Safe Securities Inc.

System and Organization Controls 3 (SOC 3)

Report on Safe Securities Inc. System Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy

Throughout the period January 01, 2025 to November 30, 2025

[Performed under TSP Section 100—2017 Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy]

Table of Contents

I. Independent Service Auditor's Report

Tel: +91 22 6277 1600
Fax: +91 22 6277 1600
www.bdo.in

The Ruby, Level 9, North West Wing,
Senapati Bapat Marg, Dadar (W),
Mumbai, 400028

Independent Service Auditor's Report

To the Management of
Safe Securities Inc.

Scope

We have examined the management's assertion, contained within the accompanying "Management's Report of its Assertions on the Effectiveness of its Controls over Product "SAFE" (Assertion), that Safe Securities Inc.'s (Safe Security) System controls were effective throughout the period January 01, 2025 to November 30, 2025 to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (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. Our examination was limited to the product 'SAFE' and was not conducted for the purpose of evaluating Safe Security cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

Management's Responsibilities

- Safe Security management is responsible for its assertion, selecting the trust services categories and associated criteria on which its assertions is based, and having a reasonable basis for its assertion. It is also responsible for:
- Identifying the Safe Security system and describing the boundaries of the system.
- Identifying its principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of the system.
- Identifying, designing, implementing, operating, and monitoring effective controls over the Safe Security system to mitigate risks that threaten the achievement of the principal service commitments and system requirements.

Our 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. 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 managements assertion, which includes (1) obtaining an understanding of Safe Security relevant Security, Availability, Processing Integrity, Confidentiality, and Privacy 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

Tel: +91 22 6277 1600
Fax: +91 22 6277 1600
www.bdo.in

The Ruby, Level 9, North West Wing,
Senapati Bapat Marg, Dadar (W),
Mumbai, 400028

provide a reasonable basis for our opinion.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability, processing integrity, confidentiality and privacy are achieved.

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. Furthermore, projections of any evaluation of effectiveness to future periods are 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.

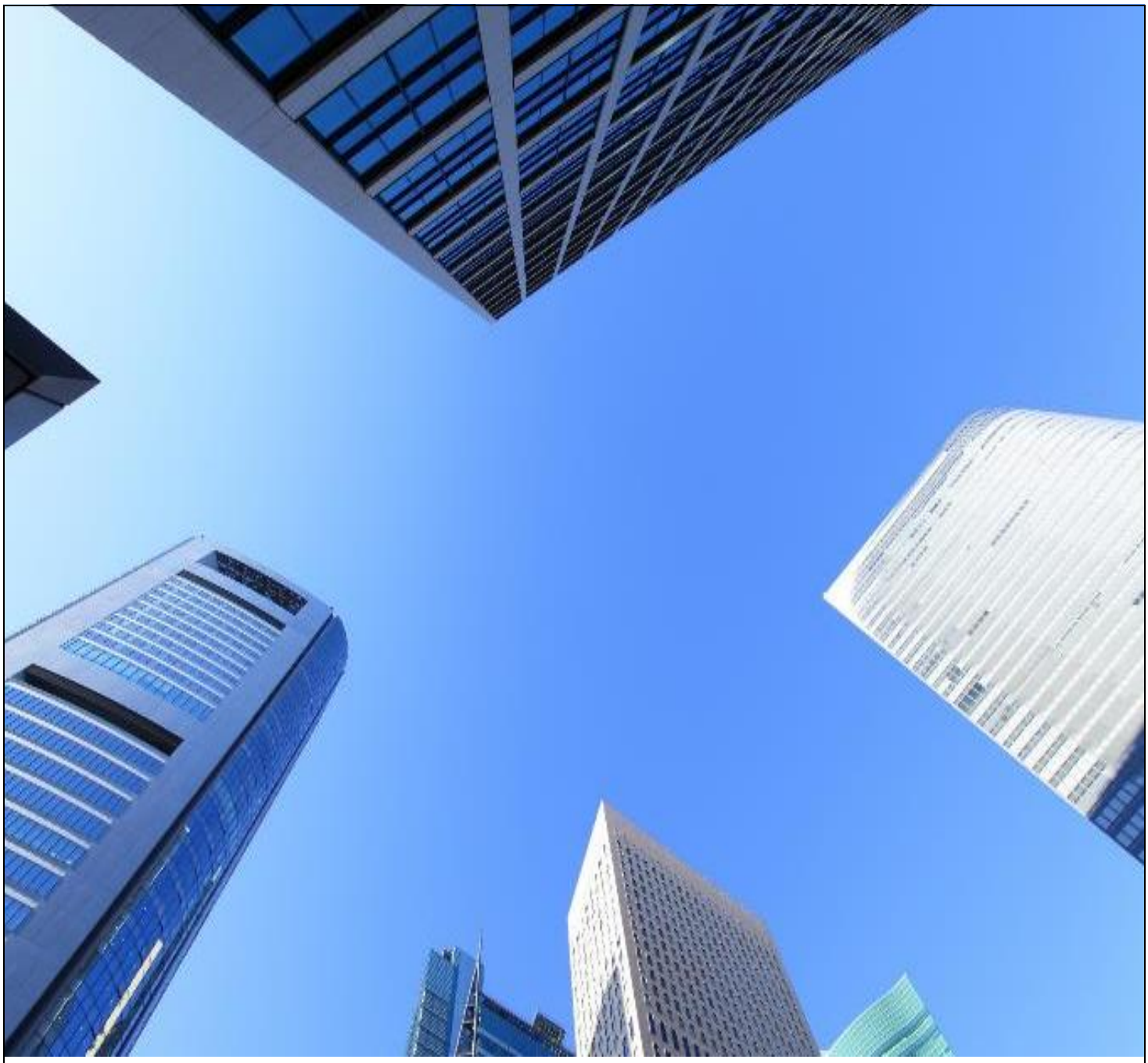
Opinion

In our opinion, Safe Securities Inc.'s controls over the systems relating to the product 'SAFE' were effective throughout the period January 01, 2025 to November 30, 2025, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the aforementioned criteria for Security, Availability, Confidentiality, Processing Integrity and Privacy.

