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, 2022 to November 30, 2022**

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, 2022 to November 30, 2022, 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.

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's 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's 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's 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 provide a reasonable basis for our opinion.

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

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, 2022 to November 30, 2022, 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 LLP

BDO India LLP

30/03/2023

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.

30/03/2023

We, as management of Safe Securities Inc. (Safe Securities) are responsible for designing, implementing, and maintaining effective controls over Safe Security's systems providing SAFE (Security Assessment Framework for Enterprises) ('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, 2022 to November 30, 2022 to achieve the commitments and system requirements related to the system using the criteria for 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, 2022 to November 30, 2022, to provide reasonable assurance that:

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

DocuSigned by:
Vidit
1A3C793E4D66484...

Safe Securities Inc.

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 is headquartered in Palo Alto with a 200-member global team. SAFE Security is a pioneer in Cybersecurity and Digital Business Risk Quantification & Management, helping organizations measure and manage cyber risk in real-time using its API-first SAFE Platform.

Services Offerings

SAFE (On Cloud)

SAFE is a Cyber Risk Quantification and Management (CRQ+M) platform that can be used to comprehensively visualize and create a common risk taxonomy to communicate (and align) stakeholders across the organization, change the security conversation from tactical project-led benefits to strategic value, and cement the security and risk leader's role as a partner and enabler to the business. Safe does this by ingesting Real-Time telemetry via Read Only APIs from 50+ cybersecurity tools such as Crowdstrike, Qualys, Tenable, AWS, Azure, GCP, KnowBe4, and Proofpoint among others while taking into account business context and external threat landscape to provide risk visibility that is objective, continuous and jargon-free. In Safe, Businesses can visualize their risk at an Enterprise / Business Unit / Application / Datacenter (or Cloud) all the way down to each Asset / Employee of an organization along with getting a prioritized set of actionable insights to mitigate the risks that matter most to the business.

Sub-service Organizations

Safe Securities uses Amazon Web Services (AWS) and Google Workplace Services (G-suite) as a sub-service organization (hereinafter referred to as the "sub-service organization"). This Description includes controls and control criteria of Safe Securities and does not include controls and control criteria of the sub-service organizations.

Relevant Aspects of Safe Securities' 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.

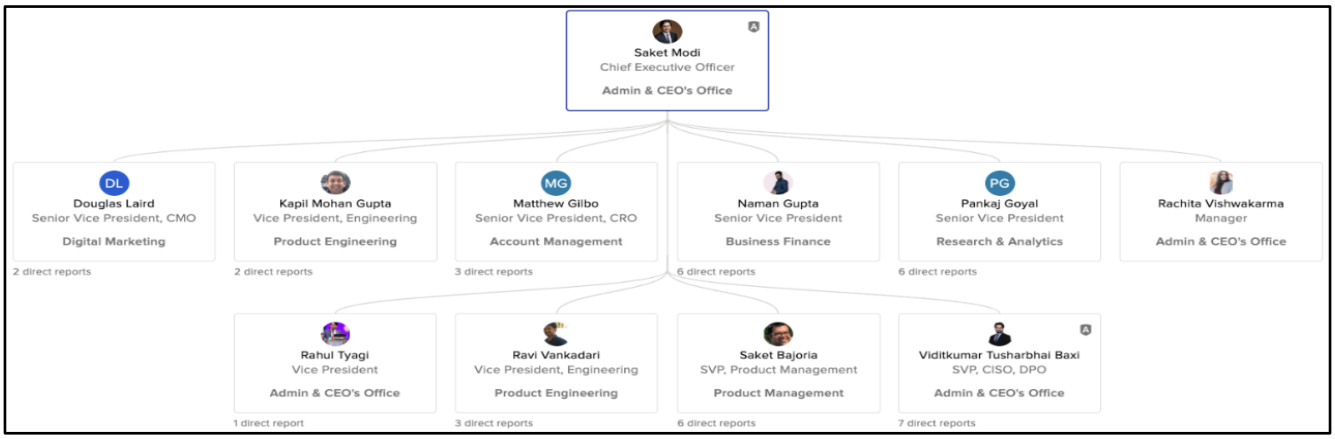
These components are general and apply to the entire organization. Appropriate involvement of the management is necessary to facilitate the functioning of the internal control structure.

