softserve

SERVICE ORGANIZATION CONTROLS (SOC) 3 REPORT

MANAGEMENT'S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER THE SOFTSERVE'S ENGINEERING SERVICES BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY, AVAILABILITY AND CONFIDENTIALITY

THROUGHOUT THE PERIOD FEBRUARY 1, 2023 TO APRIL 30, 2023

softserve

Table of Contents

softserve

Section I: Management's Report of its Assertions on the Effectiveness of its Controls over the SoftServe's Engineering Services Based on the Trust Services Criteria for Security, Availability and Confidentiality

September 6, 2023

We, as management of, SoftServe Enterprises Limited are responsible for:

- Identifying the Engineering Services (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system, which are presented in Attachment B
- Identifying, designing, implementing, operating, and monitoring effective controls over the Engineering Services to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

We assert that the controls over the system were effective throughout the period February 1, 2023 to April 30, 2023, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability and confidentiality set forth in the AICPA’s TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Lviv, Ukraine

SoftServe Enterprises Limited

Ray Attard
Director

Oleh Denys
Director

Yaroslav Lyubinets
Director

Adriyan Pavlykevych
Authorized Representative of SoftServe Enterprises Limited
Chief Information Security Officer of SoftServe
Acting as Customer Data Governance Officer of SoftServe

Building a better
working world

Ernst & Young Accountants LLP
Antonio Vivaldistraat 150
1083 HP Amsterdam
Postbus 7883
1008 AB Amsterdam

Tel: +31 88 407 10 00
Fax: +31 88 407 89 70
ey.com

Section II: Assurance Report of the independent Service Auditor

To: Management of SoftServe Enterprises Limited

Scope

We have examined SoftServe Enterprises Limited's (hereafter: SoftServe's) accompanying "Management's Report of its Assertions on the Effectiveness of its Controls over the SoftServe's Engineering Services Based on the Trust Services Criteria for Security, Availability and Confidentiality" (Assertion), that SoftServe's controls over the Engineering Services (System) were effective throughout the period February 1, 2023 to April 30, 2023, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability and confidentiality (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*.

SoftServe uses Equinix, Inc. (hereafter: Equinix) to provide data center services—physical security and environmental security controls in relation to the Engineering services provided by SoftServe. The Description presents SoftServe's system; its controls relevant to the applicable trust services criteria; and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and operating effectively at Equinix. Our procedures did not extend to the services provided by Equinix and we have not evaluated whether the controls management assumes have been implemented at Equinix have been implemented or whether such controls were suitably designed and operating effectively throughout the period February 1, 2023 to April 30, 2023.

Management's Responsibilities

SoftServe's management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of the system
- Identifying, designing, implementing, operating, and monitoring effective controls over the System to mitigate risks that threaten the achievement of the principal service commitments and system requirement.

Ernst & Young Accountants LLP is a limited liability partnership incorporated under the laws of England and Wales and registered with Companies House under number OC335594. The term partner in relation to Ernst & Young Accountants LLP is used to refer to (the representative of) a member of Ernst & Young Accountants LLP. Ernst & Young Accountants LLP has its registered office at 1 Lambeth Palace Road, London SE1 7EU, United Kingdom, its principal place of business at Boompj es 258, 3011 XZ Rotterdam, the Netherlands and is registered with the Chamber of Commerce Rotterdam number 24432944. Our services are subject to general terms and conditions, which contain a limitation of liability clause.

Our Responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our responsibility is to plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects.

We apply the Reglement Kwaliteitsbeheersing NOREA (RKBN, a standard on quality control) that is at least as demanding as the International Standard on Quality Control 1 (ISQC 1), and accordingly maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of SoftServe's relevant security, availability and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) 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.

We are required to be independent of SoftServe and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination was not conducted for the purpose of evaluating SoftServe's cybersecurity risk management program (as it is not in scope of AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*). Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Basis for our opinion

We performed our engagement in accordance with Dutch law and Dutch Guideline 3000A 'Assurance-opdrachten door IT-auditors (attest-opdrachten) (assurance engagements performed by IT-auditors (attestation engagements)) as issued by the professional association for IT-auditors in the Netherlands (NOREA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), 'Assurance Engagements Other than Audits or Reviews of Historical Financial Information', issued by the International Auditing and Assurance Standards Board. This engagement is aimed to obtain reasonable assurance.

We have complied with the NOREA 'Reglement Gedragscode' (Code of Ethics for IT-Auditors, a regulation with respect to integrity, objectivity, professional competence and due care, confidentiality and professional behavior) and with the 'Verordening inzake de onafhankelijkheid van accountants bij assurance-opdrachten' (ViO, Code of Ethics for Professional Accountants, a regulation with respect to independence). The Code of Ethics for IT-Auditors and the NOREA Guidelines related to assurance engagements are at least as demanding as the International Code of Ethics for Professional Accountants (including International Independence Standards) of the International Ethics Standards Board for Accountants (the IESBA Code).

We believe that the assurance evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Inherent limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve SoftServe's principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, SoftServe's controls over the system were effective throughout the period February 1, 2023 to April 30, 2023, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria.

Amsterdam, The Netherlands, September 6, 2023
Ernst & Young Accountants LLP

Dennis
Houtekamer

Digitally signed by Dennis
Houtekamer
DN: cn=Dennis Houtekamer,
c=NL, o=Ernst & Young
Accountants LLP
Date: 2023.09.06 20:36:37 +02'00'

drs. D. Houtekamer RE
Partner

Document reference: RITM5721534

Attachment A: Description of SoftServe’s Engineering Services System

System Overview

Company Background

SoftServe and its affiliates are represented by SOFTSERVE ENTERPRISES LTD, which will be referred to as SoftServe hereafter.

SoftServe is a global digital solutions company. For many years, SoftServe associates have successfully delivered approximately 20,000 customer projects, benefiting thousands of clients across North America, Europe, the Middle East, and Asia-Pacific (APAC). The development centers of SoftServe are in Ukraine, Poland, Bulgaria, Colombia, Mexico, Chile, and Romania, with its headquarters situated in Ukraine (Lviv) and the United States (Austin, TX).

SoftServe’s mission enables talented people to change the world by driving customer success, developing teams and the company, and fostering innovation daily. SoftServe is committed to promoting sustainability and creating a better future for its associates, company, and global communities in which they operate and reside.

Services Provided

SoftServe’s expertise is based on digital technologies and software engineering that enables digital product innovation and digital transformation for our clients. Depending on customer needs, SoftServe either consults to deliver an end-to-end solution or provides SDLC capabilities, covering necessary activities for design, development, and maintenance. In addition, SoftServe provides customized software engineering services to clients across various industries.