BDO India

BDO India LLP

Date: 13 March 2026



II. Management's Report of its Assertion on the Effectiveness of its Controls over Product 'SAFE'

SAFE

contact@safe.security
www.safe.security

Management's Report of its Assertions on the Effectiveness of its Controls over Product 'SAFE'

Based on the Trust Service Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

13/03/2026

We, as management of Safe Securities Inc. (Safe Security) are responsible for designing, implementing, and maintaining effective controls over Safe Securities Inc.' systems providing SAFE ('System') to provide reasonable assurance that commitments and system requirements related to the operation of the systems are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in security controls, an entity may achieve reasonable, but not absolute assurance that security events are prevented and, for those that are not prevented, detected on a timely basis. Furthermore, projections of any evaluation of effectiveness to future periods are 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.

We have performed an evaluation of the effectiveness of the controls over the system throughout the period January 01, 2025 to November 30, 2025 to achieve the commitments and System requirements related to the operation of the system using the criteria for the Security, Availability, Processing Integrity, Confidentiality and Privacy (Control Criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (AICPA, Trust Services Criteria). Based on this evaluation, we assert that the controls were effective throughout the period January 01, 2025 to November 30, 2025, to provide reasonable assurance that:

- Based on the control criteria, The system was protected against unauthorized access, use, or modification to achieve Safe Security service commitments and system requirements.
- Based on the control criteria, The system was available for operation and use, to achieve Safe Security service commitments and system requirements.
- Based on the control criteria, The system information is collected, used, disclosed, and retained to achieve Safe Security service commitments and system requirements based on the control criteria.

Signed by:
Viditkumar Baxi
1A3C793E4D66484...

Viditkumar Baxi,

Chief Information Security Officer, Safe Securities Inc.

Date: 13 March 2026

III. Safe Securities Inc's Description of its product 'SAFE'

Safe Securities Inc.'s Description of its product 'SAFE'

Company History and Overview of Operations

About

Safe Securities Inc. is headquartered in Palo Alto and has a global team with the vision to build Cybersecurity Superintelligence. Its Autonomous Cyber Risk Management Platform - SAFE - is an AI-native solution that helps CISOs, security leaders, and third-party risk teams continuously identify, prioritize, and manage cyber risk. SAFE represents a fundamentally new way to manage cyber risk, purpose-built as a cyber risk decision engine for modern enterprises. It unifies Cyber Risk Management (CRQ), Continuous Threat Exposure Management (CTEM), and Third-Party Risk Management (TPRM) into a single platform.

The result is an intelligent and Agentic system that links strategy to execution, internal enterprise to external ecosystem risk, and data to measurable outcomes; giving leaders clear visibility, precise prioritization, effective remediation, and the ability to scale cyber risk management across the organization.

Service Offerings

SAFE

SAFE One empowers CISOs, TPRM leaders, and cybersecurity teams, to continuously and efficiently quantify, prioritize, and mitigate cyber risks. Unlike manual, point-in-time, black-box approaches, SAFE offers Agentic AI-powered, continuous, and defensible cyber risk management, based on objective telemetry and transparent, open risk standards across the entire attack surface.

SAFE CRQ:
SAFE CRQ is the category leader, noted for its GenAI capabilities by leading analysts. SAFE CRQ, like all other SAFE products, is built upon AI-first foundations. Users leverage AI-powered summaries, dashboards, and insights which empower CISOs to know and understand cyber risk, strategically prioritize investments based on ROI, and efficiently report and communicate with the Board and Regulators

SAFE TPRM:
SAFE TPRM is the 100% autonomous TPRM platform powered by Agentic AI. From onboarding and due diligence to dashboards, reporting, and off-boarding, SAFE's Agentic workflows can be tuned to suit the users' requirements, automating every manual process across the TPRM lifecycle. SAFE delivers a unified platform to manage the entire TPRM program, coverage at scale without adding headcount, and zero-effort vendor interactions.

SAFE CTEM:
SAFE CTEM is the autonomous platform that connects exposures directly to business risk. It shifts security teams from manually collecting findings to autonomously prioritizing and remediating the most critical exposures first.

SAFE CTEM autonomously scans assets across the entire scoped attack surface to continuously update findings. SAFE CTEM can manage exposure risks autonomously from the get-go; from identifying the most high-risk exposures, to creating issues and routing remediation efforts to the correct teams via customizable agentic workflows.

