System and Organization Controls 3 (SOC 3)

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

For the Period June 01, 2021 to November 30, 2021

Table of Contents

I. REPORT OF INDEPENDENT AUDITORS

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 SAFE Product" (Assertion), that Safe Securities Inc.'s (Safe Securities) System controls were effective throughout the period June 01, 2021 to November 30, 2021, 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 SAFE product and was not conducted for the purpose of evaluating Safe Securities' cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

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 Securities 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.

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,

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

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 SAFE product were effective throughout the period June 01, 2021 to November 30, 2021, 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

March 31, 2022

II. MANAGEMENT'S REPORT OF ITS ASSERTION ON THE EFFECTIVENESS OF ITS CONTROLS OVER SAFE PRODUCT

contact@safe.security
www.safe.security

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

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

April 12, 2022

We, as management of Safe Securities Inc. (Safe Securities) are responsible for designing, implementing, and maintaining effective controls over Safe Securities' 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 June 01, 2021 to November 30, 2021 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 June 01, 2021 to November 30, 2021, to provide reasonable assurance that:

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

DocuSigned by:
Vidit
1A3C793E4D66484...

Safe Securities Inc.

March 31, 2022

III. DESCRIPTION OF SAFE SECURITIES' SYSTEM AND CONTROLS

Description of Safe Securities' System and Controls

Background and Overview of Services

Safe Securities is a Palo-Alto headquartered Cyber Risk Quantification company. It helps organizations measure and mitigates enterprise-wide cyber risk in real-time using its ML Enabled API-first SAFE platform by aggregating automated signals across people, processes, and technology, both for 1st & 3rd party to dynamically predict the breach likelihood (SAFE Score) & Risk of an organization.

User entities and their independent auditors are responsible for determining if the services provided to them by the Company are in the scope of this report.

Sub-service Organizations

Safe Securities uses Amazon Web Services (AWS) 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.

Boundaries of the System and Scope Products in Scope

Safe Securities operates on a work from home model but has its corporate office in Palo Alto, USA and New Delhi, India. The scope of this report is limited to Operations, HR Processes, Administration & Facilities, and IT activities relating to SAFE.

Product: SAFE (Security Assessment Framework for Enterprises) product, SAFE is a SaaS cybersecurity and cyber risk quantification platform.

SAFE (On Cloud)

SAFE is a SaaS cybersecurity and cyber risk quantification platform. It uses a supervised Machine Learning engine to give an output in the form of a Breach Likelihood Score (between 0-5) and the potential financial risk an organization faces within the next twelve months. With one of the world's largest API repositories, SAFE takes input from signals across people, processes, technology, cybersecurity products, and third parties. The Breach Likelihood scores (SAFE Score) are calculated at a macro and micro level and can be measured for lines of business, crown jewels, cloud assets, and more. SAFE also provides prioritized actionable insights and enables businesses to measure, manage, and mitigate enterprise-wide cyber risk.

Description of Control Environment, Control Activities, Risk Assessment, Monitoring and Information and Communication