SoftServe services include consulting, designing, developing, testing, integrating, deploying, and maintaining software applications that meet customer business requirements. Services are composed of different offer types for customization, depending on the approach with a client. For example, a SoftServe offer may describe work scope that includes Discovery, Implementation, Team Extension, Advisory, Consulting, and Software Development. Offer instances equate to projects in Workday, defining specific activities, deliverables, and outcomes.

SoftServe software engineering services include the following, but are not limited to:

- **Capacity Management.** SoftServe collaborates with its customers by delivering digital engineering capabilities, an extension of in-house teams, or managing capacity with functional skills at any stage of the SDLC. Meanwhile, other project aspects, such as product management, remain with the clients.
- **Custom Product or Solution Delivery.** SoftServe gathers customer requirements and delivers a working quality product. The comprehensive process of product development includes product management, project management, product design, engineering, and maintenance.
- **Professional Services.** SoftServe offers a range of professional services:
    - **Digital Business Consulting.** Provide expertise to identify new or amplify existing business capabilities that can be enabled via digital transformation technologies and software engineering.
    - **Technology Consulting.** Provide technical knowledge and guidance to enable strategies and roadmaps.
    - **Data Strategy.** Outline the overall strategy for client data—from defining business challenges to designing a technical solution. First, we democratize data to ensure quality and availability. Then, we strategically enable applied data to answer pressing business concerns.
    - **Implementation.** Provide technical expertise for configuring, customizing, and contextualizing packaged applications or platforms to meet business requirements.
    - **Integration.** Provide technical expertise for integrating systems, components, modules or applications to function as a holistic cohesive system.

System Boundaries

SoftServe provides comprehensive engineering services, and its system boundaries encompass all relevant components: people, hardware, software (including both internal services and products), data, and procedures. These components will be described later in this document.

Third-Party Access

Logical access to a SoftServe product or service is provided to a third party after signing a third-party agreement. Third party refers to all vendors, contractors, individuals, or organizations with access to the systems and data. Only authorized persons, such as associates, and partners' and customers' representatives, have access to corporate products and services.

Scope of SOC 3 Examination

This SOC 3 report covers customer data governance and protection activities, within provided engineering services and trust services categories for security, availability, and confidentiality. It does not include any systems or services outside of SoftServe's control or managed by the customer. For subservice organizations, the carve-out method is applied (see chapter "Subservice Organizations and Complementary Subservice Organization Controls")). The scope of this report is limited by contractual obligations to the engineering services provided by SoftServe.

- **Development physical offices:**
  - **Ukraine:** Lviv – Office 1, Lviv - Office 2, Lviv - Office 8, Lviv - Office 9, Lviv - Office HQ, Rivne - Office 1, I. Frankivsk – Office 1, Kyiv - Office 3, Kyiv - Office 4, Dnipro - Office 2, Dnipro - Office 3, Chernivtsi - Office 1
  - **Poland:** Wroclaw - Office 2, Gliwice - Office 1, Bialystok - Office 1
  - **Bulgaria:** Sofia - Office 1
- **Development co-working offices:**
  - **Romania:** Bucharest - Office 1
  - **Mexico**: Guadalajara - Office 1
  - **Colombia**: Medellin - Office 1
  - **Chile**: Santiago - Office 1
- **Data centers:**
  - **Third-party owned:** Equinix FR4 Data Center, Equinix DC1 Data Center
  - **SoftServe owned:** Lviv1 Data Center, Lviv2 Data Center, LvivHQ Data Center

Significant changes to the system during the examination period

There were no significant changes to the Engineering Services system during the examination period that require disclosure.

Components of the System

The boundaries of SoftServe are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers.

Infrastructure

The internal network is designed to facilitate the collaboration between project teams and customers through extranets by implementing network segregation. Upon a customer's request, SoftServe creates and configures the Virtual Routing and Forwarding (VRF) network and an isolated environment with secured firewalls. VRF ensures the confidentiality of customer information and prevents traffic leakage. Different project teams can work in a segregated or isolated network. If the project team is in distinct locations, VRF can be distributed between them. The widespread practice is the implementation of a secured Wi-Fi connection in the VRF environment. The VRF network is constantly monitored for suspicious activity by the InfoSec team.

If the network integration uses an encrypted site-to-site Virtual Private Network (VPN), with client, with IPSec tunneling, the PaloAlto tool as an additional level of control and threat containment is applied. For example, network segments that have connections to the customer's network are isolated by using routing (separate L3 VPN within SoftServe's network) and next-generation firewalls by PaloAlto. SoftServe has a presence at major connectivity hubs (Germany and United States), so it can interconnect with customers through dedicated VPN lines.

For increased security, remote access to the project is encrypted and protected via multi-factor authentication (MFA), using a password and digital certificate.

To protect cloud instances, according to best security practices, SoftServe has adopted an integrated Managed Hosting Platform. It includes tools like PaloAlto for compliance monitoring against NIST 800-53 control framework, vulnerability management solution, world leader EDR system, and SIEM/SOAR solution. Security alerts are being monitored by the 24/7 Cyber Security Operations Center (CSOC) Team.

Software (Products)

All applications and systems that are acquired, developed, or customized (hereafter referred to as Products, according to SoftServe Enterprise Taxonomy) for SoftServe corporate use must go through the Enterprise Service Development Lifecycle (ESDLC), whereby the conceptual needs, architectural designs and security and privacy concerns are assessed to make sure those products are designed and deployed in a secure and reliable manner for the business.

The Information Security team (InfoSec) regularly requests SOC reports from third-party suppliers as a part of its supplier management process and evaluates these reports, among other procedures, to address potential risks. Security checks also are executed for both in-house developed and acquired Products to ensure that potential security issues are addressed by the vendor. In addition, privacy and customer data checks are performed to assess the risks related to processing personal identifiable information and customer data.

Where possible, the Products are subject to a continuous vulnerability scanning process that detects and eliminates vulnerabilities. Operations managers coordinate the vulnerability-fixing process to comply with the corporate SLAs.

The company also uses SoftServe-owned and Third-party-owned Products to support the provisioning of engineering services to SoftServe's customers.

People

SoftServe has a staff of more than 12,000 associates. SoftServe's organizational structure is defined by Delivery (Division Presidents Organization), Business Operations, and Corporate Functions, such as Chief Technology Officer (CTO), Chief Information Security Officer (CISO), Chief Marketing Officer (CMO), Human Resources (HR), Administration, Finance, and Legal.

Delivery identifies and develops new strategic opportunities to diversify the customer base and gain market share, produce business with existing customers, and meet customer expectations. Delivery is formed by the divisions aligned to each industry and geographic location of the customer, which receives engineering services. Each division is led by the Division President. Specific verticals or geographical regions are led by the Executive Vice President (EVP), Senior Vice President (SVP), or Vice President (VP) of Client Success.