Relevant Aspects of Safe Securities Inc.' Overall Control Environment

The overall control structure apart from the reported controls consists of five major components:

- Control Environment
- Risk Assessment
- Monitoring
- Systems Control Activities
- Application Information and Communication

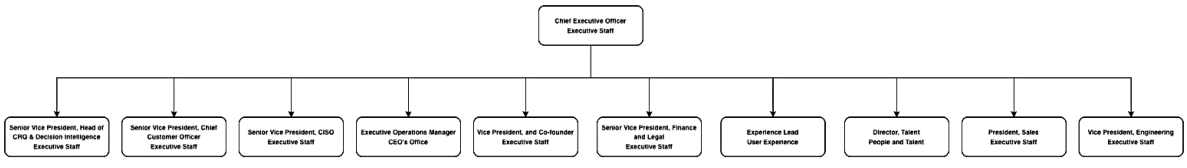
These components' primary objective is to establish an appropriate control environment to develop and implement an internal control process to help achieve specified control objectives.
These components are general and apply to the entire organization. Appropriate involvement of the management is necessary to facilitate the proper functioning of the internal control structure.

Control Environment

The following is a description of Safe Securities Inc.' key control environment elements as related to its business activities.

Organization Structure

Organization structure refers to the formal system of authority, communication, roles and responsibilities, and relationships within the organization. It determines how roles and responsibilities flow between different levels of management.



Organization Chart

Assignment of Authority and Responsibility

The control environment is greatly influenced by the extent to which individuals recognize that they will be held accountable. The extent of accountability includes the assignment of authority and responsibility for operating activities and establishing reporting relationships and authorization protocols.

The following are the responsibilities of key personnel within the organization structure:

Systems	Description
Chief Executive Officer/ Leadership	• Responsible for providing strategic direction for information security initiatives. • Responsible for providing strategic direction to the leadership management to drive business and related policies. • Responsible for facilitating strategic planning for future organizational development. • Responsible for collaboration with Directors, CFO, and Head of Business units on future business growth. • Responsible for ensuring that information security issues are appropriately addressed in the Business Plan. • Responsible for reviewing and monitoring information security aspects through the management review meeting.
Chief Information Security Officer	• Responsible for implementing, establishing, monitoring, and continuous enhancement of Information Security within the organization. • Responsible for implementing, establishing, monitoring, and continuous improvement of Information Security. • Responsible for making sure the information security Manager/Officer has the necessary authority to uphold organizational security, privacy, and compliance and to enforce governance. • Responsible for providing policy and operational guidance to the organization for protecting information assets. • Responsible for ensuring compliance with existing information security policies, standards, and procedures. • Responsible for developing and implementing organization-wide information security programs. • Responsible for documenting and disseminating information security policies and procedures. • Responsible for reviewing Information Security Annual Report/Internal Audit report etc.
Chief Financial Officer	• Responsible for overall oversight of Finance Functions • Responsible for MIS – Budget and Taxations • Responsible for management of Statutory compliances in the Finance sector • Responsible for Audit and Assurance closure • Responsible for extending necessary assistance to ensure security, privacy, and compliance objectives are met and risks are managed in accordance with defined policies and processes.
Head of Engineering	• Responsible for designing and maintaining scalable, reliable, and secure software architecture and platforms. • Responsible for leading engineering delivery, ensuring high code quality, strong development practices, testing, and secure operations.

Systems	Description
	• Responsible for overseeing system design, infrastructure, and deployments to support scalability, availability, and resilience. • Responsible for driving the engineering roadmap, technical decisions, and continuous improvement of development processes. • Responsible for managing and mentoring engineering teams, fostering collaboration, innovation, and technical ownership. • Responsible for ensuring effective integration of systems and tools to support efficient and secure product development. • Responsible for leading the development, integration, and continuous improvement of AI capabilities within the product, ensuring performance, reliability, and responsible use.
Head of Product Management	• Responsible for long- and short-term product vision • Responsible for Innovative Product Development • Responsible for Business Strategy and Development • Responsible for Collaborative Leadership • Responsible for Architectural Excellence • Responsible for the market, business case, and competitive analysis • Responsible for Works on prioritizing the upcoming requirements for the Product based on the product vision
Head of Architecture	• Responsible for Strategic Architecture Planning • Responsible for Providing strong leadership to engineering teams, fostering a culture of innovation, collaboration, and continuous improvement. • Responsible for the development of robust and scalable solutions that meet industry standards and regulatory requirements. • Responsible for Leading the design and review of architectural solutions, ensuring they adhere to best practices, architectural principles, and established patterns. • Responsible for Driving initiatives to optimize the scalability and performance of Safe Securities' platforms and systems, anticipating future growth and demand. • Responsible for collaborating with security and compliance teams to ensure that architectural designs and implementations meet industry standards and regulatory requirements. • Responsible for defining and governing the architecture of AI/ML capabilities, ensuring scalable, reliable, and responsible integration of AI into products and platforms.
Head of Customer Success	• Responsible for understanding our mission and values and communicating them to customers on a regular basis as you lead our training, onboarding, and support efforts. • Responsible for establishing and maintaining relationships with customers; continually track their behaviour and proactively help them overcome obstacles.

