SoftwareONE AG, Stans

SYSTEM AND ORGANIZATION CONTROLS REPORT (SOC3)

Cyber Security Practice

Relevant to Security, Availability, Confidentiality, Processing Integrity, and Privacy

For the period April 1, 2021 to March 31, 2022

Contents

Independent Service Auditor's Report

To

Management of SoftwareONE, AG Stans

Scope

We have examined management's assertion, contained with the accompanying "Assertion of SoftwareONE, AG Stans Management" (assertion) that SoftwareONE controls over the Cyber Security Practice (system) were effective throughout the period from 1st April, 2021 to 31st March, 2022, 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, 2021 to March 31, 2022, to provide reasonable assurance that its principal service commitments and system requirements were achieved on the applicable trust services criteria.

Jay Maru, CPA
License No. 41401
State of Washington

Date: 01-June-2022

Assertion of SoftwareONE Management

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, 2021, to March 31, 2022, 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 (subservice organization) for hosting its service environment. The description indicates that certain applicable trust services criteria can only be met if controls at the subservice organizations are suitably designed and operating effectively. The description presents SoftwareONE's system and its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organizations to meet certain applicable trust services criteria. The description does not include any of the controls implemented at the subservice organizations. Our examination did not extend to the services provided by the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 01, 2021 to March 31, 2022, to provide reasonable assurance that SoftwareONE's service commitments and system commitments were achieved based on the trust 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 1st April, 2021 to 31st March 2022, 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 1st April, 2021 to 31st March 2022.

DocuSigned by:
Bala Sethuraman
78EA2093D9964ED...

Chief Executive Officer/ CISO

Date: 20 May 2022

Description of SoftwareONE Systems

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 8,700 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 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:

- Future Workplace Security Solution – Proof Point, Trend Micro ApexONE, KnowBe4 and M365 Security and Compliance
- Future Datacentre Security Solution – Trend Micro Deep Security, Cloud Raxak and Splunk SIEM
- Authentication Security Solution - CyberArk

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 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.

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	Type	Purpose
Azure	Storage Account	Source code repository
	IAM / Identity Protection/ Privilege identity management	User Access Management
	VM	Virtual Machine
	V Net	Virtual Network
	Load Balancers	Load Balancing
	NSG	Firewall
	Log analytics	Log Monitoring
	Microsoft 365 Defenders	Endpoint/E-mail/office/ identity and cloud apps security
	Compliance and Data Protection	Data classification labelling and Microsoft 365 DLP

Software

The primary Software and applications used by SoftwareONE's Cyber Security Practice offering includes the following:

Primary Software				
Services	**Tools**	**Purpose**	**Operating Systems**	**Remarks**
Future Workspace Security Solution	• Proofpoint • ApexONE • KnowB4 • M365 Security and Compliance	• Email security Endpoint security • Security awareness training • Subscription based endpoint & workplace security	NA	Vendor hosted SaaS. Hence OS not required/known
Future Datacentre Security Solution	• Trend Micro Deep Security • Cloud Raxak • Splunk SIEM	• Cloud workload security • Security configuration management • Security Incident & Event management	• Amazon Linux • Ubuntu 18.0 • Ubuntu 16.04	SoftwareONE hosted infrastructure
Authentication Security Solution	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)
- Computer 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
- Access Control
- Back up and Restoration
- Bring your own device
- Business Continuity
- Change Management
- Code of Conduct
- Customer Offboarding
- Data Centre Physical Security
- Data Protection and Privacy
- Data Retention and Disposal
- Email Usage
- Human Resource Security
- Internet Usage
- Information Classification
- Information Risk Management
- Information Security
- Legal and Contractual
- Monitoring
- Network Management
- Offshore Development Centre Security
- Password
- Remote Access Security

- Removable media and usage
- Security Incident Management
- Software Usage
- Supplier Information Security
- System Acquisition, Development and Maintenance
- Vulnerability and Patch Management
- Whistle blowing

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.

User Access Review

A half yearly review of user access rights is completed 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

SoftwareONE team follows documented incident response plans for specific scenarios, which could impact a service. Security incidents which arise are notified to the relevant stakeholders in SoftwareONE based on severity. The Incident Manager will involve adequate resources to resolve the incident based on severity and impact. Incidents are recorded in "ServiceNow" ticketing tool. Appropriate communication will be 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.

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 and

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 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.