Business Operations (BizOps) combines customer-focused organizations not directly involved in the delivery. These organizations are responsible for activities like managing sales processes and tools, presales consulting of potential and existing SoftServe customers, and evaluating customer experiences throughout the entire customer journey.

Corporate Functions include the following entities:

- **People Office (Human Resources)** has a mission to create and shape the conditions for inspiring, energizing, and fulfilling associate and leader experiences.
  - **SoftServe University** is part of the People Office, and it offers learning opportunities for a wide range of IT disciplines, leadership, and business competencies.
- **Finance** manages accounts, corporate reporting, and analytics, while also providing financial advisory support.
- **CISO Organization** ensures the value of information through the implementation of information governance and security strategy, maintaining and developing cyber defense capabilities, and providing secure delivery of engineering services.
- **Legal** makes sure the company is compliant with contracts and daily business activities through relevant laws and requirements in every country where SoftServe operates.
- **Administration** manages the office environments.
- **CTO Organization** creates solutions for SoftServe customers. It combines customer-focused organizations not directly involved in the delivery, but engaged in activities that help with the delivery of new projects.

Procedures

Hiring

Talent Success Leads (TSLs) from the GTO department are local resource managers who facilitate the assignment management processes that ensure career growth opportunities for associates and cover the staffing needs of SoftServe's customers. Staffing within the current associates is covered by mobile reserve, apprenticeship program, skilled internship, and rotation. TSL teams operate at each Delivery Center location.

The Recruitment team is an internal team of recruiters who search and attract market talents, conduct candidate screening per company requirements, follow the company's recruitment flow to make sure candidates are the best fit for the company and job, and stay focused on a candidate's experience and vacancy journeys. Recruitment teams operate at each Development Center location.

The background check is conducted in line with the global screening procedure.

Onboarding

Onboarding journey encompasses a newcomer's engagement within the corporate and project environment and is designed to deliver an exceptional experience, provide transparency, and support operational efficiency. The onboarding agenda is equally distributed across the entire onboarding period.

Onboarding at SoftServe is divided into three components:

- **Compliance onboarding** is a set of tasks and activities needed for processing and signing the Hiring documents. The process begins immediately after a candidate has accepted the job offer. As a result, a new associate's account is created, all required documents are uploaded, and the contract is signed.
- **Corporate onboarding** is aimed at forming the feeling of belonging to SoftServe as a Company. Corporate onboarding includes various trainings and quizzes for SoftServe associates.
- **Adaptational onboarding** eases the process of integrating into the company, unit, or team environment, adapting to the organization's culture and adjusting to a particular role. **The aim is to onboard an associate into the company, build engagement and sense of belonging, and provide information about how the associate can grow.**

Associates receive access to their Onboarding Dashboard after signing the offer and then can view the relevant onboarding guidance and checklists. During their onboarding, newcomers also receive tasks and notifications, which require taking obligatory actions on the Onboarding Dashboard. Associates can also view some recommended content.

Certain types of employment exclude some parts of onboarding. For example, contingent workers cover only compliance and functional onboarding.

Performance Management and Professional Development

All SoftServe associates participate in the Professional Development and Performance Management program. As a part of this program, associates establish development objectives and align individual and team goals according to the annual top company goals set by the leadership. Associates and managers meet at least twice a year to review progress and discuss adjustments, as needed.

Associates are eligible to participate in the development and learning programs as a part of the specific segment curriculums (for example, leadership or a new hire) or individual custom programs. SoftServe associates follow the framework set within the Delivery Quality Management System to ensure people, projects, solutions, and customer excellence at all levels.

Delivery Quality Management System

- ### Delivery Excellence

Delivery Excellence (DeEx)—SoftServe's **delivery quality management system**—consists of many components, which address the delivery function success of people, projects, solutions, and leadership. Its goal is to deliver qualitative results, which meet customer requirements and expectations, while driving their needs and enhancing their satisfaction with the quality of services provided. DeEx is SoftServe's means of ensuring delivery quality at scale.

Although DeEx primarily focuses on the quality of the delivery function, security in general, and information security, which is always enhanced, it is an integral part of the delivery function. This will ensure adherence to the customer data protection framework in the future.

- ### People Excellence

People Excellence (PeEx) is a vital component of DeEx to assure success at the project, service, solution, and customer experience levels. Thus, the PeEx ecosystem is designed to reveal talent potential, promote associate experiences, boost professional development, and recognize SoftServe's top talents.

- ### Project Excellence

Project Excellence (PrEx) is a project level of DeEx that facilitates the achievement of project success and ensures meeting customer expectations and compliance with SoftServe's delivery quality standards.

- **Delivery Leadership**

The Delivery Leadership component of DeEx ensures the right associates are in leadership positions, they are onboarded and well trained, continuously develop, improve their skills, and get the necessary tools to fulfill their job and achieve targets as per industry demands and company strategy.

By identifying, defining, and cultivating leadership and job-specific skills, Delivery Leadership streamlines the creation of a strong culture fostering high performance. Delivery Leadership formalizes and continuously improves the complete set of talent management processes as per job family: hiring and staffing, evaluation, onboarding, and development.

Measuring Associate Satisfaction

The level of employee satisfaction (ESAT) within SoftServe is measured by an Employee Net Promoter Score (eNPS) survey through the Peakon platform.

Employee Satisfaction (ESAT eNPS score) reflects how satisfied and content associates are with their professional journey at the company. Feedback and eNPS score give the company management an understanding about how the organization meets associates' expectations.

Employee Satisfaction is a major factor in motivation, goal achievement, and morale in the workplace. Each survey includes a set of questions corresponding to specific drivers of engagement, against which ESAT is measured.

Termination

Every Termination process is conducted according to a procedure aimed at ensuring compliance with SoftServe policies, including information security and confidentiality. The Termination procedure contains the following steps: termination request creation, termination request approval, completion of IT questionnaire, cancellation of future days off, conduction of Exit Interview, and completion of Farewell Survey by the associate.

Customer Feedback and Complaints

To understand the level of customer satisfaction with the services provided by SoftServe, the Customer Experience department has designed and maintained a documented feedback system. During the period a service or product is delivered, the Project Manager gathers customer feedback and complaints.

SoftServe maintains the corporate **Net Promoter Score (NPS) Campaign,** which allows the company to track promoters, passives, and detractors and produce a clear measure of the organization's performance through the customers' eyes.

NPS Campaign

The Net Promoter Score (NPS) survey is a key measure of a customer's overall perception of the brand and an indication of the company's growth potential. NPS measures the loyalty level between SoftServe and its customer. The metric is based on the question "How likely are you to recommend SoftServe to a friend or colleague?" This is measured on a scale from 0 to 10.

Data

Data Protection Methods on the Corporate Level

SoftServe focuses on the security and protection of customer data and its associates' personal data. The company is continuously strengthening security information measures to meet contractual security requirements.

