quant Group Cyber Security Framework

Version **2.1**

Sept 2023

Table of Contents

Stakeholders

Name	Position	Signature	Date
Sandeep Tandon	CEO		
Dinesh Khot	Group Chief Information Security Officer		
Drishti Shah	Head of Compliance		
Deepak Pawar	Group Head Information Technology		

Version History

Version	Date	Author / Revision	Revision Description
1.0	December 2021	Dinesh Khot	Information / Cyber Security Framework (ICSF) Version 1.0
2.0	November 2022	Dinesh Khot	Review of Information / Cyber Security Framework (ICSF) Version 2.0
2.1	September 2023	Deepak Pawar Dinesh Khot	Information / Cyber Security Framework (ICSF) Version 2.1 Remove below mentioned Positions from Distribution List 1) Chief Credit Officer 2) Group Head Commercial & SME 3) Group Head - IRMD, Recovery Update BCP location

Distribution List

Unit / Person / Location	Position
Chief Information Security Officers (CISOs)	All Departments
	Chief Risk Officer
	Head of Operations
	Group Head quant
	Head of Compliance
	Head of Global Markets
	Head of HR, Training & Administration
	Chief Technology Officer
	Chief Financial Officer
	Chief Internal Audit
	Group Head - Legal Affairs and Company Secretary
	CEO

1 The Information / Cyber Security Framework

Purpose

The purpose of this document is to detail the approach that has been taken by Quant Group Information Security Dept. (quant ISD) to implement their Information Security Policy and regulatory requirements comprising:

- Regulations of Enterprise Technology Governance & Risk Management Framework for Financial Institutions
- ISO/IEC 27001:2013 titled "Information technology – Security techniques -Information security management systems";
- "Control Objectives for Information and Related Technology (COBIT 5.0)" framework by ISACA;

The contents of this framework are aimed at achieving ISD's commitment to comply with Quant's IS Policy and stated regulations by providing guidance to all employees, customers, suppliers, auditors, and all interested parties for effective implementation Information / Cyber Security principles and practices within Quant Group.

The main objective of Quant's Information / Cyber Security Framework, hereinafter referred to as ICSF, is to maintain adequate levels of confidentiality, integrity and availability across all quant's Information and Information Assets.

