be approved by Management. Company does not allow non-employees to access its systems.
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.***
	A role-based security process is setup in Active directory with groups and roles based on job requirements. A role-based security process has been defined within Azure infrastructure based on job requirements. Company does not allow reactivation of ID belonging to an exited employee.
CC6.4	***The entity restricts physical access to facilities and protected information assets (for example, data centre facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.***
	Entry to the all-office premises is restricted to authorized personnel. Physical access control system has been implemented to secure the facilities. Physical access to office premises is monitored through CCTV installed at key points within the premises. There is a security desk at the office entry manned by a security guard All visitors have to enter their details in the visitor register.

Control Point	Criteria and controls specified by the Service Organization
	Visitor badges are for identification purposes only and do not permit access to the facility. All visitors must be escorted by a Company employee when visiting office facilities. ID cards that include an employee picture must be worn at all times when accessing or leaving the facility. Physical access is setup by the Admin Dept for new joiners after all HR formalities are completed. ID cards by default does not have access to any of the sensitive areas. Physical access to sensitive areas / server rooms is granted only to privileged users / IT Team Access to such restricted zone is given against written approval by authorized official. A monthly review of physical access to sensitive areas against active employee list is carried out by IT. Upon the last day of employment, HR Team sends exit email requesting for deactivation of physical access for terminated employees. Physical access is deactivated by the Admin Team Employees are required to return their ID cards on the last day, and all ID badges are disabled. On a half yearly basis, Internal audit performs a reconciliation that physical access for terminated employees has in fact been deactivated in the physical access system. The sharing of access badges and tailgating are prohibited by policy.
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.***
	Removable Media Policy is implemented for procedures relating to disposal of information assets / equipment All data is erased from laptops and other media prior to destruction/ disposal
CC6.6	***The entity implements logical access security measures to protect against threats from sources outside its system boundaries.***

Control Point	Criteria and controls specified by the Service Organization
	External points of connectivity at office network are protected by firewall. The firewall provides unified threat management (UTM) services such as intrusion protection, web filtering and inbound and out bound traffic filtering. The production systems are hosted in AWS Cloud infrastructure and are protected by security groups set up for the virtual private cloud (VPC) provided by AWS. Only limited employees in the production team have access to production servers using SSH through a NAT gateway. Incoming connections are accepted from only whitelisted IPs in the firewall. Company has implemented a content filtering system through a firewall that blocks access to certain sites such as personal emails, storage etc. Access to modify firewall rules is restricted by management. There is no data stored outside production systems for any DR test. AWS environment has DR capabilities. Logical access to Company systems is restricted through active directory-based domain policies. Data stored in the cloud are encrypted supporting AES. Use of removable media is prohibited by policy for all desktops. For laptops given to senior managers, it is authorized by management. Connections to the Azure-hosted servers are through authenticated SSH sessions or authenticated secure browser session using HTTPS.
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.***
	Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted. VPN connections to both the corporate and cloud networks are encrypted.

Control Point	Criteria and controls specified by the Service Organization
	External users access applications hosted at cloud infrastructure (Azure) through secure https with SSL/TLS certificates. The production system at Azure is protected by security groups rules (virtual firewall) set up for the virtual private cloud (VPC) provided by Azure. VPC is used to protect all Production system hosted at Azure. database access is governed by security group policies and login credentials. Production database can only be accessed from production machines. Use of removable media is prohibited by policy for all desktops. For laptops given to senior managers, it is authorized by management. Backup media are encrypted during creation.
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.***
	Antivirus software is installed on workstations, laptops, and servers. This system provides antivirus system scans, email scans, content filtering and endpoint protection. Signature files are updated daily. Antivirus console provides compliance reports about non-updated machines. The ability to install software on workstations and laptops is restricted to IT support personnel through domain policies. No Local admin access is granted. Any viruses discovered are reported to BiT team either by the antivirus system or by the affected employees.

CC 7.0 System Operations

Control Point	Criteria and controls specified by the Service Organization
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.***
	Configuration and hardening standards are defined for all IT systems The entity monitors infrastructure and software for noncompliance with the policies/standards, which could threaten the achievement of the entity's objectives. Penetration testing is performed by on an annual basis Technical vulnerability is carried out in-house on demand and at least on quarterly intervals.
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 analysed to determine whether they represent security events.***
	The firewall protecting the corporate network notifies the IT team of suspicious activity. Alerts are responded to promptly. IT team receive requests for support through phones and emails, which may include requests to reset user passwords etc.
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.***
	A formal, defined incident management process is documented in Information Security Policies for evaluating reported events. Incidents are reported to the IT team. These are tracked.