Security drives the organizational structure, training priorities, and hiring processes, which shape corporate data centers and the technologies each uses. It is the focal point of everyday operations and disaster planning, including how threats are addressed. It is prioritized in the way customer data is managed.

To prevent unauthorized access to data or data theft, data encryption methods are used. SoftServe provides encryption of data at rest and data in transit. Corporate portable devices and personal communication devices (with connected corporate mailboxes) are encrypted. To reduce the risk of human error, SoftServe educates and creates new opportunities for associates to keep the information transfer inside and outside SoftServe safe.

To ensure secure data storage and transfer by encryption, the following Sensitive Data Protection Methods are used:

- Azure Rights Management Service (RMS)
- Azure Information Protection
- Sensitivity labels
- Office 365 Message Encryption

Sensitive Data Protection Methods consist of a built-in solution in the Office 365 suite and a custom-developed feature for specific project needs. These methods' primary purpose is to guarantee secure storage, transfer by encryption, and manage the recipient list.

To control how Software as a Service (SaaS) apps are used and how information is shared through them, Microsoft Defender for Cloud Apps is used, formerly known as the Cloud Application Security Broker (CASB) solution. This solution identifies what files and information are stored in Microsoft apps and who has access to them. If there are issues, Microsoft Defender provides tools to remove external sharing permissions and encrypt or delete files. The solution learns the behavior of users and builds a behavioral profile around them. **It alerts if any suspicious behavior is detected, including:**

- Anomalous user behavior if the use of apps deviates from the profiled behavior.
- Data exfiltration when there are indicators that data is being removed using a cloud app.
- Malware, if malicious files are detected in storage applications.

Microsoft Defender works with an identity and access management solution, Azure AD, and alerts to better detect anomalous behavior and block compromised accounts and potentially malicious connections to data. All activities are monitored around the clock by the cybersecurity operations center (CSOC).

Customer Data Governance

Customer data is a subset of data processed and is safeguarded by SoftServe. This data is the subject of protection methods described in the Data Protection Methods of the Corporate Level chapter. Customer data is managed according to the classification described in the Customer Data Catalog–the data classification that prioritizes the handling and protection of customer data based on its sensitivity and regulatory requirements.

The Customer Data Governance organization is responsible for secure and effective customer data governance within SoftServe. It ensures that customer data is collected, stored, and used ethically and securely, complying with relevant laws, regulations, and business commitments managed by Customer Data Governance Stewards team. The responsibilities of Customer Data Stewards include overseeing customer data management, ensuring compliance with data confidentiality regulations, defining data policies and procedures, classifying data based on its level of sensitivity, and monitoring the usage and storage of customer data. They also collaborate with delivery and non-delivery organizations to identify and resolve any issues related to customer data management.

Customer Data Governance framework refers to a structured approach for managing and safeguarding customer data within SoftServe. It includes policies, procedures, and guidelines for collecting, storing, and using customer data. The framework also outlines the roles and responsibilities of various stakeholders involved in managing customer data. Customer Data Governance Stewards work on the CsDG framework implementation, monitor the execution of the framework or its parts, and perform operational activities regarding the CsDG framework implementation in Delivery.

Delivery and project management handle sensitive customer data under the recommendations and rules provided by the Customer Data Governance organization and common rules applicable to sensitive corporate data.

Customer data is primarily collected and managed during the delivery project execution, making the project a key object of investigation when it comes to data archiving and deletion. Therefore, retention and deletion policies for the project closure phase have been realized.

Project managers are responsible for implementing the customer data management process on the project. They are educated through obligatory Data Management Training for Project Managers (PMs) conducted yearly, the Customer Data Governance organization knowledge library, and consulting with the Customer Data Stewards team.

Control Environment

Management Philosophy

SoftServe is conducting its business based on the principles of integrity, diversification, and autonomy of corporate functions.

In all business dealings, SoftServe behaves in a responsible and ethical manner, following applicable laws and regulations. All stakeholders, including customers, employees, and the community, are treated with respect and fairness.

The commitment to a diversification strategy allows reducing risks and efficiently addressing market challenges and customer demands while spreading global delivery expansion. Diversification of the delivery structure allows for better catering for the needs of specific geographical regions or industries.

The autonomy of corporate functions allows us to make quick, efficient decisions. This approach is based on the following principles:

- Global distribution of operations and infrastructure.
- Networked organizational design with an elevated level of independent management.
- Associates' mobility—both physical and job mobility.

Commitment to the above-mentioned principles in combination with the diverse backgrounds and areas of expertise of the company management makes it possible to deliver impressive results for our clients consistently.

Security Management

The SoftServe Board of Directors (BoD) has established an Operating Committee (OpCom) as the ultimate operational management body of the company. OpCom is responsible for making decisions regarding significant changes in the organizational environment, business circumstances, legal conditions, or technical environment that are likely to have an impact on information security. If those changes can have a major impact on the company operations, they are reviewed by the Legal and Risk Committee of the Board and presented to the full Board for final approval.

The SoftServe CISO Organization is accountable for the information security at SoftServe. The Chief Information Security Officer, who reports to the CEO and is a member of OpCom is appointed responsible for the management and control of information security risks.

Division Presidents who are accountable for managing customer-related risks within the dedicated division are members of the extended Operational Committee. OpCom gives an overall strategic direction by approving and mandating information security principles and delegating responsibilities for physical and information security to the CISO.

All SoftServe information security measures are described in the Integrated Management System and are annually updated and reviewed by both internal and external certification auditors, independent third-party party assessors (e.g., penetration testing), and customer security assessors. The Internal Audit team reviews SoftServe's compliance with the best security practices and provides assessments according to the designed audit program, checks controls, processes, and systems, then defines areas for improvement. Certification auditors provide independent validation of compliance with the leading international standards.

Annual Independent Penetration Testing is conducted by an independent security service provider to identify and mitigate security vulnerabilities.

SoftServe obtained a certification of its Information Security Management System (ISMS) to the ISO/IEC 27001:2013 standard, and the ISMS is a subject of continuous improvement.

To help ensure compliance with applicable privacy requirements, SoftServe obtained the ISO/IEC 27701:2019 certification. This international certification sets requirements and specifies guidance on the building, usage, and improvement of information privacy management.

Other SoftServe certifications related to the Information Technology Service Management System are ISO/IEC 20000:2018, a service management system (SMS) standard, and ISO/IEC 13485:2016, which specifies requirements for a quality management system. They both promote the adoption of an integrated approach to delivering managed IT services. This standard is aligned and fully compatible with the Information Technology Infrastructure Library (ITIL) framework. SoftServe follows the best practices of ITIL for organizing IT service management. A set of practices like Change Management, Incident Management, Vulnerability Management, and Patch Management help the company maximize business value by using information technology, increasing customer satisfaction, avoiding major incidents, and keeping risks in check.