Framework Review

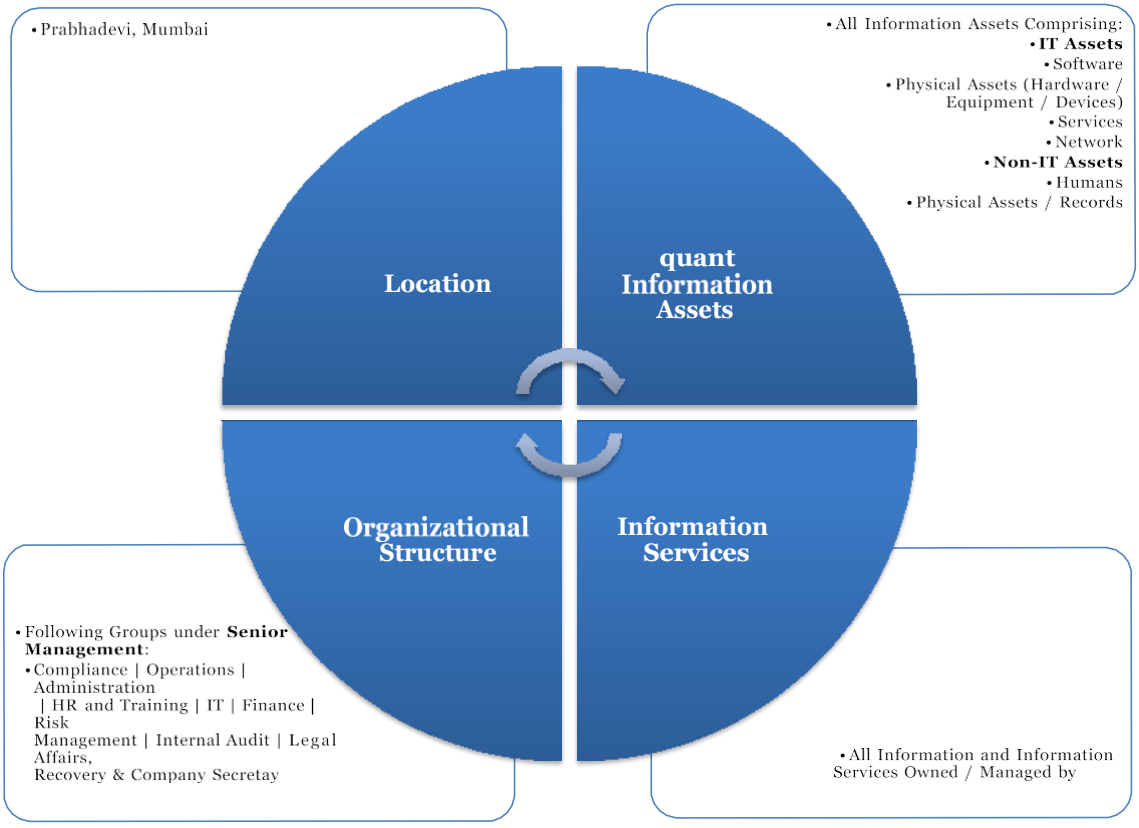
This framework will be reviewed after every One (01) years for its continued suitability and adequacy keeping in view the change in the technical, operational and legal environment. Any material change(s) shall be formally implemented into the framework following approval from the Board, while any immaterial changes shall be presented in the Change Review Committee meetings for subsequent deliberation, review and approval by the committee.

Scope and Boundary

The scope of this ICSF includes the management and protection of quant Information and Information Assets falling under the ownership of Executive / Senior Management.

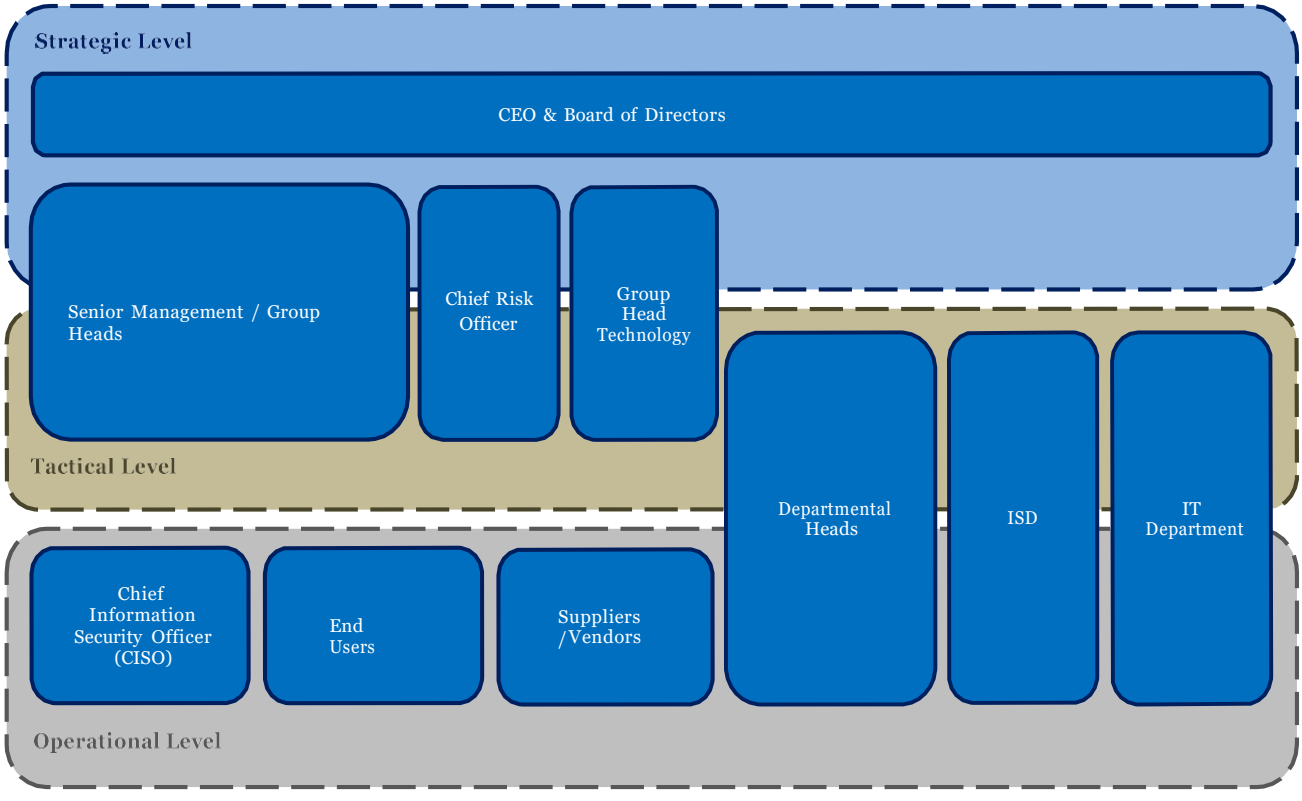
Any hardware, infrastructure and applications that are not managed or owned by quant shall fall outside of the scope of quant's Information / Cyber Security Management.