Control Environment

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

Organization Structure

Service Organization's organization structure provides the framework within which its activities for achieving the organization's entity-wide objectives are planned, executed, controlled, and monitored. Significant aspects of establishing a relevant organizational structure include defining critical areas of authority and responsibility and establishing appropriate reporting lines.



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:

Roles	Responsibilities
Chief Executive Officer/ Leadership	• Provide strategic direction for information security initiatives. • Provide strategic direction to the leadership management to drive business and related policies. • Facilitate strategic planning for future organizational development. • Collaborate with Directors, CFO, and Head of Business units on future business growth. • Ensure that information security issues are appropriately addressed in the Business Plan. • Review and monitor information security aspects through the management review meeting.
Chief Information Security Officer	• Responsibility for implementing, establishing, monitoring, and continuous enhancement of Information Security within the organization.

	• Responsibility for implementing, establishing, monitoring, and continuous improvement of Information Security. • Make sure the information security Manager/Officer has the necessary authority to uphold organizational security, privacy, and compliance and to enforce governance. • Provides policy and operational guidance to the organization for protecting information assets. • Ensures compliance with existing information security policies, standards, and procedures. • Developing and implementing organization-wide information security programs. • Documenting and disseminating information security policies and procedures. • Review Information Security Annual Report/Internal Audit report etc.
Chief Finance Controller	• 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	**People:** • Responsible for motivation of their Direct reports • Ensures Direct reports are aligned to the Company's, Product's and Team's vision. • Ensures their direct reports are working for the agreed-upon time. • Assist career development of team members. • Conducts weekly meetings with the team. **Process:** • Responsible for the overall "How" to fix an issue or implement a defined feature. • Removes overall bottlenecks in the system. • Ensures Engineering Best practices are met. • Ensure Secure Coding guidelines are followed. • Responsible for the rate of production and lead time (what each engineer needs to fulfil their commitment) • Responsible for initial high-level sizing • Maintains Engineering + Quality metrics. **Technology:** • Pro-actively works with the team to improve technical solution/architecture. • Responsible for conducting forward-leaning technology investigations (spikes) • Negotiating with the architect on technical approaches
Head of Product Management	• Responsible for long- and short-term product vision • Responsible for the market, business case, and competitive analysis • Responsible for ROI of an Epic

	• Captures and incorporates relevant customer feedback. • Prioritizes features for releases based upon expected ROI. • Maintains and prioritizes an Epic backlog of the product. • Makes trade-off decisions between scope (value in Expected ROI) and schedule (higher operating expense in longer releases) • Ensures that features are being developed in conjunction with Product Owners to meet Customer Expectations • Works on prioritizing the upcoming requirements for the Product based on the product vision
Head of Architecture	• Evaluates the architecture and works with the development and project management teams to create new and existing features. • Analyse project constraints to identify alternatives, reduce risks, and, if necessary, implement process re-engineering. • Fixes technical issues as they arise. • Examines the potential business effects that specific technical decisions may have on the operational procedures of a client. • Supervises and guides development teams. • Monitor and guide CI/CD pipelines. • Monitor AWS infrastructure
Head of Customer Success	• Understand our mission and values and communicate them to customers on a regular basis as you lead our training, onboarding, and support efforts. • Establish and maintain relationships with customers; continually track their behaviour and proactively help them overcome obstacles. • 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. • For each sprint, create, keep up with, and order JIRA tickets in accordance with client comments/requests. • Establish and improve the customer lifecycle, customer base segmentation, and different approaches (e.g., self-serve vs managed enterprise, etc.) • Measure and improve adoption cycles by defining adoption metrics and goals. • Increase renewal rates and NPS while reducing churn
Head of Human Resources	• Responsible Takes care of the complete employee life cycle of the Company • Designing and implementing HR policies • Takes care of the legal and regulatory process • Accountable for the safety, and well-being, engagement, and morale of employees responsible • Responsible for Performance Management System

Human Resources (HR)

The HR department's responsibilities are to manage the entire Employee Life Cycle, which mainly includes Manpower Staffing, Joining Formalities, Background Verification, Employee Training, Employee Appraisal, Employee Transfer, Training, Disciplinary Process, and Employee Resignation.