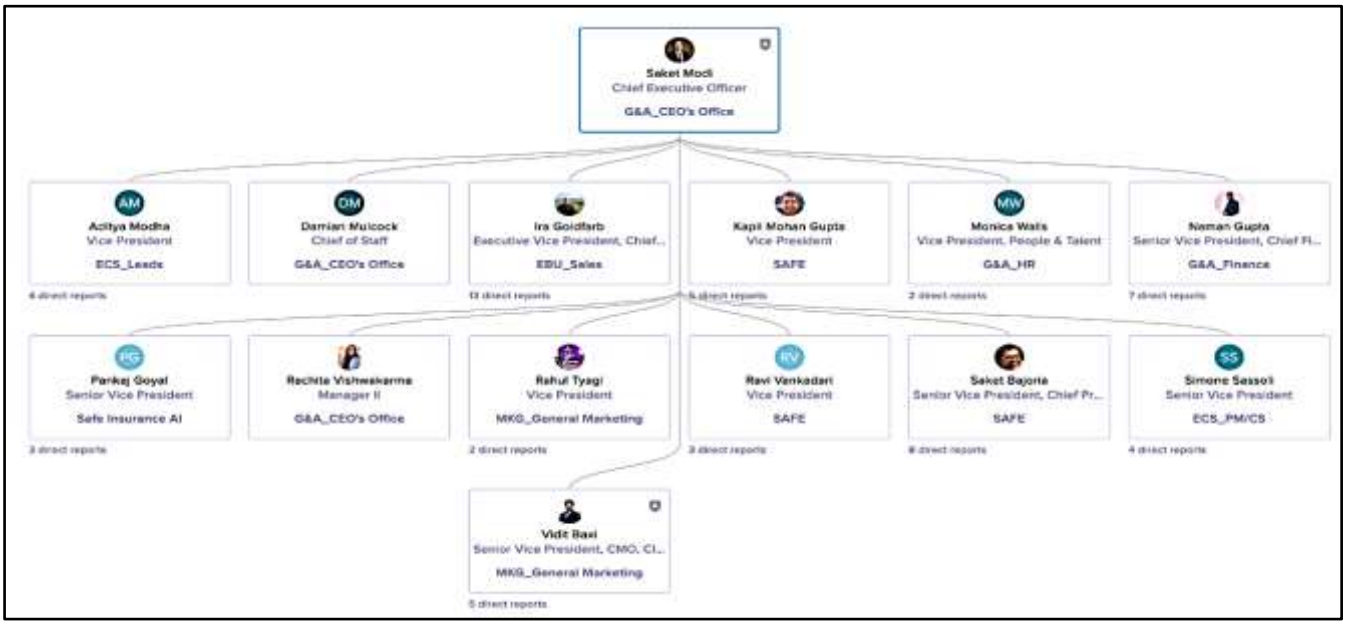
Integrity and Ethical Values

Safe Securities requires directors, officers, and employees to observe high standards of business and personal ethics in conducting their duties and responsibilities. Honesty and integrity are core principles of the company, and all employees are expected to fulfil their responsibilities based on these principles and comply with all applicable laws and regulations. Safe Securities promotes an environment of open communication and has

created an environment where employees are protected from any kind of retaliation should a good faith report of an ethics violation occur. Executive management has the exclusive responsibility to investigate all reported violations and to take corrective action when warranted.

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 major 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 Manager/Officer is empowered to enforce governance and maintain Organization level security, privacy and compliance. • Ensure that information security issues are appropriately addressed in the Business Plan. • Review and monitor information security aspects through the management review meeting.

Roles	Responsibilities
Chief Information Security Officer	• Responsibility for implementing, establishing, monitoring and continuous improvement of Information Security. • Provides policy and operational guidance to the organization. • Provides security standards and guides for protecting information assets. • Ensures compliance to existing information security policies, standards and procedures. • Developing and implementing organization-wide information security programs. • Documenting and disseminating information security policies and procedures. • Review and approve the information security policies and risks periodically. • Review Information Security Annual Report/Internal Audit report • Drive the strategic direction of our technology, product & offerings considering emerging and legacy technologies. • Oversee all aspects of the technology, including technical strategy, technology architecture, best practices & technology stack. • Prepare and/or review high-level and detailed design documents. • Responsible for overseeing complete IT operations and IS operations.
Chief Financial Officer	• Overall oversight of Finance Functions • MIS – Budget and Taxations • Statutory compliances in the Finance area • Audit and Assurance closure • Extending required support to ensure security, privacy, compliance objectives are achieved & risks are well managed as per the defined policies at Org level including Finance
Head of Engineering	**People:** • Ensures 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 • Assists 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 • 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 the market, business case, and competitive analysis • Responsible for long- and short-term product vision • Responsible for ROI of a feature • Captures and incorporates relevant customer’s feedback • Prioritizes features for releases based upon expected ROI • Provide Acceptance Criteria for each feature • Maintains and prioritizes a feature backlog of the product

Roles	Responsibilities
	• Makes trade-off decisions between scope (value in Expected ROI) and schedule (higher operating expense in longer release cycles) • Works with Product Owners to ensure features are getting developed that Customers expect • Works on prioritizing the Next Cycle's Feature
Head of Architecture	• Conducts an architecture evaluation and collaborates with project management and IT development teams for new and existing features. • Evaluate project constraints to find alternatives, alleviate risks, and perform process re-engineering if required. • Fixes technical issues as they arise. • Analyses the business impact that certain technical choices may have on a client’s business processes. • Supervises and guides development teams. • Monitor and guide in CI/CD pipelines. • Monitor AWS infrastructure, IAM accesses
Head of Customer Success	• Understand our mission and values and communicate them to customers regularly as you lead our training, on-boarding and support efforts • Build/maintain customer relationships; continuously monitor customer use and proactively ease them out of roadblocks • Be the customer concierge and the liaison between customers and our Agile product team; foster collaboration within the team and across the customer lifecycle • Create, maintain, and prioritize JIRA tickets based on customer feedback/requests for each sprint • Define and optimize the customer lifecycle, segmentation of customer base and varying strategies (e.g., self-serve vs managed enterprise, etc.) • Define adoption metrics and goals, measure and improve adoption cycles • Increase renewal rates and NPS while reducing churn • Recruit and lead customer success team as we grow
Head of Human Resource	• Takes care of the complete employee's life cycle of the Company • Designing and implementing HR policies • Takes care of the legal and regulatory process • Responsible for Employee engagement, morale, welfare and safety • Performance Management System
Office Admin Manager	• Maintain and order necessary office equipment and supplies, as needed. • Help organize small to large scale events and provide ongoing assistance during events. • Responsible for supervision of general and clerical office activities. • Manage organisation's office and storage space, providing maintenance and security and other occupancy and logistics services
Procurement Manager	• Sourcing and engaging reliable vendors and suppliers and negotiating with them. • Issuing purchase orders and organizing delivery of goods and services. • Controlling the procurement budget and saving on procurement costs. • Overseeing and managing systems for tracking inventory and supply of goods and materials.