An illustration of the ISMS scope and boundaries is included underneath:



2 Information / Cyber Security Organization

Organizational Structure



Responsibilities and Authority

Effective implementation of ICSF is the responsibility of all quant employees and concerned parties. It requires active involvement from employees at various levels from the Strategic, Tactical and Operational perspectives. Specific (high-level) responsibilities include:

Strategic Level

This will be represented by the Board of Directors, the quant CEO, Chief Risk Officer, Chief Technology Officer, and other Senior Management / Group Heads who set the strategic direction for Information / Cyber Security within quant. At the strategic level, the entities involved shall be required to establish leadership and commitment towards Information / Cyber Security of the Quant.

Role of the Board of Directors

The Board of Directors shall assume a high-level responsibility to ensure effective governance, management, and implementation of Information Security within the quant. The responsibilities mainly involve:

- Providing a strategic direction on the alignment of Information Security with the quant's objectives.
- Maintaining oversight on the quant's Information Security Management Framework.
- Providing the required support to the Executive Management for effective functioning and strengthening of the Information Security function.

Role of Senior Management / Group Heads

- Assume ultimate responsibility for Information Security within their respective business / areas.
- Ensure that the IS activities and initiatives of their respective Groups are in line with the quant's IS Policy.

Role of the Chief Risk Officer (CRO)

- Ensuring effectiveness of the Information Security Department
- Escalation of significant matters related to Information Security through Risk and Compliance Committee (RCC) and Board Risk Committee (BRC).

Role of the Group Head Technology

- Provide valuable insight and resources to support the ISD for the purpose of enhancing the existing Information Security posture of the Quant.

Tactical Level

The tactical level requires active involvement from the Group Heads, the Chief Risk Officer, Group Head Technology, Departmental Heads, IT Department, and the Information Security Dept. (ISD). At this level, the entities involved shall be responsible for defining and ensuring effective implementation of quant's Information Security policies and procedures.

Role of Senior Management / Group Heads

- Ensure effective implementation of the Quant's Information Security Policy and relevant Procedures in their respective groups.
- Appoint Business Information Security Officer(s) (BISO) at the Group / Departmental level to ensure effective implementation of Information Security Policy within each Group.

Role of the Chief Risk Officer (CRO)

- Supervise the overall functioning of Information Security in quant.
- Ensure periodic update and review of the Information Security Policy for the approval of the BoD.