As part of an employee's joining process, all new hires for SAFE need to undergo a verification check, verification checks are conducted, where a third-party vendor verifies credentials submitted by new hires. Further, all employees read and sign the appointment letter and intellectual property & confidentiality agreement. They undergo an Induction program intending to induct a new hire and give them an overview of the organization.

Human Resources (HR) is responsible for managing personnel and related activities within an organization, such as recruitment and selection, training and development, compensation and benefits, performance management, employee relations etc. HR's mission is to foster a positive and productive work environment that contributes to the overall success of the organization.

As part of the pre-joining process, all new hires at Safe Security are subjected to background checks. An approved contractor/vendor and/or the appropriate law enforcement agencies perform the checks.

Additionally, all employees must read and sign both the appointment letter and the confidentiality agreement. They go through an induction programme designed to welcome new employees and give them an overview of the organization and its departments, as well as knowledge of the Product (Domain), Technical Skills, Professional Tools, and organizational culture.

Employee Training

The CISO and department heads provide overall supervision and guidance to the System. The people team walks new hires through the policies, benefits, and guidelines, followed by a cultural orientation.
Annual information security training is provided to all employees of the organization via an online portal.

Employee Onboarding

Employee onboarding is the process of integrating new employees and providing them with the resources, support, and guidance they need to become successful and productive team members. Access to G Suite and Slack is shared with the new joiner during Onboarding, followed by the Orientation programme, where they are briefed on policies and guidelines. Non-disclosure agreements and other joining formalities are discussed with the new hire, and then department-specific tools and training are provided.

Employee Offboarding

Employee notifies the department lead, HR team, reporting manager (RM), and department head via email that they have decided to part ways. The employee is contacted by the People Business Partner, who conducts an exit interview. Additionally, the teams are made aware of the resignation and the start of the exit process. The team lead oversees a knowledge transfer to transfer the ongoing duties and activities. All accesses are terminated, and assets are reclaimed after the notice period has ended and on the last working day.

IT Operation

The internal IT team is in charge of managing the firewall, network, patch, incident, security administration, desktop and server, and the entire internal IT systems and infrastructure.

In order to ensure the efficiency and accessibility of IT systems and services, the team is also in charge of looking into, identifying, and fixing network, hardware, and software issues.

Finance

The 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.

Other crucial tasks performed by the team include raising 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 Administration

The administration 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.

Procurement

The Procurement team takes care of all types of procurement and is primarily responsible for negotiating with vendors and suppliers to acquire the most effective deals and reduce procurement expenses. It coordinates with the finance division and relevant project/ department heads to agree on payment issues, and budget allocation and ensure compliance with project requirements.

Legal

The Legal Department manages the contracts, regulatory compliance, and risk management concerning contracts, regulatory compliance, and litigation. The Legal team is the central authority for contractual arrangements entered into by the Safe Securities team and acts as a monitoring function to track legal and regulatory exposures.

It also aims at preserving the company's IP assets such as trademarks, patents, copyrights, and brand names, providing transaction support, helping understand the legislative and regulatory changes that may impact business operations, coordinating with management, business heads, clients, business partners for consultation and strategic direction that may be required for the consummation of a transaction, liaison with relevant local, state, and central government/ regulatory bodies.

Customer Support

Customer Support drives the customer relationship after the handover to Operations. It helps the customer achieve the business objective by guiding them in the implementation of Playbook use-cases to ensure optimum ROI and understanding the new feature requirements or enhancements in the existing one to fulfil the implementation of the playbook use-cases. Customer Support handles the customer communication for the bugs/ incidents reported by the customers and manages the updates and upgrades communication.

Information Security

Implementing, establishing, overseeing, and continuously enhancing the organization's information security process and governance in accordance with industry best practices is the responsibility of the infosec team. The team is in charge of making sure that every aspect of the organization adheres to the security framework, which keeps track of all infrastructure and operations, regulatory compliances, risk management, incident management, business continuity management, vulnerability management, etc.

The information security team is also in charge of conducting information security audits on a regular basis and assessing compliance with industry best practices. During a routine management review meeting, the results of these audits and assessments are presented to the management.