Systems	Description
	• Responsible for Foster collaboration within the team and throughout the customer lifecycle; serve as the go-to resource for customers and the point of contact between customers and our Agile product team. • Responsible for Establishing and improving the customer lifecycle, customer base segmentation, and different approaches (e.g., self-serve vs managed enterprise, etc.) • Responsible for measuring and improving adoption cycles by defining adoption metrics and goals. • Increase renewal rates, MAU and NPS while reducing churn.
Head of Human Resource	• Responsible for taking care of the complete employee life cycle. • Responsible for Designing and implementing HR policies. • Responsible for taking care of the legal and regulatory process. • Responsible for the safety, and well-being, engagement, and morale of employees responsible • Responsible for Performance Management System

Human Resources ('HR')

The Human Resources (HR) department plays a crucial role in developing key strategies to facilitate employee communication and create an engaging and productive work environment. HR is responsible for managing the entire employee life cycle, which includes manpower staffing, onboarding, background verification, employee training, performance appraisals, transfers, disciplinary processes, and resignations.

As part of the onboarding process, all new hires for SAFE must undergo a rigorous background verification conducted by a third-party vendor to validate their submitted credentials. Additionally, all employees are required to read and sign the appointment letter and the intellectual property & confidentiality agreement. They also participate in an induction program designed to familiarize them with the organization, their respective departments, product domain, technical skills, professional tools, and company culture.

Employee Training

Safe Securities Inc. has established a robust Employee Security Awareness program to ensure that all employees receive annual security and privacy training. This comprehensive program includes interactive, real-world simulations designed to equip employees with the knowledge to recognize and respond to potential threats and cyberattacks effectively. Additionally, Safe continuously updates its training materials to keep employees informed about emerging cybersecurity risks and best practices, reinforcing a proactive security culture within the organization.

Employee Onboarding and Exit Management

Employee onboarding at Safe Securities Inc. is a structured process designed to integrate new hires seamlessly into the organization while providing them with the necessary resources, support, and guidance to ensure their success and productivity. During onboarding, new employees receive access to Google Suite and Slack, followed

by an orientation program where they are introduced to the company culture, teams, organizational structure, policies, and guidelines. Additionally, non-disclosure agreements and other formalities are discussed, and department-specific tools and training are provided.

When an employee decides to leave Safe Securities Inc., they formally notify the department lead, HR team, reporting manager (RM), and department head via email. A People Business Partner then conducts an exit interview to gather feedback. The respective teams are informed of the resignation, and the exit process is initiated. The team lead oversees a structured knowledge transfer to ensure the smooth transition of ongoing duties and responsibilities. All access credentials are revoked, and company assets are retrieved at the end of the notice period on the employee’s last working day.

IT Operation

Safe Securities internal IT department is responsible for managing all aspects of the organization's IT systems and infrastructure, including software management, incident response, security measures, end-user support and training, budgeting and procurement, compliance and governance, disaster recovery, and more.

Additionally, the team is responsible for actively investigating and addressing any hardware issues to maintain the efficiency and accessibility of IT systems and services. Through vigilant monitoring and proactive intervention, the IT department ensures the smooth operation of digital assets, preventing disruptions and maximizing organizational productivity. This involves continuously evaluating and improving IT processes, resource allocation, and strategic planning to align technological capabilities with business objectives

Finance

Safe Securities Inc.' entire financial and accounting operations of the business are managed by the finance team. To ensure the efficient operation of the company, this team collaborates closely with the pertinent departments, particularly human resources, sales and delivery teams, the team also takes part in client-related activities i.e. billing and collections.

Key responsibilities of the finance team include securing funds to support the company’s needs, allocating funds among departments, managing cash flow, reviewing, monitoring, and managing budgets, creating long-term business plans, and monitoring accounting and tax compliance, among others.

Office Admin

Safe Securities Inc. function supervises the daily support operations of our company and ensures day-to-day office operations are performed seamlessly and efficiently. The admin works actively, internally, and externally with the third-party vendors to ensure each department's needs are met. The duties include logistics management at the time of onboarding or exit of any team member, event management, inventory control, handling and verification of assets, travel bookings and management, employee safety, workplace, and warehouse management.

Legal

Legal Department at Safe Securities Inc. overseas contract management, regulatory compliance, corporate governance data privacy & security and risk mitigation related to contracts, applicable law including rules & regulations, and legal proceedings. Serving as the central authority for contractual agreements made by the Safe Securities Inc. Additionally, the legal department: (i) safeguards the company's intellectual property assets, including trademarks, patents, copyrights, and brand names; (ii) advice on employment-related matters, including employee contracts, workplace policies, discrimination claims, and labour disputes, to ensure compliance with employment laws and regulations; (iii) provides legal support and due diligence assistance in mergers, acquisitions, and other strategic transactions, including drafting transaction documents, conducting legal reviews, and ensuring regulatory compliance; and (iv) handles disputes, lawsuits, and other legal proceedings involving the company, including representing the company in court, negotiating settlements, and working with external legal counsel when necessary. It provides transactional support, aids in understanding legislative and regulatory changes affecting business operations, and collaborates with management, department heads, clients, and business partners for consultation and strategic direction necessary for transactional completion. Moreover, it liaises with relevant local, state, and central government/regulatory bodies in order to ensure smooth functioning of Company's day to day business operations in compliance with law.

Customer Support

Customer Success in SAFE ensures that our customers meet and exceed their desired business objectives from the SAFE platform and have an outstanding experience when using the platform. This is achieved through a combination of three functions:

Customer Success Advisors - who work with customers on a regular basis to develop risk programs for the usage of SAFE within their business, consulting and informing key stakeholders as they do so.

Risk Advisory services - who provide professional services advising customers on how to model and understand the risks detailed by the SAFE platform.