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.

Employee Training

HR creates training plans based on the various roles in the organization or training requests received from various teams. Information Security training is conducted periodically through an online portal for all the Employees of the organization.

Employee Onboarding and Exit Management

As a part of joining formalities, recruit information is collected as per the defined process. Candidates are registered in the HRIS, and an employee ID is created for each new employee. A joining announcement email is sent to the respective relevant stakeholders, and the workstation allocation process is initiated.

As a part of exit management, once the employee resigns from the employment to the HR via email, resignation information is intimated to the Payroll SPOC and updated in the HRMS system. An exit interview is conducted, and the employee is required to hand over his/her current activities/responsibilities to a fellow team member. The employee is asked to get clearance from relevant departments on the release date, and his/her access is revoked on the last working day.

IT Operation

The IT operations team is responsible for internal IT-related services i.e., network operations and desktop support, and IT Security which includes Firewall management, support server management, security administration, patch management, network monitoring, electronic mail ('e-mail') administration. The team is also responsible for analysing, troubleshooting, and resolving system hardware, software, and networking issues.

Office Admin

The administration function supervises the periodically support operations of our company and ensures day-to-day office operations are performed seamlessly and efficiently. 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, 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.

Finance

The finance team is responsible for the entire financial and accounting functions of the Company. This team works closely with the relevant departments, mainly human resources, and delivery teams, to ensure the Company's smooth functioning. This team is also involved, along with the sales and delivery teams, in client matters such as billing and collections.

The other vital functions of the team are to raise funds to meet the needs of the business; allocate funds among the department; monitor and manage cash flows; review, monitor and manage budgets; develop long-term business plans; keep track of accounting and tax compliances and the like.

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, upgrades communication.

Risk Assessment and Risk Management

The In-scope Safe teams are responsible for providing leadership and oversight for effective management of strategic, operational, managerial, business, legal, regulatory, and reputational risks.

The organization has a risk assessment framework in place. The identification, assessment, and management of risks within the technology environment are carried out periodically by the respective teams.

The risk management process adopted in the organization comprises primarily of the following steps:

Risk Identification

The process involves finding, recognizing, and describing the risks that could affect the achievement of an organization's objectives. It is used to identify possible sources of risk and the events and circumstances that could affect the achievement of objectives. It also includes the identification of possible causes and potential consequences.

Risk Assessment

The process is used to understand the nature, sources, and causes of the risks identified and estimate the risk level. It is also used to study impacts and consequences and to examine the controls that currently exist.

Risk Review and Validation

The process is used to compare risk analysis results with risk criteria to determine whether a specified level of risk is acceptable or tolerable.

Control Environment and Information Security

Safe Securities' internal control environment reflects the overall attitude, awareness, and actions of management concerning the importance of controls, and the emphasis given to controls in the Company's policies, procedures, methods, and organizational structure.

The Chief Executive Officer, the Senior Management Team and all employees are committed to establishing and operating an effective Information Security Management System in accordance with its strategic business objectives. The Management at Safe Securities' is committed to the Information Security Management System, and ensures that IT policies are communicated, understood, implemented, and maintained at all levels of the organization and regularly reviewed for continual suitability.

The team at Safe is responsible for implementing, establishing, monitoring and continually improving the Information Security process and its governance as per industry best practices within the organization. The Information Security team is also responsible for periodically reviewing and conducting Technology and process audits and reviewing compliance against industry best practices. Results of these audits and assessments are shared with the Management as part of a periodic management review meeting.

Monitoring

Monitoring is a process that assesses the quality of internal control performance over time.

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

Cloud Security Monitoring

Safe has implemented cloud security controls based on industry best practices and standards and are enabled to monitor cloud workloads continuously.

The events are managed using the configured solutions and services deployed on the cloud. Safe has configured a chatbot service which is integrated with Safe communication channels for real-time reporting of the new alerts generated to the team.

AWS Billing custom reports are generated periodically and pushed to stakeholders via Safe communication channels to be aware of the system components used and costs associated with it.

Application Monitoring

A centralized dashboard portal to monitor all the customer deployed instances is implemented. It provides the health status of all instances to super admin users and approved support personnel. Alerts are configured at the telemetry server and real-time monitoring is performed by the support personnel tracking and monitoring alerts generated.