Role of the Group Head Technology

- Ensure that the Information Security requirements are appropriately adhered to within IT Initiatives and operations.

Role of Department Heads

- Liaise between the Group Heads and Information Security Management at the Departmental Level (BISOs) to ensure effective Implementation of the IS activities within each Department.
- Ensure that the IS activities and initiatives of their respective Departments are in line with the

Quant's IS policy.

Role of the Chief Information Security Officer

- Ensure that the IS Framework and Objectives are strategically aligned with the Quant's IT and Business Objectives.
- Plan, Execute, Monitor and Review the activities and effectiveness of the Information Security Dept. (ISD) on ongoing basis.

Responsibilities of Information Technology Department (ITD)

- Provide insight to ISD and obtain the necessary inputs on various projects and / or initiatives.
- Ensure active involvement from the ISD throughout the project lifecycle.

Operational Level

The operational level requires active involvement from the Group Heads, Departmental Heads, IT Department, the Chief Information Security Officer (CISO), and the Information Security Dept. (ISD). At this level, the entities involved shall be responsible for implementing and maintaining Quant's Information Security policies and procedures. This will be represented by:

Role of Department Heads

- Responsible for implementation of the quant's Information Security Policy and relevant Procedures in their respective Departments.

The Information Security Department (ISD)

Specific responsibilities of the ISD include:

- Prepare an Information Security Action Plan aligned with the Quant's IS Policy.
- On an annual basis, conduct IS Risk Assessment in consultation with the concerned business to identify new threats and vulnerabilities and identify appropriate controls to mitigate any new risks.
- Provide awareness on the contents of the Information Security Policy.
- Review the Information Security Policy after every one year or on need basis to maintain adequacy in light of emergent business requirements or security threats.
- Review and improve the Information Security procedures on need basis to ensure their effectiveness.
- Maintain, update and distribute the Incident Response Plan and Procedures to all users.
- Complete tasks as required by the Information Security Procedures.

Responsibilities of Information Technology Department (ITD)

Information Technology Department's responsibilities with respect to Information Security include, but are not limited to:

- Applying Quant's Information Security Policy and relevant procedures as applicable to all IT assets.
- Administering user authentication.
- Implementing IT related countermeasures identified during IS Risk Assessment exercise.
- Facilitating ISD in performing IS Risk Assessment activities.
- Facilitating the ISD with monitoring and controlling all access to Quant's Information Systems.
- Maintaining an up-to-date network diagram.
- Restricting access to critical information assets.
- Comply with the Information Security Procedures.

Responsibilities of the Business Information Security Officer (BISO)

The responsibility for carrying out the departmental Information Security activities shall rest with the Business Information Security Officers (BISO) that will reside within each department across the quant and shall coordinate closely with the ISD for all IS activities. The areas of responsibilities of BISOs have been classified into the following functions:

- Implementing policies and perform regular monitoring and review
- Assist ISU to provide Training and Awareness
- Assist ISU to conduct IS Risk Assessment exercise
- Active involvement in Incident reporting and further investigation
- Coordination in internal, external and regulatory audits
- Assist ISU in conducting IS reviews as and when required
- Undertake logs review of user activities of applications / systems where applicable

- Conduct reviews as defined in IS Policy

Responsibilities of End-Users

Each user of Quant's computing and information resources shall realize the fundamental importance of information resources and recognize their responsibility for safekeeping of those resources. Users must guard against abuses that disrupt or threaten the viability of all systems. The following are specific responsibilities of all Quant's information system users:

- Understand what the consequences of their actions are with regard to computing security practices and act accordingly.
- Maintain awareness of the contents of the Information Security Policy.
- Notify the BISO and / or the relevant Department Head of any breach of control, cyber incident or any information (confidential or sensitive) received unclassified. Limit the distribution of this information accordingly.