Technical Operations and Field Engineering - who provide customer technical support and custom integration services, as well as operating all production infrastructure and SAFE platform instances.

Information Security

Safe Securities Inc.'s information security team is responsible for implementing, establishing, overseeing, and continuously enhancing the organization’s information security processes and governance, ensuring alignment with industry best practices. The team is tasked with ensuring that all aspects of the organization comply with the security framework, which includes infrastructure and operations, regulatory requirements, risk mitigation, incident response, business continuity planning, vulnerability management, and more.

Additionally, the information security team conducts regular audits to assess compliance with industry best practices. The results of these audits and assessments are presented to management during routine review meetings, offering valuable insights into the organization’s security posture and identifying areas for

improvement. Through their dedicated efforts, the information security team plays a crucial role in protecting the organization's assets, maintaining regulatory compliance, and effectively mitigating security risks.

Risk Assessment

The organization has established a formal risk management process to identify, assess, and manage risks across the enterprise, including organizational, product, technology, cybersecurity, AI, privacy, legal, regulatory, and reputational domains.

Risk Management Process

The Information Security, Product, Engineering, Privacy, and relevant business teams are responsible for ensuring that strategic, operational, technical, AI-related, and compliance risks are identified and effectively managed. The organization maintains a risk assessment framework that evaluates risks across business operations, products and services, data processing activities, AI capabilities, and supporting infrastructure. Risk assessments are performed at least annually and upon significant changes such as new product releases, architectural changes, introduction of AI features, or regulatory updates. The risk management process follows a structured approach to identifying, assessing, treating, and monitoring risks.

Process Steps

Risk Identification

Identifying potential sources of risk that could impact organizational objectives, including risks related to operations, product functionality, cybersecurity threats, AI model behavior, data protection, third-party dependencies, and regulatory obligations.

Risk Assessment

Analysing the likelihood and impact of each identified risk and prioritizing the risks based on their level of severity.

Risk Evaluation

Determining the most appropriate response to each risk, including accepting, mitigating, transferring, or avoiding the risk.

Risk Control

Implementing controls to manage risks, including security safeguards, privacy protections, AI governance measures, process improvements, technical controls, training, and contractual or insurance mechanisms.

Risk Monitoring and Review

Continuously monitoring risks and control effectiveness through periodic reviews, metrics, audits, and change management processes to ensure risks remain within acceptable levels and to address emerging threats, including those related to evolving technologies and AI.

Monitoring

Monitoring is a process that assesses the quality of internal control performance over time. Monitoring controls define how senior management continually:

- Evaluate internal and external issues and risks faced by the Company.
- Provide strategic direction for major information security initiatives.
- Provide strategic direction to the leadership management to drive business and related policies.
- Review and monitor information security aspects through the management review meeting.

Safe Securities Inc.'s management and leadership team actively monitor the quality of internal control performance as part of their ongoing activities. To support this monitoring, management has implemented a series of management reports, which are reviewed by the relevant stakeholders. Actions are taken based on the observations in these reports whenever necessary.

Cloud Security Monitoring

Safe Securities Inc. employs a comprehensive suite of cloud security tools to continuously monitor its cloud workloads. The company leverages CrowdStrike, Wiz, Observe, AWS products such as GuardDuty, CloudTrail, CloudWatch, and other tools to proactively detect and respond to potential security threats within its cloud environment. This multi-layered approach enables Safe Securities Inc. to monitor and swiftly address any suspicious or malicious activities across its cloud accounts and servers.

To ensure the ongoing security of its infrastructure, Safe Securities Inc. conducts Architecture Reviews on a sprint-to-sprint basis. This proactive approach allows the company to assess any new architectural changes introduced in its product and enhance its Infrastructure as Code templates to maintain a secure configuration.

Application Monitoring

A centralized dashboard to monitor all customer-deployed instances is available through Observe. It provides the health status of all instances to approved Support personnel, allowing them to quickly assess and address any potential issues. Alerts are configured in the Observe Monitoring section, and real-time notifications are sent to Slack for immediate visibility across the team. For Priority 1 alerts, which require urgent attention, the Customer Support team’s on-call rotation team is paged directly to ensure swift response and resolution. This ensures that critical incidents are addressed promptly, minimizing potential disruptions to customer services.

System Control Activities

Safe Securities Inc. utilizes process documents as the foundation for its control environment, ensuring that business objectives are achieved through controlled means. These documents are supported by periodic reviews of the implemented controls to identify and address risks, aligning efforts with business goals. Control activities are applied across all levels of the organization and by function. These activities include segregation of duties, defined approval processes for system management and changes, access control standards, and periodic reviews to assess the effectiveness of the implemented controls.

