SoftwareOne AG, Stans, Switzerland

SYSTEM AND ORGANIZATION CONTROLS (SOC 3) REPORT

Cyber Security Practice

Relevant to Security, Availability and Confidentiality

For the period April 1, 2025, to March 31, 2026

Report of Independent service auditor issued by

Precision Assurance

Contents

Report of Independent Service Auditor 3
Assertion of SoftwareOne Management 6
Description of SoftwareOne Systems 8

Report of Independent Service Auditor

To

Management of SoftwareOne AG

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, 2025 to 31st March, 2026, 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, 2025, to March 31, 2026, to provide reasonable assurance that its principal service commitments and system requirements were achieved on the applicable trust services criteria.

Precision Assurance CPA LLC

Certified Public Accountants
License No. CF - 0010917
Dover, Delaware

Date - 6th July, 2026

Assertion of SoftwareOne Management

Assertion of SoftwareOne Management

We, the management of SoftwareOne Cyber Security Practice (the "System"), are responsible for designing, implementing, operating, and maintaining effective controls within the System throughout the period April 1, 2025, to March 31, 2026. These controls provide reasonable assurance that SoftwareOne's service commitments and system requirements relevant to security were achieved.

A description of the boundaries of the System is included in the section titled "SoftwareOne Description of the System" within the accompanying report. This description identifies the aspects of the System covered by this assertion.

SoftwareOne leverages SOC 2 Type 2 compliant AWS and Azure infrastructures for hosting its service environment. The description includes only the controls of SoftwareOne and excludes controls of the subservice organizations. It is important to note that specific Trust Services Criteria may be met only if the subservice organizations' controls, as assumed in the design of SoftwareOne's controls, are suitably designed and operating effectively alongside related controls at our organization. The description does not extend to controls of subservice organizations.

Similarly, certain Trust Services Criteria can be satisfied only with the proper design and operation of complementary user entity controls, which are not within the scope of this assertion.

We performed an evaluation of the effectiveness of the controls within the System throughout the period April 1, 2025, to March 31, 2026, to provide reasonable assurance that SoftwareOne's service commitments and system requirements were met. This evaluation was based on the Trust Services Criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy, as set forth in the AICPA TSP section 100, 2017 Trust Services Criteria.

SoftwareOne's objectives with respect to these criteria are embodied in its service commitments and system requirements, detailed in the accompanying System Description.

We acknowledge that inherent limitations exist in any system of internal control, including the possibility of human error and circumvention of controls, and thus only reasonable, not absolute, assurance can be provided.

Accordingly, we assert that the controls within the System were effective throughout the entire period from April 1, 2025, to March 31, 2026. This assertion assumes that subservice organizations applied the complementary controls assumed in the design of SoftwareOne's controls throughout this period.

Sincerely,

Chief Information Security Officer

SoftwareOne AG
15 Mar 2026

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 Marketplace, 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 Integrity, Accountability, Momentum, Passion, Customer Focus, and Trust.

Code of Conduct

The SoftwareOne Code of Conduct is for employees and Board members as well as for SoftwareOne Partners and suppliers. 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 and has representation from all business functions and serves as the multidisciplinary decision-making body of the Company. The Management team meets on a weekly basis to discuss operational matters for immediate decisions, actions and outcomes, and it meets bi-weekly to discuss strategic aspects of the business. The objective of the Management team is to ensure the business is executing the defined strategy. The Co-CEO is accountable for security at the Executive level.

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.

IT & Solutions Team

IT&S Team is led by the Chief Information Officer (CIO) and responsible for defining the enterprise technology strategy, operating model and governance framework. It is set up as a global business-domain centric function, combining product management aligned to business domains with centralized technology and delivery capabilities responsible for providing core infrastructure, digital workplace, service desk and enterprise platforms.

Sales, Service, Support & Marketing

The sales, services, support and marketing functions are organized into the geographical segments in which they operate headed by a Regional President who reports into the Co-CEO, with the Chief Operating Officer (COO) and Chief Partner and Sales Officer (CPSO) responsible for the Global functions in these departments. These divisions spearhead the marketing, sales and service initiatives and are responsible for positioning SoftwareOne's services in the global market and delivery to our customers.