Risk Assessment

The organization has implemented the following process to manage various risks faced by the Company.

Risk Management Process

The Information Security Group and the Product team are in charge of ensuring that strategic, operational, managerial, business, legal, regulatory, and reputational risks are effectively managed.

The organization has implemented a risk assessment framework. The Information Security Group identifies, assesses, and manages risks in the technological environment at least once a year.

The organization's risk management process takes a systematic approach in identifying, assessing, controlling, and monitoring risks.

The process typically consists of the following steps:

Risk Identification

Identifying potential sources of risk that could affect the organization's objectives.

Risk Assessment

Analyzing 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 measures to manage the risks, such as modifying processes or policies, increasing resources, or acquiring insurance.

Risk monitoring and review

Ongoing monitoring of risks and risk control measures to ensure their effectiveness and to identify any changes that may require updating the risk management Process.

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 organization.
- Provide strategic direction for major information security initiatives.
- Assist the leadership and management with providing strategic direction for the business and related policies.
- Review and monitor information security aspects through the management review meeting.

Safe Securities' management and leadership team monitor the quality of internal control performance as part of their activities. To aid in this monitoring, management has implemented a series of management reports that are reviewed by appropriate stakeholders, and actions are taken on observations as needed.

Cloud Security Monitoring

The following Cloud Security tools are enabled to monitor cloud workloads continuously:

- Crowdstrike
- AWS GuardDuty
- AWS Security Hub
- AWS Cloud Trail
- AWS WAF
- AWS Macie
- AWS Cloud Watch
- Data Dog

The findings are managed using AWS Security Hub. AWS Chatbot service is also enabled and integrated with Slack for real-time reporting of the new alerts generated to the team.

AWS Billing custom reports are generated weekly and monthly and pushed to stakeholders via Slack to be aware of the system components used and the costs associated with them. Additionally, Hourly and Daily updated AWS Cost Monitoring dashboards are also available in AWS Quicksight for the whole organization to monitor the cloud cost in real-time and a weekly report email is sent to the subscribers.

Application Monitoring

A centralized dashboard to monitor all the customer-deployed instances is available at https://app.datadoghq.eu/dashboard. It provides the health status of all instances to approved Support personnel. Alerts are configured in the Datadog Monitoring section and real-time notifications are sent to Slack for visibility. For Priority 1 alerts which require immediate attention, the Customer Support team's on-call rotation team is paged via Datadog -> OpsGenie integration.

System Control Activities

Process documents serve as the foundation for the control environment to help ensure that business objectives are attained through managed methods and spaces, accompanied by recurring reviews of the controls that have been put in place to find and address risks in order to achieve business objectives. At all organizational levels and according to each function, control activities are implemented. Implemented control measures include separation of duties, clear approval procedures for system management and changes, requirements for access controls, and periodic evaluations of the effectiveness of the implemented control measures.

We have established our Policies and Procedures for critical processes as part of Information Security Management System v1.14 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
- IS Awareness Policy
- Physical & Environmental Security Policy
- Mobile Device Policy
- Information Security Group Operational Policy
- Access Control Policy
- Vendor Management Policy and Process
- 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 and process
- Information Security Incident Management Policy
- Information Storage, Retention & Retrieval Policy
- Risk Management Policy
- Fraud Management Policy
- Compliance Management Policy
- SDLC Process
- Business Continuity Management Policy
- Breach Notification Policy

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 desktops/laptops are hardened as per the defined hardening guidelines.
Anti-virus	Workstations and servers are set up and updated with the EDR. The status of EDR is monitored on a regular basis, and any discrepancies are documented and resolved by the IT and ISG teams.
E-mail	G-Suite is the email communication tool used by the service organization. Using corporate email, important organizational communications, business events, and activity updates are shared.
Patch Management	Service Organization uses the Patch management tool to patch all the endpoints and AWS instances. Endpoints and Customer instances are tracked, and patches are applied periodically.
IT Service Management	Service Organization uses a tool that allows IT support to be more organized, focused, efficient, and effective. End users raise service tickets, and incident tickets to notify their problems, and IT managers can track the same.