Corporate Security Governance

To ensure effective security governance throughout the organization, SoftServe has developed an Integrated Management System (IMS). It combines the ISMS, SMS, and Privacy Information Management System (PIMS), compliant with world-class certifications (ISO/IEC 27001:2013, ISO/IEC 27701:2019, ISO/IEC 20000:2018, and ISO/IEC 13485:2016), corporate policies and standards that are regularly reviewed and updated.

SoftServe maintains the Integrated Management System to ensure policies and procedures are:

- Communicated throughout the organization.
- Reviewed and approved by an appropriate Accountable Manager.
- Managed on a version-controlled basis.
- Adhered to business objectives and regulatory obligations.
- Focused on continual iteration and improvement.

Corporate governance documentation is reviewed at planned intervals, or if significant changes occur, to ensure its continuing suitability, adequacy, and effectiveness. The review includes the assessment of the opportunities for improving documentation and approach to managing information security in response to changes in the organizational environment, business circumstances, legal conditions, or technical environment.

Security governance documents that state rules and requirements for associates are incorporated into the Information Security Awareness Training described later in this document (chapter ”Operational Security”). SoftServe associates learn about the basic security rules during their onboarding and then annually acknowledge it by taking the Information Security Awareness Quiz or Training.

Operational Security

General Concepts

The protection of company assets and provisioning of reliable services and products with expected value are vital to the success of SoftServe's business. SoftServe has established the Information Security Management System (ISMS) through protection for privacy of personally identifiable information (PII) principles. The ISMS operates all the processes required to identify the information needed to protect and how it must be protected, including information privacy and the Service Management System (SMS), to provide the services and products expected by the customers.

Due to merging ISMS, SMS, and PIMS, SoftServe has established the Integrated Management System, which provides and ensures the convenient and integrated management of interdependent processes.

Because the needs of SoftServe's business change, SoftServe recognizes the management system must be continually changed and improved to meet these needs. To this effect, SoftServe is continuously setting new objectives and regularly reviewing the IT and IT Security processes.

SoftServe is committed to protecting its customer data, intellectual property, and personal information of SoftServe associates and contingent workers and providing IT services and products to them at an agreed level, aligning them with the company's strategy and continuous improvement.

Cybersecurity

To monitor security events and proactively prevent any cybersecurity incidents, SoftServe operates a mature Cyber Security Operations Center (CSOC). The CSOC provides continuous 24/7 monitoring of suspicious activity alerts, detailed threat hunting, and analysis. Additionally, there is a capability to perform corrective actions on network segments, user accounts, registry entries, folders, files, processes, and services. Events from all security controls, including Next-Generation Firewalls (NG FW), Intrusion Prevention System (IPS), DNS protection, CASB, and next-generation anti-malware ecosystem are forwarded to the SIEM/Security Orchestration, Automation, and Response (SOAR) for future correlation and security monitoring.

The Security Logging and Monitoring method is used to detect threats and inconsistencies and check if effective security practices and controls are in place.

Security Corporate Infrastructure

SoftServe's IMS aims to balance risks against the cost of implementing controls. A periodic review of the risks and security controls is done to address changing business requirements and priorities. All security policies are annually assessed and reviewed. Evaluation of the risks and controls is accomplished in line with the Risk Management Framework.

SoftServe built a layered approach to security with appropriate controls to prevent, detect, and mitigate potential threats.

The **"security first"** and **"zero trust"** approach always differentiates SoftServe from its competitors. Thus, our Infrastructure and Operations team, collaborating with the SoftServe InfoSec team, implemented the unique solution to guarantee a Secured Work From Home (SWFH) environment.

Information Security Awareness and Training

SoftServe creates an inclusive and highly professional security culture within its entire company. It implements security awareness rules and practices through training, quizzes, and posts on Workplace.

All SoftServe associates must take mandatory Information Security Awareness Quiz or Training. The training is assigned to newcomers during their first week of onboarding and then the knowledge is proved by annually passing the Information Security Awareness Quiz or Training. Newcomers have 5 days to complete the training and associates have 90 days to prove their knowledge by passing the quiz or training again. The training and quiz are managed and tracked by the corporate learning platform to ensure its completion.

The training content is continuously updated and improved with the use cases that result from incidents or yearly risk assessments. Training sessions include the principal security requirements and guidelines that help prevent security events and incidents caused by associates (for example, phishing or social engineering). The Information Security Awareness Quiz consists of questions regarding mandatory security topics, which ensure a proper awareness level. Therefore, if the quiz is passed by existing associates they do not need to complete the full training again.

To ensure training sessions are effective and associates can recognize phishing attacks and promptly respond, SoftServe regularly launches a phishing simulation campaign. Depending on the project, specific, deeper internal security training may be assigned. For instance, on any of the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), or Open Worldwide Application Security Project (OWASP) top 10 training.

The company cares about the growing number of professionals in a particular field and continuously raises security and data privacy awareness for the teams responsible for corporate information security. To always stay on top of current trends and developments, the Security and IT teams regularly attend international conferences and obtain certifications in professional security.

Physical Security and Environmental Controls

SoftServe protects all areas like telecommunications, cabling, and off-site containing Information Processing Systems, or media that include customer information. Access to premises is controlled by a defined security perimeter, appropriate security barriers, and security guards who go through background checks, training, and authentication control.

An intrusion alarm system is used as an additional control tool to protect restricted areas, according to the risk assessment analysis.

Access to offices is controlled using Radio Frequency Identification (RFID) cards, which each associate receives during the employment process. Every visitor must be accompanied by an associate.

A video surveillance system monitors vulnerable areas and rooms with unique requirements for physical security controls. Access logs and camera footage are preserved and available as proof of an event in case of any incident.

SoftServe offices have a backup power supply through either redundant power grid connections, priority power supply lines, or diesel generators. Data centers are equipped with water leak detectors, and there are Uninterruptible Power Supply (UPS) devices connected to the monitoring systems. The offices are equipped with smoke detectors, fire detection alarms, and fire extinguishers. Checks and maintenance of diesel generators, UPS devices, water leak detection, and fire protection equipment are regularly done.

Some premises are owned by SoftServe, and others are rented. Based on conditions specified in the contracts with the landlords, landlords are responsible for fire alarm systems, smoke protection, and air conditioning in the rented offices.

Vulnerability Management

Vulnerabilities in corporate services and products are tracked via the Vulnerability Management System. Existing internal and external vulnerabilities are reviewed and resolved, according to the Vulnerability Management Policy, within defined periods. The vulnerability process automation notifies the appropriate Service/Product Owners, responsible DevOps, and IT Operations Coordinators about open security vulnerabilities and vulnerabilities with approaching due dates. Vulnerabilities not remediated by the due date are reported to IT Management by IT Operations Coordinators. Regular reviews of all identified vulnerabilities are conducted daily during morning meetings with both the Information Security and IT teams.