3 Information Security Implementation Roadmap

The Plan-Do-Check-Act (PDCA) Cycle

Plan

Leadership and Commitment

QUANT Top management (comprising the Senior Management, CRO and GH) will demonstrate leadership and commitment with respect to QUANT IS Management by:

- Ensuring through the ISD that the Information Security objectives and the Information Security Policies are established;
- Establish the IS Management Organizational Structure and ensuring that the resources required for IS Management are appropriately allocated and deployed;
- Communicating the importance of effective Information Security management and conforming to the IS Management requirements; and
- Promoting continual improvement.

Actions to Address Risks and Improvement Opportunities

As part of planning for the IS Management, QUANT will determine and consider the risks and opportunities that need to be addressed to:

- Ensure that the ISD can achieve its intended outcome;
- Prevent, or reduce, undesired effects; and
- Achieve continual improvement.

Relevant Documents / Tools

Document / Tool	Document Owner
Procedure for Information Security Risk Management	Information Security Dept.

Information Security Risk Treatment

QUANT will ensure the implementation of the Risk Treatment Plan based on the IS Risk Assessment results and the appropriate selection of controls by assigning the adequate financial, human and business resources and defining relevant roles and responsibilities. As part of the Risk Treatment Plan, QUANT will:

- Select appropriate Information Security risk treatment options (acceptance / mitigate / avoid / transfer), taking into account the IS Risk Assessment results;
- Determine the necessary controls to implement the Information Security risk treatment option(s) chosen;
- Obtain due approvals from the Information Asset Owners and the acceptance of the residual Information Security risks; and
- Retain appropriate documentation about the Information Security Risk Treatment process.

Relevant Documents / Tools

Document / Tool	Document Owner
Procedure for Information Security Risk Management	ISD
Risk Register	ISD

Information Security Objective Setting

QUANT will establish its Information Security objectives after taking into account applicable Information Security requirements, and results from IS Risk Assessment and risk treatment;

The Information Security objectives that are set will:

- Be consistent with the QUANT Information Security Policy;
- Be communicated; and
- Be updated as appropriate.

Do

Operational Planning and Control

QUANT will plan, implement and control the operational processes needed to meet its Information Security requirements and implement the actions needed to address its Information Security risks and opportunities. This shall be applicable to outsourced processes too. All the relevant operational processes will be documented and maintained to the extent necessary to provide confidence that the processes have been carried out as planned.

All planned changes will be controlled and relevant actions to mitigate any adverse effects will be taken, as necessary.

Relevant Documents / Tools

Document / Tool	Document Owner
Information Asset Management Guidelines	ISD
Access Management Guidelines	ISD
Cryptography Standards	ISD
Procedure for Information Security Risk Management	ISD
Risk Register	ISD
Information Security Incident Management Procedure	ISD
Information Asset Management Guidelines - Clear Desk Procedure	ISD
Information Asset Management Guidelines - Clear Screen Procedure	ISD

Document / Tool	Document Owner
Information Asset Management Guidelines - Acceptable Use of Information Assets	ISD
Safety and Security Manual	Administration Department
Access Management Procedure	SSAU
Access Management Procedure	IT
Change Management Procedure	IT
Policy and SOPs for Record Retention	Operations Department

Information Security Risk Assessment

ISD in consultation with the concerned entities will conduct Information Security Risk Assessment considering the following areas; alongside the requirements of the Quant's IS Policy:

- Internet Banking
- IT Infrastructure including but not limited to: applications, operating systems, databases, network appliances, etc.
- Cyber Security Controls

The ISD will review the Information Security Risk Assessment results on annual basis and identify any new risks to continually assess the risks based on the changes to the Quant in terms of the environment, technology, people, external or natural events, identified threats, implemented controls effectiveness assessment and business objectives and processes. All identified changes will be reflected in the relevant documentations such as IS Risk Assessment / Corrective Action Reports and Risk Treatment Plan.