Systems	Description
Network and System Monitoring	All the service requests are logged in the Service request log and tracked to closure. Network bandwidth is monitored daily.
WAF	The AWS services are controlled and used behind the firewall. All the traffic is routed using a firewall.
AWS GuardDuty	Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behaviour in order to protect your AWS accounts, workloads, and data stored in Amazon S3.
AWS Security Hub	AWS Security Hub is a cloud security posture management service that provides a centralized view of security findings generated by various AWS security services
AWS Detective	Amazon Detective makes it easy to analyse, investigate, and quickly identify the root cause of potential security issues or suspicious activities.
AWS Config	AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. Config continuously monitors and records your AWS resource configurations and allows you to automate the evaluation of recorded configurations against desired configurations.
AWS Cloud Trail	Amazon CloudTrail is a service provided by Amazon Web Services (AWS) that logs AWS API calls and events for your AWS accounts.
Data Dog	Datadog is a cloud-based monitoring and analytics platform that provides real-time visibility into the performance, availability, and overall health of your infrastructure, applications, and logs.

Network and Telecommunication

Safe Securities hosts its network in the cloud, and only VPN access is permitted to all of the vital systems, which are all access-controlled. Using a cloud through a VPN involves establishing a secure, encrypted connection between the user's device and the cloud server. This connection protects the data being transmitted over the internet from unauthorized access, eavesdropping, and tampering. For any device, before being installed it is securely configured and hardened.

System Acquisition and Maintenance

Safe Securities Business Heads and CISOs ensure that utmost importance is provided to the product/ system's security features while evaluating the vendor products/ services. Wherever applicable, communication paths used to communicate between the parties are encrypted, and secure protocols are used. All third parties are categorized into four tiers (Critical/ High/ Medium/ Low) as defined in the Vendor Management process; vendors are subjected to a third-party assessment before onboarding.

Electronic Mail

Safe Securities uses the G-Suite product for communication. Google Workspace provides professional email, online storage, shared calendars, video meetings, and several other features. Business communications, corporate

events, and activity updates are some primary events communicated using the organization's corporate email. G-Suite administrative rights are restricted to the required individual and provided on a Need-to-Know and Need-to-use basis. User access rights and administrative access rights are reviewed quarterly.

Corporate Shared Drive

The corporate Shared Drive in Safe Securities is accessible to all employees as part of G-Suite online storage. Access to business and security policies, procedures, and process documents is made simple for staff members by the shared drive. All additional updates on the organization's various activities are also included on the drive. Significant processes' policies and procedures are outlined in documentation and are accessible on the organization's shared drive.

Data Classification and Handling

Safe Securities have defined the Information Classification and Handling policy for the classification and handling of information stored within the organization. The organization has defined guidelines that prescribe identification and classification of information, labelling of information, and secure storage of information based on confidentiality requirements. Access to the information is restricted based on the classification category it possesses and privileged access to sensitive resources is restricted to defined user roles post requisite approval. Creation and modification of access control records for the information management systems occur through the Access Management Policy.

Vulnerability and Patch Management

Safe Securities has defined the Vulnerability and Patch Management policy to effectively implement vulnerability and patch management within the organization. SAFE follows the Agile model and Agile 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 after every sprint and on every newly developed feature. The developed code is dynamically tested for any hardcoded credentials/secrets All the identified Critical/ High/ Medium/ Low Vulnerabilities are remediated and deployed on the system following the Change Management process.

For the Endpoint patching, the patches are configured and pushed using the Automox application. Daily cron jobs are scheduled for patching 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 has defined a Backup policy and process which captures all the backup requirements of the SAFE product. Server and Databases are backed up daily on the AWS cloud. Database backups are encrypted and stored

using AWS Backup service, and all the backed-up data is stored for 35 days, and periodic integrity checks are performed.

Change Management

Safe Securities' Change management process is carried out on a priority level based on Business Impact. A Change is requested by the requestor mentioning the details and Justification.

After the change request is submitted, all changes are documented, tracked, and approved by the appropriate stakeholders. The necessary updates are successfully tested and rolled out before being deployed on production. The concerned team or business unit that could be impacted by the change is informed of the change's downtime details and other specifications.