We have established Policies and Procedures for critical processes as part of the Information Security Management System v1.16. These include the following:

- Information Security Policy
- Document Control Policy
- Information Classification and Handling Policy
- Clear Desk & Clear Screen Policy
- Password Security Policy
- Human Resources Security Policy
- Acceptable Use Policy
- Email Access & Usage Policy
- Internet Access & Usage Policy
- Asset Management Policy
- Removable Media Policy
- Malware Protection Policy
- Remote Access Policy
- Privacy & Protection Policy
- Information Security Awareness Policy
- Physical & Environmental Security Policy
- Mobile Device Policy
- Bring Your Own Device Policy
- Information Security Group Operational Policy
- Access Control Policy
- Vendor Management Policy
- Equipment Security Policy
- Encryption Policy
- Change Control Policy
- Log Management Policy
- Data Security Policy
- Information Systems Acquisition, Development, and Maintenance
- System Configuration & Security Policy
- Network Configuration & Security Policy
- Servers Configuration & Security Policy
- Application Development & Deployment Policy
- Cloud Security & Compliance Policy
- Vulnerability and Patch Management Policy
- Information Security Incident Management Policy
- Information Storage, Retention & Retrieval Policy
- Risk Management Policy
- Fraud Management Policy

- Compliance Management Policy
- Software Development and Lifecycle Policy
- Hardening Policy
- Business Continuity Management Policy
- Breach Notification Policy

Service Organization Quality Manual outlines the organization's approach to maintaining quality within the Management system. It provides the guiding principles and responsibilities necessary to enforce and safeguard the quality parameter of services.

Information and Communication

Pertinent control information is critical to maintaining an effective internal control system. Information is identified, captured, and communicated in a form that enables organization personnel to carry out their responsibilities.

The in-scope systems, software, and applications are as follows:

Systems	Description
Workstations (Laptops/ Desktops)	All Workstations (Desktops/Laptops) are hardened as per the Device hardening requirements defined in Hardening Policy.
Anti-virus	Workstations and Servers are configured and updated regularly with the latest Anti-Virus signature, and identified discrepancies are recorded and resolved by the IT Team.
E-mail	Google Suite is used as the primary tool for communication of emails. Critical organizational communications, corporate events, and activity updates are communicated over corporate email.
Patch Management	Patch Management of all Workstations and Endpoints is performed using the Automox tool, and AWS Patch Manager is used for patching of AWS services. All Organisational Endpoints and Customer instances are tracked, and patches are applied periodically.
IT Service Management	Jira Service Desk platform allows IT support to be more organized, focused, efficient, and effective. End users raise service tickets, incident tickets to notify their problems, which are tracked by the respective IT managers.
Network and System Monitoring	All the service requests are logged in the Service request log and tracked to closure. Network bandwidth is monitored daily.
AWS WAF	The AWS services are access controlled and protected from external attacks by the usage of AWS WAF. All inbound and outbound network traffic is routed through a firewall.

Systems	Description
AWS GuardDuty	Amazon GuardDuty is a threat detection service that continuously monitors malicious activity and unauthorized behaviour to protect AWS accounts, workloads, and data stored in Amazon S3.
AWS Macie	To discover and protect sensitive data stored in AWS resources.
AWS Config	AWS Config service is used to assess, audit, and evaluate the configurations of AWS resources. AWS Config continuously monitors and records AWS resource configurations and allows the respective teams to automate the evaluation of recorded configurations against desired configurations.
Observe	Observe is a cloud-native security monitoring platform designed to provide real-time visibility into the health and security of cloud environments. Observe is used to track and analyse the cloud infrastructure, identifying potential threats, vulnerabilities, and performance issues.
Wiz	Wiz is a cloud security platform used to secure the cloud environments by identifying vulnerabilities, misconfigurations, and compliance risks. It provides real-time visibility into cloud infrastructure and workloads, allowing teams to continuously monitor and manage security posture.
Semgrep	Semgrep is a static analysis tool that enables developers to detect security vulnerabilities, code quality issues, and bugs by scanning source code. It supports multiple programming languages and is designed to perform fast, lightweight, and customizable code reviews.

Network

Safe Securities Inc. operates its network infrastructure in the cloud, with exclusive VPN access granted to all critical systems, each of which is meticulously access controlled. Access to the cloud infrastructure via VPN entails establishing a secure, encrypted connection between the user's device and the cloud services. This connection safeguards transmitted data from unauthorized access, eavesdropping, and tampering. Prior to deployment, every device undergoes a rigorous and secure configuration process to ensure its resilience against potential security threats.

Vendor Management

Safe Security adopts a structured, risk-tier–based approach to Third-Party Risk Management in alignment with its Vendor Management Policy. Third parties are classified into defined tiers based on business criticality, type of service provided, and the sensitivity of data accessed or processed. This tiering model ensures that the depth and rigor of due diligence are proportionate to the level of risk each vendor introduces. For all vendors, Safe conducts a baseline security review that includes a questionnaire-driven assessment to validate the vendor's security, privacy, and operational controls. For higher-tier and business-critical vendors, the assessment scope

is expanded to include detailed evidence review, risk evaluation, and formal approval based on defined satisfaction criteria.

In addition to documentation-based reviews, Safe performs an automated Outside-In security assessment for applicable vendors using SAFE's Third-Party Module. This capability evaluates the vendor's external security posture through digital attack surface discovery based on domains and internet-facing assets, covering 100+ automated controls across areas such as DNS Security, Email Security, Application Security, Network Security, System Security, Breach Exposure, and Compromised Assets.

The tiered model enables Safe to apply enhanced scrutiny to high-risk vendors while maintaining efficient oversight of lower-risk providers, ensuring consistent, risk-aligned third-party governance across the vendor lifecycle.

Electronic Mail

Safe Securities Inc employs advanced techniques to secure electronic communications, including robust spam filtering, sophisticated phishing detection, and encryption protocols such as DMARC, DKIM, and SPF to ensure email integrity and prevent spoofing. We also utilize Email DLP to help prevent unauthorized sharing of sensitive information via email. Continuous monitoring and policy updates further enhance email security and reduce exposure to evolving threats.