Finance

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

Legal and Compliance

The Legal and Compliance team is led by the Chief Legal Officer and is responsible for ensuring compliance with applicable laws, regulations and contractual obligations across the organization. Legal responsibilities are executed through defined Global and Regional roles. The Compliance function is led by the Chief Compliance Officer and is responsible for promoting ethical conduct and ensuring the organization adheres to applicable legal, regulatory, contractual and internal policy requirements. People & Culture (Human Resources)

The human resource team is led by the Chief Human Resources Officer (CHRO) and is responsible for the organization's human resources strategy, workforce management and employee-related governance. It oversees key people processes including recruitment, onboarding, learning and development, compensation and benefits, performance management, employee relations and offboarding. It is set up with global and regional leadership, including business partners, to ensure the organization is supported.

Communication and Information

Internal Communication

SoftwareOne maintains communication with personnel using internal collaboration tools, knowledge databases and e-mail. The communication includes but is not limited to communication of SoftwareOne's code of conduct, policies and procedures, corporate events, new initiatives, and awareness and training (including security awareness).

Changes and updates to SoftwareOne policies and procedures, and implementation of changes on SoftwareOne network and security devices are communicated to relevant SoftwareOne personnel through internal collaboration tools.

Policies and procedures specific to SoftwareOne's operations, including those for managing security and confidentiality, are made available to SoftwareOne personnel through the company intranet.

Security Awareness training is provided to personnel at least annually, which provides them with an understanding and awareness of their responsibility and accountability for SoftwareOne's information security and confidentiality matters. Training materials are developed jointly by the Information Security Team, IT Team, and HR Manager, and maintained annually or more frequently as changes occur.

External Communication

SoftwareOne utilizes agreements, its website, collaboration tooling and email to communicate to external customers, vendors, and other parties.

A service description is included on SoftwareOne's website. SoftwareOne's Master Services Agreement (MSA) and addendum (or equivalent customer contract) clearly communicate to customers the functionality of the services provided, and the responsibilities of each party in relation to such services (this includes information on the boundaries that exist between SoftwareOne's provision of the services, and a customer's use of the services). Links on the website include details about the SoftwareOne service, its intended use and privacy policy. SoftwareOne's security webpage describes security measures that SoftwareOne has in place, including network infrastructure and data security, privacy and availability. An impact analysis is performed prior to contracting with any third-party service provider in line with the Service Provider Security Policy.

A non-disclosure agreement is signed by third parties prior to confidential information being shared with those parties. All non-disclosure agreements, and third-party contracts, communicate SoftwareOne's security commitments and required security obligations, terms, conditions, and responsibilities and are signed by authorized approvers and their approval signifies management agreement.

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 disaster recovery capabilities of entire IT infrastructure of SoftwareOne were successfully tested and the report was submitted to management. As per the Management direction, currently the organization is working on a hybrid model, where part of the employees is permitted to work from home on a regular basis.

System Components

Services provided by a Third Party

SoftwareOne's facilities do not self-host any systems that transmit, process, or store Restricted Information. SoftwareOne uses Azure / AWS Web Service cloud platforms for its services. Azure's / AWS's controls are reviewed annually via third party attestation reports to provide SoftwareOne with comfort the control

environment deployed by both Azure / AWS on its behalf aligns with the SoftwareOne Security and Confidentiality governance framework.

Infrastructure

The primary infrastructure used to provide services to customers by SoftwareOne 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	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 Security	Endpoint/E-mail/office/ identity and cloud apps security
	Microsoft Purview	Data classification labelling and Microsoft 365 DLP, Microsoft Purview
	Microsoft Defender	Defender for endpoint, Defender for cloud, Defender for O365

Software

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

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

Primary Software			
Tools	**Tools/Services**	**Operating Systems**	**Remarks**
Proofpoint	Email Security	NA	Vendor hosted SaaS.
Trend Micro CloudONE	Cloud workload security	NA	
KnowB4	Security Awareness Training	NA	

Primary Software			
Tools	**Tools/Services**	**Operating Systems**	**Remarks**
InTune	Workplace Security	NA	
Zscaler	Secure Web gateway	NA	
Microsoft Defender XDR	Endpoint Security	NA	
Abnormal	Email Security	NA	
Cloud Raxak	Security Configuration management	NA	Cloud Raxak cloud
Splunk Cloud SaaS	Security Incident and Event Management	NA	Splunk Cloud
CyberArk	Privileged access management	Window Server	SoftwareOne hosted infrastructure
ServiceNow	Ticketing System	NA	Vendor hosted SaaS.
Microsoft365	Modern workplace productivity tooling (email, word processing etc)	NA	Vendor hosted SaaS.
Atlassian	Confluence	NA	Vendor hosted SaaS
Qualys	Vulnerability Management Scanner	NA	Vendor hosted SaaS