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:

- Workstations (Laptops/ Desktops)
- Anti-virus
- E-mail
- Patch Management
- IT Service Management
- Network and System Monitoring
- WAF
- AWS GuardDuty
- AWS Detective
- AWS config
- AWS Macie
- GitHub
- Slack
- Gsuite
- AWS Cloud portal

Network and Telecommunication

Safe Securities hosts its network on the cloud and access to all the critical systems are access controlled and accessed only through VPN. The organization uses multiple cloud applications for day-to-day operations with controlled access. All network equipment devices, including firewall, routers, and operating systems for desktops/laptops & servers, are securely configured, and hardened before placing it in the network.

System Acquisition and Maintenance

Safe Securities ensures that due importance is given 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 a SaaS product for email communication. The SaaS product provides professional email, online storage, shared calendars, video meetings, and several other features such as business communications, corporate events, and activity updates. Administrative rights to the SaaS product are restricted to the required individual and provided on a Need to Know and Need to use basis and are reviewed periodically.

Corporate Shared Drive

The Shared Drive provides employees with easy access to Business and Security policy, procedure, and process documents. The drive also contains all other updates of various activities of the organization. Policy and Procedures for significant processes are documented and available on the organization's shared drive.

Data Classification and Handling

Safe Securities has 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.

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 cycle workflow. Automated Vulnerability Assessment is conducted continuously, and Manual Vulnerability Assessment and Penetration Testing are conducted on SAFE Product after every sprint and on every newly developed feature. All the identified Critical/ High/ Medium/ Low Vulnerabilities are remediated and deployed on the system following the Change Management process.

For the Endpoints patching, the patches are configured and pushed using a patch management system implemented for endpoints. For the cloud instance patching, the patches are configured and pushed from the cloud deployed patch manager.

Backup and Restoration

Safe Securities has defined a Backup policy and process which captures all the backup requirements of the SAFE product. Code Repositories, Gateway servers, and Databases are backed up periodically. Database backups are encrypted and stored in a separate location, and all the backed-up data is stored with a defined retention period, 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 consists of change management details as required by the policy.

Once the change request is raised the changes are recorded and tracked through the Change Management Process, all the changes are reviewed and approved by the relevant stakeholders. The required changes are

tested and rolled out successfully to be deployed on the production. The change details for downtime and other specifications are communicated to the concerned team/business unit who may be affected by the change.

Security Incidents

At Safe Securities, security incident calls are logged by the system via mail, call, or in person. An IT engineer is assigned for the issue logged. 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) 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 defined a Business Continuity policy. The platform is configured to operate across multiple availability zones to support continuous availability. Customer assessment, code repositories, database, gateway server, etc. data is backed up per the Backup process. The organization has defined the Business Continuity and Disaster Recovery plan and tested for effectiveness periodically through Continuity drills and BCP tests.

Third-Party Management

Safe Securities has defined the Vendor Management policy. Wherever applicable, communication paths used to communicate between the parties are encrypted and secure protocols are used. All the third parties are categorized into four tiers (Critical / High/ Medium / Low) as defined in the Vendor Management Process and vendors are subjected to a Third-party assessment and periodic review based on the tiers they fall.

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. Email to support@safe.security
3. Telephonic conversation with the Customer Success and/or Program Manager only in case of Critical and High Incidents

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 product enhancements and bug fixes in two-weeks sprints. Major product versions are released to customers after every sprint. Also, bug fixes on supported major 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, periodically, weekly, monthly updates and QBRs during execution till project closure.

Cloud Platform and Application Management

Cloud

In the context of SAFE, the cloud refers to workloads running in AWS Accounts. Production workloads run in dedicated AWS accounts separate from development AWS accounts. Changes to production accounts are through automated planned deployments. Any manual updates are tracked via tickets in the change tracking product. Currently, SAFE is deployed in various AWS regions based on customer needs.

Application

The SAFE product offers SaaS service 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 final deployment. Automated and Manual VAPT of the application is performed by a separate team that was not directly involved in the development of the product. Deployment and upgrades are managed by the Customer Support team. Customers have the option to choose to upgrade to the latest version. Customer issues are handled by the Customer Support team. If these issues need Engineering support, a dedicated Customer Engineering team handles them. Customer issues that need to be delivered to the customer without waiting for the next major release are done by the Customer Engineering team in the form of Service packs.

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.

Breach Management

Safe Securities defines the Breach Notification Policy for defining the notification requirement to be followed in case of any information security breach that occurs in the organization. All the data breach is divided into two categories Critical and Non-Critical data breach w.r.t to the timelines for each breach type. The Notification defines the Internal and External Stakeholders i.e., Board Member, Customer, Insurers, Employee, Media, etc.

-- End of Report --

[This space is left blank intentionally]