Relevant Documents / Tools

Document / Tool	Document Owner
Risk Register	ISD
IS Risk Assessment (Corrective Action) Report	ISD

Information Security Risk Treatment

Concerned QUANT entities along with ISD will implement an Information Security Risk Treatment Plan after taking into consideration the outcome of IS Risk Assessment. Only the risk that requires treatment will be identified and followed upon for closure. The risk treatment and the results of follow-up will be adequately archived and maintained.

Relevant Documents / Tools

Document / Tool	Document Owner
Risk Register ISD	

Check

Monitoring, Measurement, Analysis and Evaluation

QUANT Information Security will define KPIs to measure Information Security controls' status across QUANT and contribute to improve Information Security understanding, planning and communication between different stakeholders.

Moreover, hardening standards will be designed for various tiers of the Quant's Information Systems such as (Systems, Applications, Database, Domain, and Network) for baseline standards which, at minimum, should be accomplished.

Relevant Documents / Tools

Document / Tool	Document Owner
Information Security Hardening Standards	ISD

Management Review

The Risk Management Group (RMG) will ensure independent reviews after every three years on the adequacy and effectiveness of Quant's IS Management. The review will include assessing improvement opportunities that can be supplementary to the existing IS Management. The review will be based on the following:

- Internal or independent IS Risk Assessment results;
- Incident reports;
- Status of preventive and corrective actions;
- Changes in regulatory or legal requirements; and
- Follow up actions from previous independent reviews.

The significant IS Management activities will be updated at different forums like ITSC, CRCC, BITC,

BRC, etc. to ensure that Information Security activities and strategy remains aligned with Quant's overall objectives and IS Policy.

Relevant Documents / Tools

Document / Tool	Document Owner
Incident Management Procedure - Corrective and Preventive Action	ISD
IS Risk Assessment (Corrective Action) Report	ISD

Act

Non-Conformity and Corrective Actions

All the identified actions and improvements that need to be performed will be reflected in relevant documentations. Corrective / Preventive actions will be conducted in accordance with the "IS Corrective and Preventive Action Procedure" of the ISD which requires the following steps to be performed:

- Identify non-conformities and potential non-conformities;
- Determine the causes of non-conformities;
- Evaluate the need for actions to ensure that non-conformities do not occur or recur;
- Country Risk and Compliance Committee (CRCC) Reviews;
- Implement and record the action taken; and
- Review the action taken.

Moreover, the protection measures for the Quant's Information Systems at various tiers such as (Systems, Applications, Database, Domain, and Network) will be ensured by means of implementing the respective hardening standards.

Relevant Documents / Tools

Document / Tool	Document Owner
Incident Management Procedure - Corrective and Preventive Action	ISD
IS Risk Assessment (Corrective Action) Report	ISD

In addition, training sessions will be organized to ensure the correct execution of major changes implemented in-line with Quant's Information Security Policy. Moreover, the effectiveness of the implemented actions / improvements will be reviewed through regular IS Risk Assessments, internal audits and management reviews with the aim to achieve the intended objectives.

Regulatory Compliance

In protecting QUANT Information and Information Assets, the PDCA approach described in Section 3 alongside standard (Information Security) requirements should also cover certain regulatory components specific to the security of Internet quanting and Cyber Security.

Security of Remote System Access

- Define a process for granting remote system access to the end users.
- Implement Two-factor authentication.
- Implement additional layer security critical activities carried out remotely
- Implementation of a Strong Password Standard to authenticate users
- Prepare an IS Risk Management Procedure to assess and mitigate risks.
- Implement the following controls on quant employees who access system remotely:
  - Access Rights Management
  - Operating Systems Controls
  - Remote Access
  - Physical Access
- Implement safeguards to monitor and secure Internet Quanting transactions.

Prevention against Cyber Attacks

- Identify and assess emerging threats and risks on a continual basis covering the following components; in accordance with the Quant's IS Risk Management Procedure:
  - Risk Ownership and Management Responsibility
  - Periodic evaluation and monitoring of cyber security controls
  - Regular independent assessments and tests
  - Industry collaboration and contingency plan
- A Summary Report on major security incidents (threats and attacks) to be shared with the Board.
- An organizational action plan for Cyber Security to be reviewed and updated on annual basis.