Corporate Shared Drive

Safe Securities Inc.'s corporate Shared Drive serves as a centralized repository for all employees, streamlining access to a comprehensive collection of essential organizational documents including business and security policies, procedures, and process documents, as part of the Google Suite online storage solution. This process simplifies and enables staff members to quickly locate and reference important materials.

The Shared Drive is regularly updated with information about the organization's various activities, ensuring that employees stay informed about the latest developments. Documentation detailing the policies and procedures for significant processes is meticulously organized and readily accessible, providing a transparent and reliable resource for the entire organization.

Data Classification and Handling

Safe Securities Inc. has established an Information Classification and Handling Policy to govern the classification and management of information within the organization. This policy outlines guidelines for identifying and classifying information, labelling data, and securely storing it based on confidentiality requirements.

Access to information is restricted according to its classification level, ensuring that sensitive data is only accessible to authorized personnel. Privileged access to critical resources is granted strictly based on defined user roles and requires requisite approval. Additionally, the creation and modification of access control records for information management systems are governed by the Access Management Policy.

Vulnerability and Patch Management

Safe Securities Inc. has defined the Vulnerability and Patch Management policy to effectively implement vulnerability and patch management within the organization. SAFE follows the Agile model and sprint workflow to help organizations tackle overall project work. Automated Vulnerability Assessment which includes both Static Application Security Testing and Software Composition Analysis is conducted continuously, and Manual Vulnerability Assessment and Penetration Testing are conducted on SAFE Products every sprint on newly developed features. The developed code is dynamically tested for any hardcoded credentials/secrets. All the identified Critical/ High/ Medium/ Low severity Vulnerabilities are remediated and deployed on the system following the Change Management process.

For the Endpoints, the vulnerability patches are configured and pushed using the Automox tool. Daily cron jobs are scheduled for periodic patching of all the endpoints. Once the process is completed the overall report is generated to validate the pending patches and re-deploy them as applicable.

For the AWS EC2 instance Patching, the patches are configured and pushed from the AWS Patch Manager. All the patches on the AWS are deployed on the system following the Change Management process. Once the process is completed, the sanity check is performed to test the working of the system.

Backup and Restoration

Safe Securities Inc. has established a Backup Policy and process to ensure the secure and reliable backup of the SAFE product. Code repositories, gateway servers, and databases are backed up daily on the AWS cloud. Database backups are encrypted and stored in a S3 bucket, ensuring data confidentiality and integrity. All backed-up data is retained for 35 days, with periodic integrity checks performed to verify data consistency and recoverability.

Change Management

Safe Securities Inc. implements a rigorous Change Management Process, prioritizing changes based on Business Impact to minimize operational disruptions. Change requests must include detailed justifications and are meticulously documented, tracked, and approved by relevant stakeholders. Before deployment in the production environment, all changes undergo thorough testing to meet quality and security standards. Additionally, affected teams and business units are informed in advance about potential downtime and other relevant details to ensure seamless transitions.

Security Incidents

Safe Securities Inc. follows a structured and rigorous approach to managing security incidents. Upon detection, incidents are promptly logged via service desk and assessed by the Information Security Group (ISG) based on severity High, Medium, or Low. Immediate containment measures, such as isolating compromised systems, are taken to prevent further impact. A thorough investigation is conducted to identify the root cause and develop a Corrective Action Plan. This plan focuses on both resolving the current issue and enhancing security controls to prevent recurrence. Lessons learned from each incident are documented and used to refine security strategies.

Regular reviews and updates to incident response procedures ensure continuous improvement. Through this proactive approach, Safe Securities Inc. maintains the integrity, resilience, and operational continuity of its information systems.

Business Continuity

Safe Securities Inc. has established a robust Business Continuity Policy and Plan to ensure uninterrupted operations. The platform is designed for high availability, leveraging multiple availability zones and regular data backups for seamless recovery. Critical data, including customer assessments, code repositories, databases, and gateway servers, is backed up consistently. A comprehensive Business Continuity and Disaster Recovery (BCDR) plan is in place, ensuring rapid response to disruptions. To validate its effectiveness, Safe Securities Inc. conducts annual continuity drills and Business Continuity Plan (BCP) tests. These proactive measures enhance resilience, minimize downtime, and maintain operational integrity.

Breach Management

Safe Securities Inc. has implemented a Breach Notification Policy to ensure a structured response to security breaches. The policy classifies breaches as critical or non-critical, each with specific notification timelines. It defines key stakeholders for notification, including Board Members, Customers, Insurers, Employees, and Media outlets. This structured approach ensures timely communication, enhancing transparency and accountability. By promptly informing relevant parties, the organization minimizes the impact of security incidents and maintains trust. The policy aligns with regulatory requirements, reinforcing Safe Securities Inc.'s commitment to security and compliance.

SLA Management

The Service Level Agreement (SLA) outlines Safe Security's commitment to providing timely support for customer requests and incidents. SLA commitments are defined and governed as per the applicable customer contract. Customers can report issues through the following communication channel:

- JIRA Service Desk – Used for logging, tracking, and managing support tickets to ensure timely resolution in accordance with agreed service levels.

Cloud Platform and Application Management

Cloud

All SAFE workloads operate on AWS, with development, testing, and production accounts centrally managed through AWS Organizations. SAFE is deployed across various AWS regions based on customer requirements. Production workloads are hosted in separate AWS accounts from development and UAT environments to maintain security and isolation. Any changes to production accounts follow a structured process using automated planned deployments, ensuring consistency and minimizing risks.