Change Management

SoftServe's leadership and Board of Directors (BoD) authorize enterprise-level changes, guided by the Strategy Office. These changes are then translated into Top Company Goals (TCGs) and Key Performance Indicators (KPIs) to ensure effective implementation.

Change Management within IT Services is a crucial component for ensuring successful service delivery and maintaining accurate tracking. This process maximizes service availability and prevents disruptions to SoftServe's business processes caused by undesirable changes to technology systems and components.

The Change Management process achieves enhanced performance, promoting business continuity, optimizing risk management, increasing accountability, and improving the reliability of technology services.

System Monitoring and Protection

System Monitoring

SoftServe distinguishes between Operational IT monitoring and Security monitoring. Operational IT monitoring is focused on availability, while Security monitoring is focused on confidentiality and integrity.

Security Logging and Monitoring is a method used to detect threats and inconsistencies. It also helps check whether effective security practices and controls are in place. The SIEM provides real-time security monitoring (confidentiality and integrity) and then sends notifications of any detected suspicious activity or vulnerability exploitation attempts.

In terms of availability, the IT department uses appropriate tools to ensure all corporate services are up and running within the agreed-upon SLAs. A cross-functional IT Operations Team reacts to the availability incidents around the clock.

System Protection

SoftServe has strategically adopted a defense-in-depth approach to system protection. It means the implementation of control measures at each endpoint, such as DNS level protection, Next-Generation Endpoint Detection and Response (NG EDR), host firewall management, group policies, and full drive encryption.

DNS protection provides the first line of defense against internet threats and uncovers and blocks a broad spectrum of malicious domains, IPs, URLs, and files used during attacks. It blocks requests to malicious and unwanted destinations, even before the connection is established.

To prevent more advanced security threats, the company uses the world-class NG EDR system, which leverages execution profiling and predictive security analytics, instead of focusing on malware signatures, indicators of compromise, exploits, and vulnerabilities. For advanced anti-malware capabilities, the company uses sandboxing for in-depth behavior investigation and detection of hidden, evasive threats. With host-based firewalls, SoftServe manages firewall protection on all endpoint devices. In case of theft, full drive encryption helps prevent data leakage.

Problem Management

The goal of Problem Management is to reduce the number and frequency of incidents and improve the level of service to users. To achieve this, SoftServe investigates the causes of incidents and resolves them through managed actions. Another goal is to reduce the overhead costs of supporting services and products and maximize the warranty.

Problem Management follows a clear, well-designed process that, together with targeted tools, helps increase service availability and improves user satisfaction.

Access Management

SoftServe has established strong governance and technical measures for company products through appropriate account management. The Account Management Policy implements the requirements for the role-based security approach to limit and control access. Administrative access to all corporate products is restricted to only authorized associates.

Each person who accesses SoftServe information products is uniquely identified by their account in the system. The domain username cannot be changed.

Privileged accounts are tracked in the Configuration Management Database with a clear record of the associate acting as an account owner.

The use of Privileged accounts is logged and monitored in compliance with SoftServe's Security Monitoring and Logging Policy.

The access granting process is defined and documented in the corporate Access Management Procedure and implemented at the corporate level.

Access management rules are regularly reviewed per Product in accordance with the Access Review process.

Business Continuity and Operational Resilience

Business Continuity

SoftServe's Continuity and Operational Resilience strategy focuses on ensuring that the company proactively plans to support business continuity and remains resilient to disruptive events. The corporate approach to business continuity and resilience ensures continuous readiness by regularly exercising and testing. This allows management to focus business continuity planning around the most important aspect—ensuring continuity of services to customers in case of a disaster.

The Emergency Response Team (ERT) was established to manage crisis situations throughout SoftServe and provide support to its associates and business. The ERT is a dedicated, cross-functional team consisting of stakeholders and executives of various areas within the organization. The team is accountable for immediately reacting to unpredictable crisis situations, monitoring global or local impending crises, and providing real-time updates and warning notifications.

Company IT and security infrastructure are cloud-centric, with 95% of business applications being SaaS (cloud native), while the remaining services are delivered from distributed data centers in CEE, EU, and the USA.

Data center sites integrate private connectivity to customers' environments in a fully redundant mode. They are a crucial element of the IT Disaster Recovery plans as backup and restore facilities for private computing, data, and toolsets for IT and SecOps. There is also an off-site and offline backup strategy implemented to protect SoftServe data and systems against cyber-attacks and physical disasters.

Infrastructure Resilience

SoftServe's infrastructure across all development centers has multiple levels of redundancy. The company is independent of local internet providers and telecommunication operators.

SoftServe leases dedicated optical communications channels through diverse geographical paths between data centers in the EU and Ukraine. Additionally, at least one office building in each city is equipped with an independent satellite communication link to the internet, offering emergency communication capabilities.

SoftServe's vital records are periodically backed up and stored at an off-site location, as a part of normal operations.

An IT Disaster Recovery Plan (DRP) has been developed for IT services, with a defined criticality level for restoration after a disaster. Our ongoing BCP/DRP procedures, related to the testing of our IT systems, is an operational process activity. SoftServe decided to shift from one-time annual activity to a more agile process. Throughout the year, we perform tests called IT major incident simulations. These simulations are made based on the applicable threats observed. During these tests, we simulate events of total unavailability of our main production sites or significant systems unavailability hosted there.

Before the war, SoftServe took preventive measures to secure its infrastructure and backup hosted services. Our dedicated Site Recovery Team (SRT) are continuously improving our infrastructure, procedures, and processes to meet and exceed IT Disaster Recovery Plan baselines. Our SRT team in the EU work on a 24/7 rotation to establish smooth operations and recovery of our services independently of the events in Ukraine. Considering the current development of the situation in Ukraine, all operations from Ukraine are being switched to EU, with the option to entirely shut down our operations in Ukraine in case of further escalation.

Incidents Management

Operational Incident Management

SoftServe has established an Incident Management process to quickly restore normal service operations and minimize the adverse impact on business operations. The company follows a multi-layered service support model.

All incidents are registered in the IT Service Management System. An incident ticket is created via the HelpDesk Portal or other tools. Incidents also are automatically generated via monitoring systems or email. Then, the incident is categorized, prioritized, and routed by the HelpDesk team or automatically by the system. Routing depends on the classification of the incident. Service availability incidents are routed to IT Operations, while security and confidentiality incidents are routed to the CSOC team.

Security Incident Management

Security Incident Management resolves information security incidents that may affect the confidentiality, integrity, or availability (CIA) of SoftServe associate data or customer data. SoftServe associates are aware of the Information security incident reporting procedure. If a security incident occurs, the CSOC team prioritizes it according to its impact on the data, service, or business. The incidents that directly impact customer data are assigned the highest priority.

