Security & Technology Risk Management

Overview

A BANK TO TRUST

Security & Technology Risk Management

Security & Technology Risk Definitions

- **Technology Risk:** **The business risks that may arise due to the potential of technology failures, or disruptions associated with the use, ownership, operation, evolution and adoption of internally developed or Third-party acquired Information Technology and Information Systems that support the business functions and provided services within the Bank.**

- **Security Risk:** **The business risk that may arise due to the potential unauthorized access, use, disclosure, modification or destruction of the Bank's information and information systems that will affect the information's confidentiality, integrity and availability.**

Information Security	Cyber Security	IT & Security Third-party
IT Project Execution	IT Resilience & Continuity	Security & Technology Controls' Assurance

Security & Technology Risk Management

III Lines of Defense

The III LOD Model provides for the basis of formalizing and institutionalizing risk management awareness and accountability. It ensures [illegible] standardized approach to risk assessments, risk scoring, reporting metrics and governance.

Security & Technology Risk Management

III Lines of Defense || Key Transformations

The III LOD Model provides for the basis of formalizing and institutionalizing risk management awareness and accountability. It ensures [illegible] standardized approach to risk assessments, risk scoring, reporting metrics and governance.

1st Line of Defense

- Risk Identification & Analysis
- Controls Implementation & Monitoring
- Security & Technology Operations
- Security & Technology Integration
- Security & Technology Architecture & Design
- Security Hardening
- Business Resiliency & Disaster Recovery
- Training & Awareness
- Operational Governance
- Compliance / Control Checks

2nd Line of Defense

Risk Management
- Risk Assessment Framework
- Risk Management Process
- Asset & Threat Landscaping
- Risk Assessments / Evaluations

Assurance Management
- Compliance & Controls Framework
- Controls Assurance & Compliance Management
- Policy Alignment

Governance & Reporting
- Operational Governance
- Strategic Governance

3rd Line of Defense

- Internal and/or External Compliance Audits
- Performance Audits & Reviews
- Corrective Action Plans for Gaps Closure

2nd Line of Defense (CRO Organization)

Risk Management Functions

- Risk Management
- Risk Identification
- Risk Advisory
- Risk Management Documentation
- Independent Risk Assessments

Assurance Functions

- Compliance Framework
- Internal Compliance Assessment
- Baseline Doc & Policy Reviews

Risk Governance & Reporting Functions

- Operational Governance
  - CSO
  - IT
  - Third Parties
- Strategic Governance
  - Board
  - External Orgs
  - Internal Audit

Security & Technology Risk Management

Scope

Security & Technology Risk Management – 2nd Line of Defense

Acts as an independent second line of defense within the Risk Group organization, the Security & Technology Risk Management is responsible for managing the following bank-wide risks:

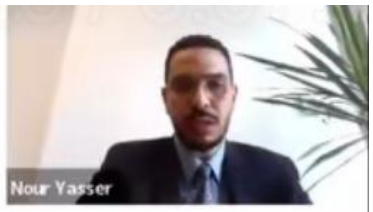
- Information Security Risk, Cyber Security Risk, IT & Security Third-party Risk, IT Resilience & Continuity Risk, IT Project Execution Risk, and Security & Technology Controls' Assurance Risk.
- Risks of non-Compliance with relevant CBE regulations and industry standards.

The STRM is responsible for defining and implementing the Security & Technology Risk Management framework to support mitigating Security & Technology Risks, in order to:

- Minimize and mitigate potential and unexpected losses
- Improve Control environment effectiveness within the bank
- Align business operations and risk exposure to appropriate levels
- Ensure alignment with risk management requirements that have been mandated by relevant legal and regulatory bodies
- Track, report & monitor Security & Technology risks along with their risk assessment and treatment plans.

Security & Technology Risk Management

Approved Structure



Security & Technology Risk Management

1. **Risk Assessment Framework**
2. **Risk Management Process**
3. **Risk Assessments / Evaluations**

Security & Technology Assurance Management

1. **Compliance Requirement Management**
2. **Compliance & Control Frameworks**
3. **Policy Alignment**

Security & Technology Governance & Reporting

1. **Operational Governance**
2. **Strategic Governance**

Security & Technology Risk Management

Scope

The main scope of the Security & Technology Risk Management is to ensure an effective risk management process is being followed in alignment with the ERM framework.

❖ **Pro-active Risk Assessment**

❑ ***1st Line of Defense Reporting of Identified Risks***

Risks are initially assessed by the risk owner and reported to the Security & Technology Risk Management team:

- RCSA Exercise
- Vulnerability Management Program & Different Security Assessments
- Secure Software Development / Acquisition Life Cycle
- Change Management & Project Execution Processes
- Others

❑ ***Risk Assessment of Security & Technology Corpus & Documentation***

Review and concur all documentation produced from the Security & Resilience Management or Information Technology Management areas, to address any key control gaps identified and highlight any bank-wide security or technology risks for effective risk management.

❑ ***Independent Risk & Assurance Assessment***

Based on the current threat landscape, defined priorities and risk appetite, the Security & Technology Risk Management team might perform on-demand / ad-hoc independent risk & assurance assessments for a defined scope of services / information systems, to proactively identify security and technology risks.

Security & Technology Risk Management

Scope

❖ **Reactive Risk Assessment**

❑ ***Risk Assessment of Identified Security & Technology Audit Gaps***

To ensure identified security or technology audit gaps are assessed as well from risk perspective

- Identification of new bank-wide Security or Technology Risks as a result of ineffective / missing controls
- Re-assessment of associated security & technology risks, as a result of ineffective / missing controls

❑ ***Risk Assessment of Key Security & Technology Incidents***

To ensure key / major security or technology incidents are assessed as well from risk perspective

- Incident root cause has been identified with an appropriate resolution action in place to avoid incident re-occurrence.
- Identification of new bank-wide Security or Technology Risks as a result of ineffective / missing controls that could have led to such incidents.
- Re-assessment of associated security & technology risks, as a result of ineffective / missing controls that could have led to such incidents.

❑ ***Evaluation of Risk Response Effectiveness***

Different KRIs and RAIs are developed and reported to act as early warning signals to monitor the risks' status and set the effectiveness criteria for the identified risk response associated with the key security & technology risks.

Security & Technology Risk Management

Process

Security & Technology Risk Management Process

The process for managing Security & Technology risks ensures risks are continuously identified, assessed in terms of their impact on the business and likelihood of occurrence, appropriate risk treatment plans are in place, aligned with the bank's risk appetite and defined priorities, the relevant stakeholders are involved and are kept informed with the ongoing monitoring of the risk treatment effectiveness.

Security & Technology Risk Management

Governance Model

Security & Technology Risks Governance & Reporting

Operational and strategic governance of security & technology risks provide regular monitoring and assessment to the organizational risks' exposure and status.

Risk dashboards & reports are frequently generated to ensure governance at two levels Operational and Strategic. Operational governance with 1st LoD functions to collect needed KRIs, RAIs and needed escalations in Security & Technology Risk Committee (STRC). Strategic governance with 3rd line of defense, Risk & Audit Committees to report on Risk posture, key exceptions, and arbitrations.