Control Point	Criteria and controls specified by the Service Organization
	Reported incidents are logged as tickets and include the following details Severity Data and Time of incident Details Status Root Cause (High severity incidents only)
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.***
	Critical security incidents are reported to the Management. Root Cause Analysis, Corrective and preventive actions are done for all critical incidents. Change management requests are opened for events that require permanent fixes. Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives. Incident remediation plans for critical security incidents are communicated internally and if required, externally. Unauthorized access or disclosure of personal data is reported to Management. HR policies include code of conduct and disciplinary policy for employee misconduct.
CC7.5	***The entity identifies, develops, and implements activities to recover from identified security incidents.***
	Root cause analysis is performed for all critical incidents. Additional architecture or changes are considered to prevent recurrence of critical incidents. Lessons learned are analyzed, and the incident response plan and recovery procedures are improved. Lessons learnt are shared internally, if required.

CC8.0 Change Management

Control Point	Criteria and controls specified by the Service Organization
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.***
	Entity has defined its change management and approval processes in its information security policies. All change requests are logged and change request tickets created. Major changes are approved by Change Authorization Board (CAB) The change management process has defined roles and assignments thereby providing segregation of roles in the change management process. A risk assessment is performed on a periodic basis. The risk assessment includes identifying potential threats and assessing the risks associated with being identified. Change requests are created based on the identified needs. For high severity incidents, change requests are created. A process exists to manage emergency changes. Emergency changes, due to their urgent nature, may be performed without prior review.

CC9.0 Risk Mitigation

Control Point	Criteria and controls specified by the Service Organization
CC9.1	***The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.***
	Entity has a documented BCP and DR guideline to be used in the event of a crisis. Business continuity and disaster recovery plans, including restoration of backups, are tested annually.
CC9.2	***The entity assesses and manages risks associated with vendors and business partners.***
	Company obtains and reviews compliance reports and certificates such as ISO 27001, SOC1 or SOC2 for its cloud service provider. Opinion section and relevant controls are reviewed for any exceptions. This is part of vendor monitoring. A formal contract is executed between Company and Third-Party Service Providers before the work is initiated. Agreement includes terms on confidentiality, responsibilities of both parties. There is no information sharing with vendors or any third party. A confidentiality agreement is signed by all employees at the time of joining. In addition, NDAs are signed with third parties wherever required. Company has a limited number of vendors such as office lease, security service vendor and housekeeping services. There is no requirement for SOC2 for these vendors since there is no information shared with them. The entity obtains privacy commitments, consistent with the entity's privacy commitments and requirements, from vendors and business partners who have access to personal information. Vendor's/ Partner's compliance to entity's privacy commitments and requirements are assessed on a need basis.

A1 Additional criteria for Availability

Control Point	Criteria and controls specified by the Service Organization
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.***
	The Entity monitors system processing capacity and usage and takes correction actions to address changing requirements. Processing capacity for cloud infrastructure for Azure is monitored using Azure tools on an ongoing basis. Critical infrastructure components have been reviewed for criticality classification and assignment of a minimum level of redundancy.
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.***
	Environmental controls (like fire extinguishers and smoke detectors) have been installed to protect the perimeter area. CCTV is installed at key points for surveillance. Devices are checked on a periodic basis and checklists are prepared. Fire drill is conducted annually by the building administration. Uninterruptible power supply (UPS) devices are in place to secure critical IT equipment against power failures and fluctuations. DG set of sufficient capacity is provided to provide power during outage. Company has multiple ISPs in place to provide redundancy in case of link failure Temperature in server room is monitored on a daily basis to corrective actions in case of discrepancy. Vendor warranty specifications are complied with and tested to determine if the system is properly configured. Facilities and admin personnel monitor the status of environmental protections on a regular basis. Maintenance checklists are used where applicable. Backup policy is defined in the information security policies.

Control Point	Criteria and controls specified by the Service Organization
	Automated backup systems are in place to perform scheduled differential and full back up of production systems and internal office data. Local office backup taken on OneDrive. Frequency of data backup is multiple times a day. Automated backup systems are configured to send alert notifications to IT personnel regarding backup completion status. No backups are performed on external hard drives or tapes
A1.3	***The entity tests recovery plan procedures supporting system recovery to meet its objectives.***
	Disaster recovery and Business Continuity plans and procedures for various disruption scenarios are documented for all in scope systems. Business continuity plans, including restoration of backups, are tested at least annually for all in scope systems.

C1 Additional criteria for Confidentiality

Control Point	Criteria and controls specified by the Service Organization
C1.1	***The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.***
	Retention period and secure destruction of confidential information is established. Destruction of confidential information no longer needed is ensured.
	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.
	Retention period and secure destruction of confidential information is established. Destruction of confidential information no longer needed is ensured.

End of Report