SoftServe’s Security Incident Management process is structured around best practices like ITIL for handling incidents. When investigating information security events, the team performs an analysis of precursors and indicators, looking for correlating information. To prevent similar future incidents, CSOC performs a root cause analysis and regular risk assessments based on security incident reports and analytics. Periodically, monitoring controls are performed and communicated quarterly to top management.

Customer Security Requirements Compliance

To ensure the fulfillment of commitments and expectations stated by SoftServe customers, contract agreements are analyzed by the Legal team. A Legal professional reviews each contract thoroughly to understand the terms and conditions and highlights risks or requirements, which shall be additionally verified, ensuring all terms are fair, enforceable, and straightforward. The Legal team also engages experts from other functions, such as Finance, CSL/Delivery Managers, InfoSec, GRC, and Privacy, to align responsibilities and expectations from all perspectives.

Security, availability, and confidentiality requirements from SoftServe Customers stated in the contract agreements are registered by the GRC team and reviewed for compliance with appropriate Project Managers/Delivery Managers. Those requirements are also integrated with PrEx, with visibility for each respective Project Manager.

Supplier Due Diligence

The company enforces strict controls during supplier onboarding based on eligibility criteria and a Code of Conduct. Risk assessments start from the supplier onboarding process and involve subject matter experts in areas like Information Security, Personally Identifiable Information (PII), Finance, Legal, and other risks. Responsibilities, terms, security, availability, confidentiality, environmental, and other aspects, depending on the contract, in line with obligations, are addressed in the commitment formalization by sole contract or independently. These measures ensure supplier compliance with the requirements to meet their obligations and minimize the risk of non-performance, business disruption, and reputational harm.

Risk Assessment

SoftServe's risk management objective is to systematically identify, assess, and mitigate risks that may impact the company's operations and strategic objectives, with a focus on prompt reporting of high-impact risks to Executive Management for review and approval of proposed mitigation strategies.

SoftServe operations and management rely heavily on decentralized decision-making for scalability and agility purposes. To support a decentralized decision-making process, risk management must be done with a similar organizational approach.

SoftServe manages risks in accordance with the Enterprise Risk Management Policy. Risk assessment and reporting are performed annually. Risk assessment requires evaluation of the likelihood and the potential impact on the company's strategic, operational, and financial objectives. The risk mitigation strategy is planned by the Risk Owner based on the levels of identified risks. The proposed mitigation strategy may require the implementation of new or changes to the existing risk-reducing controls.

Information Security Risk Management is conducted in accordance with the Enterprise Risk Management Framework aligned with the ISO 27001 requirements and based on the NIST best practices. The Information Security Risk Assessment is annually reviewed, and mitigation reports are agreed upon and approved by C-level management.

Project-level risks are evaluated within each project by a Project Manager, primarily focusing on risks that impact project objectives, scope, schedule, cost, and quality. Mitigation options are planned and implemented, considering project specifics. Evaluation and mitigation results are reported to the upper management.

Information and Communication

Internal Communication

SoftServe communicates security, availability, and confidentiality criteria to internal users through the onboarding process, policies, and procedures stored on Confluence.

Internal communication covers policies, guidelines, privacy, security, and new services. Changes to policies are communicated via the Integrated Management System space on Confluence and the corporate website, when applicable. Important and immediate changes like Password Policy are communicated to associates by email and Workplace.

External Communication

SoftServe's communication with external audiences includes owned digital media and PR communications.

Owned digital media is comprised of social media platforms, whereby the company provides information about vacancies, events, courses, and other activities. These are:

- **SoftServe's social media:**
    - LinkedIn, Facebook, and Instagram accounts
    - "SoftServe Education" channel on Telegram
    - TikTok official account
    - Business account on X - Twitter
    - Two channels on YouTube: Business channel and Career channel
- **SoftServe's blogs:** Business blog and Career blog
- SoftServe's website
- **SoftServe's podcasts:**
    - SoundCloud
    - Google Podcasts ("PRODcast," "Це солюшн" (ENG: "It's a Solution"), "People, Tech and other Weirdness" ENG | UA)
    - iTunes ("PRODcast," "Це солюшн" (ENG: "It's a Solution"), "People, Tech and other Weirdness")
    - Spotify ("PRODcast," "Це солюшн" (ENG: "It's a Solution"), "People, Tech and other Weirdness")

- **Paid media ads.** This refers to targeted digital advertising aimed at brand awareness, website traffic, content engagement, lead generation, and video views run on different campaign platforms.

PR communications focus on:

- **Public relations.** Delivers important SoftServe news and announcements to a broad business audience. The primary means of communication are press releases distributed via the Business Wire service across the USA, EMEA, and APAC tech media outlets and to repost them on relevant websites.
- **Analyst relations.** Refers to targeted communication with analyst firms to build and deepen business relationships with industry analysts. The primary means of communication include one-to-one briefings, group briefings, analyst inquiries, events, and other relevant activities involving analyst firms.

Monitoring

Project Checks and Audits

Each project in the scope of Delivery Excellence is subject to regular checks or audits, which may vary depending on the level of complexity and efforts required for their execution. These checks and audits are performed using the Project Excellence Platform and Delivery Data Analytics. These tools help analyze portfolio coverage with checks and audits and provide access to respective stakeholders for outcomes at each level of the project portfolio.

Project checks and audits are conducted by the Project Leadership team, with or without external experts or auditors. **The project processes and practices are analyzed to:**

- Ensure compliance with SoftServe execution standards
- Identify risks caused by non-compliance with SoftServe execution standards
- Recommend and link to SoftServe best practices for dealing with identified risks

Moreover, project audits evaluate the performance against the customer’s success criteria and project goals, ensuring the project is on the right track.

Checks provide health monitoring for project services or functional practices. There are two types of checks: a self-check and a health check. **Self-check** is self-service. **Health check** is a service with an external expert.

A Project Management function audit (PM function audit) provides an expert judgment of an as-is project state, evaluates the quality of project processes, along with the quality of their outcomes, and assesses the project performance against project goals and targets. Audits are carried out as a full-cycle project audit or peer-to-peer review sessions for each project function.

All active projects must regularly undergo a self-check and either a health check or a PM function audit.

External and Internal Audits

External Certification Audits, which follow the ISO 27001, ISO 27701, ISO 20000, and ISO 13485 standards, are conducted annually to ensure the compliance of SoftServe IT, security, and privacy processes with the existing best practices.

Internal Audits ensure controls are properly designed and operationally effective, while providing SoftServe regular and more precise internal audits based on the ISO (International Organization for Standardization) and IPPF (International Professional Practices Framework) standards within the COSO framework. Findings are reported to control owners. Critical findings are reported to the Board of Directors.