Application

The SAFE product provides SaaS services to customers, with the Engineering teams following Agile methodology for continuous delivery. The application progresses through Design, Development, Validation, Staging, UAT, and

Deployment phases. Each two-week sprint integrates the Secure Development Lifecycle to ensure security best practices. Automated and manual Vulnerability Assessment and Penetration Testing (VAPT) are conducted by the Security team to identify and mitigate risks.

Artificial Intelligence (AI)

SAFE incorporates Artificial Intelligence capabilities across the platform to support automated data processing, AI Agents, workflow assistance, and generation of contextual insights for users. The platform uses a combination of internally managed models, open-source models, and third-party hosted large language models to support features such as risk analysis, summarization, and search across modules including CRQ, TPRM, and CTEM. AI processes customer inputs within the tenant context to generate requested outputs, with logical segregation maintained between customers. Prompts and outputs may be retained for limited operational purposes such as usage history. Customers can manage the availability of AI features within the platform.
AI capabilities operate within the SAFE application environment and follow established development, monitoring, and change management processes. Interactions with AI services are logged, and access to AI functionality is governed by user roles and permissions. Data transmitted for AI processing is encrypted in transit and handled in accordance with platform security practices. The organization periodically reviews AI features to evaluate performance and reliability. These practices help ensure that AI functions as an integrated component of the SAFE service environment.

Development Cycles

Safe Security employs an Agile Product Development methodology for the development of the SAFE platform. This approach involves multiple cross-functional Scrum teams that perform planning, development, integration, testing, and delivery within two-week sprint cycles. In addition to regular sprint releases, Safe Security addresses defects in supported versions through minor releases as needed.

The development methodology incorporates continuous security testing, including Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST) and Software Composition Analysis (SCA), along with periodic manual Vulnerability Assessment and Penetration Testing (VAPT) to ensure the security and integrity of the product. Performance benchmarking is also conducted to ensure the platform meets defined performance and scalability requirements.

Project Management

Safe Securities Inc. follows the defined Project management methodology. Multiple engagements are delivered by standard processes defined across all 11 knowledge areas and 5 process groups - initiating, planning, executing, monitoring/controlling, and closing:

- Project Integration Management
- Project Scope Management
- Project Schedule Management
- Project Cost Management
- Project Quality Management

- Project Resource Management
- Project Communications Management
- Project Risk Management
- Project Procurement Management
- Project Release and Program Management
- Project Stakeholders Management

Here, Safe gathers requirements, responds to RFPs, sends quotations and once the PO (Purchase order) gets released Safe takes a kick-off call with the client followed by pre-requisites sharing.
The continuous governance takes place through daily, weekly, and monthly updates and QBRs during execution till project closure. Safe use Tools and Technology to create project artifacts, reports. This helps in secure data storage and maintaining confidentiality.

Personal Data Handling and Protection

Safe Securities Inc. databases enforce the authentication for all employees who have access to personal information. Furthermore, Safe actively prevents third parties from getting access to the personal information that Safe stores and/or processes on our database. Safe have implemented reasonable security measures in our website and application i.e., using the HTTPS protocol, SSL Tunnel, etc. to actively safeguard the data flow.

Personal Data Retention & Disposal

Safe Securities Inc. has established a Privacy and Protection Policy to manage personal data. When users register on the website, application, or platform, SAFE collects Personally Identifiable Information (PII) such as Name, Email, and Contact Number. This data is securely stored in a database and can be updated via email or account settings. PII is retained as long as necessary to fulfil its purpose and for a reasonable period thereafter to meet audit, contractual, legal, or business requirements. This ensures compliance and protection of user information.

Principal Service Commitments and System Requirements

Safe Securities Inc. designs its processes and procedures to meet its objectives for the SAFE system. Those objectives are based on the service commitments that SAFE makes to user entities (customer), the laws and regulations that govern the provision of the SAFE System, and the financial, operational and compliance requirements that SAFE has established for the services.

The Safe Security services are subject to relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which SAFE operates.

- Security, Availability, Confidentiality, Integrity, and Privacy commitments to SAFE are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided on the AWS website. Security, Availability, Confidentiality, Integrity, and Privacy commitments are standardized and include, but are not limited to, the following:

- Security and Confidentiality principles inherent to the fundamental design of the SAFE System are designed to appropriately restrict unauthorized internal and external access to data and customer data is appropriately segregated from other customers.
- Security and Confidentiality principles inherent to the fundamental design of the SAFE System are designed to safeguard data from within and outside of the boundaries of environments which store a customer's content to meet the service commitments.
- Availability principles inherent to the fundamental design of the safe system are designed to make the data accessible to authorized and appropriate backups are taken and maintained to ensure accessibility.
- Integrity principles inherent to the fundamental design of the safe system are designed to appropriately restrict unauthorized internal and external modifications to data and customer data is appropriately segregated.
- Privacy principles inherent to the fundamental design of the safe system are designed to protect and safeguard personal information and appropriately handle data.

Safe Security establishes operational requirements that support the achievement of Security, Availability and Confidentiality, Integrity and Privacy commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in 'SAFE' system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Safe Security.

-- End of Report –

[This space is left blank intentionally]

[This space is left blank intentionally]