Controls Overview

SoftwareOne has developed formal company-wide policies and procedures for meeting the requirements related to security and confidentiality. These documents are available via the company intranet/SharePoint to all personnel. The Information Security Policies include:

- Access Control
- AI Policy – Internet Usage of AI Tools
- Asset Management
- Backup and Restoration
- Bring Your Own Device (BYOD)
- Business Continuity
- Change Management
- Customer Offboarding
- Cloud Security
- Data Centre Physical Security
- Data Protection and Privacy

- Data Retention and Disposal
- Email Usage
- Human Resource Security
- Information Classification
- Information Security and Privacy Risk Management
- Internet Usage
- Legal and Contractual
- Monitoring
- Network Management
- Offshore Development Centre Security
- Password
- Privacy Organization
- Remote Access Security
- Removable Media Usage
- Security Incident Management
- Security Organization
- Software Usage
- Supplier Information Security
- System Acquisition, Development and Maintenance
- Threat Intelligence

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 Classification and Access Control

SoftwareOne assets and information are documented in the Asset and Risk Register and the asset value classified as Public/ Internal/ Confidential/ Private/ Customer Confidential/ Customer Private, along with the risk probability classified from 1 to 5, 1 being lowest and 5 being the highest. The asset owner is responsible for the classification of the assets and the requisite level of protection. The classification enables personnel to determine what types of information can be disclosed, as well as the sensitivity of the information.

Personnel requesting access to Restricted Information as part of their work is strictly on need-to-know basis / need to have basis, which is approved by the respective managers.

Personnel connecting to the Production Environment Network require two-factor/ multi-factor authentication based on the level of access.

SoftwareOne performs periodic user access reviews to ensure that all access is appropriate and has been approved. If any account is found to be violating SoftwareOne's Information Access Control Policy, the respective accounts are disabled.

Physical Security

Production Environment Physical Access:

All restricted data is stored at a SoftwareOne secured facility, which is hosted within Microsoft Azure / AWS. Controls for ensuring physical and environmental security are implemented and managed by Azure / AWS 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 / AWS 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 multi-factor authentication. All customer accounts and administrative access to the Customer Portal will be revoked following termination of an Addendum / SoW. 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

Password policies are in place across production environments as per the password requirements stipulated in the security policy.

Separate security policies are implemented across company workstations (desktops/laptops) and servers within the SoftwareOne network. Access to environments holding restricted information is controlled via multi-factor authentication.

Unattended workstations are locked using a password protected screen saver after a defined period of inactivity.

Backups

SoftwareOne has a Backup and Restoration policy that governs the performance of data and data restoration. Azure / AWS 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 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. All 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.

Customer Services:

A dedicated Customers 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 Customers 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 / AWS and are therefore out of scope for this report. For the internal end point devices, security patches have been set to auto-update".

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 system acquisition, change and release management policies and processes to communicate management's expectations in regard to performing changes to the production environment. These policies 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.

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:

- Reports from employees and third parties on potential risks identified

- 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 through tooling.
- Alerting services provide real-time information on security trends and threats.
- Operational data and alerts from application and infrastructure log analysis.
- Ongoing monitoring of compliance activities and trends by the CISO and CIO
- Review of user logs of privileged users, showing system login attempts and failures.
- Subscription to relevant newsletters and attendance at relevant forums
- Alerts generated through security tooling and SIEM monitored by the Security Operations Center team

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 ITS team.
- Application security monitoring, including anomalous application behaviour detection and response, is managed by the respective teams.

Controls at Subservice Organizations

SoftwareOne uses Azure / AWS 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 Load Balancing (ELB) and electronic storage (S3).

The controls relevant to SoftwareOne's system include logical and physical access to SoftwareOne's facilities, environmental monitoring, media disposal, and infrastructure availability. SoftwareOne's controls, as described in this report, are designed to operate in conjunction with the complementary subservice organization controls at Azure and AWS.

SoftwareOne has an established monitoring program over controls which have been outsourced to subservice organizations. Assessment of these activities has been performed in relation to Control Objective "CC 4.0 - Common Criteria Related to Monitoring of Controls".

End of Report