Control owners analyze and address the findings. Operational management reports the significant findings via management reviews to Operational Committee and Quarterly Business Reviews, and appropriate improvements are discussed and then implemented.

User Entity Responsibilities

SoftServe services are designed with the assumption that SoftServe customers (user entities) are also responsible to achieve SoftServe's service commitments and system requirements.

User entities and their auditors must exercise judgment in selecting and reviewing these **responsibilities, which are as follows:**

- Developing their own disaster recovery and business continuity plans that address their ability to access or use SoftServe services.
- Ensuring user IDs and passwords for access to SoftServe applications are secure and only used by authorized associates.
- Using MFA as security enforcement control.
- Notifying SoftServe in a timely manner of changes made to technical or administrative contact information.

- Understanding and defining data storage requirements and informing SoftServe about the data classification.
- Understanding and implementing encryption protocols to protect data during the transfer to SoftServe.
- Immediately notifying SoftServe of any actual or suspected information security breaches, including compromised user accounts and passwords.
- Notifying SoftServe of any regulatory issues that may affect the services provided by SoftServe.

If the client does not adhere to the proposed flows, it will be difficult for the company to ensure the safety of customer data and compliance with contracting criteria.

Subservice Organizations and Complementary Subservice Organization Controls

Subservice Organization

SoftServe uses a set of collocation services provided by Equinix, Inc. (hereafter, Equinix), a subservice organization for providing SoftServe's engineering services. Equinix provides data center services—physical security and environmental security controls—in relation to the engineering services provided by SoftServe. Equinix is identified as a subservice organization, whereby controls at Equinix in combination with SoftServe's controls are needed to provide reasonable assurance that SoftServe's service commitments and system requirements are achieved based on applicable trust services criteria. The services provided by Equinix are excluded from this report via the carve-out method.

Complementary Subservice Organization Controls

In designing its system, SoftServe has decided certain controls must be implemented by the subservice organizations like Equinix to meet certain criteria applicable to security, availability, and confidentiality.

This section describes additional controls that must be in operation at the subservice organization to complement the controls at SoftServe. The following identified controls cannot be regarded as a comprehensive list of all controls deployed by the subservice organization. There may be additional, appropriate controls not shown in this report for subservice organizations.

Subservice Organization	Responsibility	TSC
Equinix	Ensure appropriate physical security over servers, where SoftServe data is hosted.	CC6.4 CC6.5
Equinix	Ensure that physical access to servers, where SoftServe data is hosted, is approved, and granted as requested and removed in a timely manner upon the termination or change in job responsibilities.	CC6.4 CC6.5
Equinix	Ensure that each of its customers has a defined space and is physically secured.	CC6.4 CC6.5
Equinix	Ensure appropriate environmental controls, such as fire extinguishers, smoke detectors, UPSes, and other items, exist for servers, where SoftServe data is hosted.	A1.1 A1.2
Equinix	Periodically perform BCP and Disaster Recovery tests.	A1.2 A1.3

Impact of the War in Ukraine on SoftServe's Control Environment

Assessment Overview

Since the annexation of Crimea by Russia in 2014, the company started re-evaluating the risks arising from the military actions on the territory of Ukraine such as the risks related to the safety of our associates, physical security of our premises, and power outages throughout Ukraine. The major escalation of military actions in Ukrainian regions started on February 24, 2022, which caused the activation of the Business Continuity Plan. Since October 2022, the power grids and related infrastructure were attacked that affected the energy distribution across Ukraine and required us to constantly monitor and review the existing controls. SoftServe performed an internal assessment to determine and evaluate the impact of the war on the control environment that might have affected SoftServe’s service commitments.

During the assessment, all 85 controls have been evaluated to determine the war impact on the control environment during the period from April 1, 2022 to April 30, 2023. As a result, the following was analyzed:

- The war impact on the processes and control activities that are within the control owners’ areas of responsibility.
- The changes that the controls have undergone in case of the war impact.
- The additional measures that have been taken to strengthen the control environment in case of the war impact.

Based on the results of the assessment, it was concluded that the majority of controls have not been impacted by the war. All 85 controls are operating as designed and implemented. Among them, the controls within the Business Continuity Plan, Physical Security, Office Support, IT Infrastructure and Operation, IT Asset Management, and Finance areas were strengthened and improved in order to mitigate the risks arising from the war. Some control activities within the Human Resources and Governance Risk and Compliance areas were temporarily postponed due to the war, however, it didn't affect the control environment and fulfillment of service commitments. Finally, no major incidents caused by the war were identified during the period from April 1, 2022 to April 30, 2023. Thus, the war did not have an adverse effect on SoftServe’s control environment and service commitments defined for the assessed period.

Attachment B: Service commitments and system requirements

SoftServe's system of internal control is evaluated using the trust services criteria within the context of the entity's ability to achieve its business objectives and sub-objectives. SoftServe provides services to user entities, its objectives and sub-objectives relate primarily to the following:

- The achievement of the service commitments made to user entities related to the system used to provide the services and the system requirements necessary to achieve those commitments
- Compliance with laws and regulations regarding the provision of the services by the system
- The achievement of the other objectives the service organization has for the system

Service commitments

SoftServe provides a range of engineering services to its customers. According to contractual obligations, customers may provide SoftServe with access to their data at the scale sufficient and necessary to perform the agreed services. Therefore, customer data can be stored and processed on internal assets and accessed by SoftServe Delivery units, IT personnel, the Global Delivery Leadership (GDL) team, and SoftServe contractors in compliance with the terms of legal agreements between SoftServe and its customers.

SoftServe is committed to ensuring customer data governance and protection in the scope of provided services based on the following Trust Service Categories:

- **Security**. Customer data is secured in compliance with relevant laws and regulations. These commitments include data encryption, authentication mechanisms, physical security, and other relevant security controls.
- **Availability**. Availability of engineering services is ensured by disaster recovery procedures, continuous backup mechanisms, and business continuity processes.
- **Confidentiality**. Confidentiality of customers' data is maintained through data classification policies, data encryption, and other relevant security controls.

SoftServe is responsible for delivering its service commitments and for designing, implementing, and operating effective controls within the system to ensure these commitments are achieved.

Service commitments related to data protection are documented and communicated in the legal agreements. Data originated by SoftServe associates and direct contractors to fulfill contract obligations is subject to the same controls as customer-originated data.

System requirements

Operational requirements are established to support the achievement of service commitments, relevant laws, and regulations. These requirements are outlined in SoftServe’s policies, procedures, documentation, and legal agreements with its customers. Corporate information security policies describe how systems and data are protected. These policies include rules about how engineering services are provided; products and services are designed, developed, and operated; networks are managed; and associates are hired, trained, and evaluated.

SoftServe also maintains standard procedures about how to perform specific manual and automated processes required during the operation and development of engineering services.