Security Incidents

At Safe Securities, security incident calls are logged by the system via mail, call, or in person. An IT engineer is assigned to the issue logged. If the problem is identified as an information security incident the incident severity is defined (High, Medium, and Low) and the reporting process is followed. The reported incident is informed to the relevant stakeholder and the implementation of correction is initiated. Post that the root cause of the incident is identified, and the affected information system(s) is isolated from the network (as applicable). Once the Root cause is completely identified the Corrective action plan is defined and implemented to mitigate the future possibility of the Incident.

Business Continuity

Safe Securities has established a Business Continuity policy and plan. To support continuous availability, the platform is set up to operate across multiple availability zones and the backup of data is maintained to enable the continuity requirement. Data from customer assessments, code repositories, databases, gateway servers, and other sources are backed up using the Backup process. The organization has defined a Business Continuity and Disaster Recovery plan and tests its effectiveness annually through continuity drills and BCP tests.

Breach Management

Safe Securities defines the Breach Notification Policy as defining the notification requirements to be followed in the event of an information security breach in the organization. There are two types of data breaches critical and non-critical w.r.t the timelines for each breach type. The Notification defines the Internal and External Stakeholders, such as Board Members, Customers, Insurers, Employees, Media, and so on.

Third-Party Management

The Vendor Management policy has been defined by Safe Securities. Wherever possible, communication paths between the parties are encrypted, and secure protocols are used. All third parties are classified into four tiers (Critical / High / Medium / Low), and vendors are subjected to a third-party assessment and periodic review based on their tier.

SLA Management

Service level agreement defines the commitment from the Safe team to support customers within the stipulated time for any support request or incident reported by the customers. Customers can raise the support requests via the below-mentioned communication mediums:

1. Service Manager
2. Telephonic conversation with the Customer Success and/or Program Manager only in case of Critical and High Incidents

Cloud Platform and Application Management

Cloud

All workloads in the SAFE run-on AWS. AWS accounts for development, testing, and production are linked to AWS Organizations for centralized management. SAFE deployed in various AWS regions based on customer requirements. Production workloads run on separate AWS accounts from development or UAT accounts. Changes to production accounts are made via automated planned deployments.

Application

The SAFE product offers SaaS services to customers. The Engineering teams follow Agile methodology to deliver new versions of the application. The application goes through the various phases of Design, Development, Validation, Staging, UAT, and Deployment. The Engineering team follows a two-week sprint where the Secure Development Lifecycle is followed during each phase of the process. A Security team performs automated and Manual VAPT of the application.

Development Cycles

Safe Securities follows Agile Product Development Methodology for SAFE product development. Multiple cross-functional SCRUM teams continuously plan, develop, integrate, test, and deliver products in two-weeks sprints. Also, bug fixes on major supported versions are released to customers as minor versions as and when needed.
We perform continuous SAST, SCA, manual Vulnerability Assessment and Penetration Testing (VAPT) analysis, performance benchmarking, customer bugs review, sprint reviews, etc. to achieve the above engineering metrics.

Project Management

Safe Securities follows the Project management methodology defined. 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 Stakeholders Management

Here, we gather requirements, respond to RFPs, send quotations and once the PO (Purchase order) gets released we take 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. All project artifacts, reports, and data are stored safely, and complete confidentiality is maintained. Mutual NDAs are signed to ensure this. Post engagement closure NPS and feedback are gathered, and lessons learnt are captured for future reference.

Personal Data Handling and Protection

Databases require usernames and passwords for our employees who can access personal information. In addition, Safe actively prevents third parties from getting access to the personal information that we store and/or process on our database. We 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 have defined the Privacy and Protection policy to deal with and handle personal data, currently SAFE collects personal information when the user registers to use the website, application, or platform. Organizations collect personal information (also referred to as Personally Identifiable Information or "PII"), including name, address, online contact information such as your email address or username, phone number, and other personal information. The information collected will be stored in the database. The PII is retained for as long as needed to fulfil the purpose for which we collected it and for a reasonable period thereafter to comply with the audit, contractual, or legal requirements, or where we have a legitimate interest in doing so.

Principal Service Commitments and System Requirements

Safe Securities 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 Securities 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 Securities 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 Securities.

-- End of Report --

[This space is left blank intentionally]