Information / Cyber Security Activities

Following activities will be performed in line with the QUANT IS Policy.

Sr #	Activity Title	Responsibility	Dependency
1	Perform IS Risk Assessment: Risk Identification	ISD**	IT Department / Relevant Business Units
2	Perform IS Risk Assessment: Risk Evaluation	ISD**	IT Department / Relevant Business Units
3	Perform Vulnerability Assessment	Vendor/ISD***	IT
4	Perform Penetration Testing	Vendor/ISD***	IT
5	Review Information Systems' Hardening	ISD*	IT
6	Perform Information Security Reviews as per IS Action Plan	ISD*	IT
7	Execute ISRP	ISD*	IT
8	Awareness / Training Sessions	ISD	None
9	Business Continuity Management Exercise / Drill	ISD**	IT and Admin

* Activities to be performed in collaboration with IT Department

** Activities to be performed in collaboration with the concerned / relevant departments

*** Depends on feasibility of carrying out the exercise in-house through procured software or via third party vendor without procuring related software

Support

Resources

QUANT will determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of QUANT IS Management Function.

Relevant Documents / Tools

Document / Tool	Document Owner
QUANT ISD program	ISD - RMG
Information / Cyber Security Organizational Structure	RMG

Currently, QUANT is equipped with the following tools / safeguards to meet Information / Cyber Security requirements:

Tool / Safeguards	Vendor
Security Information and Event Management (SIEM)	Manage Engine Log 360 Application

Intrusion Detection & Prevention System	Sophos XGS 2100 Firewall
Firewall	Sophos XGS 2100
Vulnerability Assessment and Penetration Testing Services	ProTechmanize Solutions Pvt. Ltd
Guardian for Database Security	quant Group
Antivirus (Security Center)	Sophos Endpoint Antivirus
Data Leakage Prevention Module	
Network / Server Monitoring Tool	
Encryption	

Competence

QUANT will determine the competence of the resources necessary to perform the job that affects Quant's Information Security performance. Relevant trainings will be provided to the resources to maintain their competencies.

Awareness

QUANT will roll out mandatory Information Security training and awareness sessions to ensure that all employees are made aware of QUANT Information Security requirements, risks and their roles and responsibilities.

Users will be appropriately communicated regarding policies, procedures and guidelines, based on the roles and responsibilities towards QUANT Information Security. The awareness and communication will be made through security awareness training sessions, tailored messages, and e-bulletins.

Information security awareness and training programs will be designed to help personnel to:

- Become familiar with their roles and responsibilities;
- Under the Information Security risks and the measures to mitigate those risks;
- Help understand and support security requirements;
- Help learn about, how to fulfill their security responsibilities; and
- Foster an effective security culture and sound decision-making practices.
- Familiarize customers with the risks and frauds associated with Payment Cards, New Payment Methods, Internet Banking and Mobile Banking.
- Explain liabilities, roles and responsibilities for using payment cards and Internet/Mobile Quanting Products

Relevant Documents / Tools

Document / Tool	Document Owner
Security Awareness programs for Employees & Customers	ISD

Documented Information

Documented information will be controlled in accordance with the relevant procedures listed underneath to ensure the alignment of the Information Security documentation with the QUANT documented information requirements.

All the records that provide evidence of conformity to Information Security requirements and the effective operation of QUANT IS Management Function will be maintained, protected and controlled. The management of these records will include its retention after due considerations of the legal, regulatory and contractual obligations.

Relevant Documents / Tools

Document / Tool	Document Owner
Control of Documents Procedure	ISD
Policy and SOP for Record Retention	Operations Department

Reporting

- The IS related significant matters will be reported in RCC.
- Security breaches / Incident and Analysis Reports for security breaches will be reported to compliance which in turn will report tot SEBI
- The IS Risk Assessment Results will be shared with the concerned Group Heads.