IBM Security

# Information Security Management Models

NEW APPROACHES FOR EFFECTIVE AND EFFICIENT SECURITY MANAGMENT

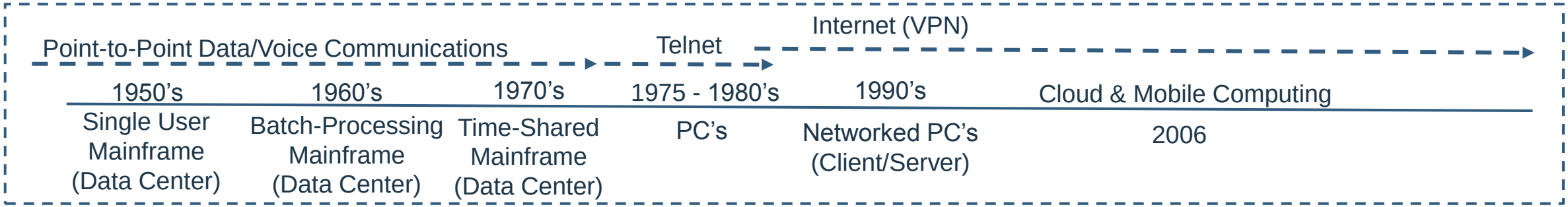
**Rob Dyson**
Partner, IBM Security Services

June 2016

IBM

# Companies are transforming the way they manage information and IT risks

- Information security was traditionally only an IT problem and organizations relied on the information technology department personnel for security.
- The introduction of cloud, social, and mobile business solutions are introducing new business threats and risks forcing a higher priority on Information Security roles and responsibilities.
- Financial Services organizations are investing aggressively to transform their Information Security operations.
- All leading Financial Services companies are dedicating an Executive to manage IT risk (physical and technical) for the entire company and related 3rd parties.

# Security Management Transformation Drivers

- Clear understanding of security accountabilities and responsibilities
- Executive level leadership from person that has skills and experience in IT Risk Management
- Segregation of Duties
  - Separate the responsibility for managing risk from building and running the business
- Security Program alignment with Business & IT Objectives and Priorities
- Avoids isolated risk decision making
  - Reduce or eliminate an individual making a risk decision that impacts the company, employees, customers, business partners, etc.

# CISO roles and responsibilities span across the organization and require multi-discipline skills


**These roles and responsibilities can be grouped into five themes**

| Leadership & Oversight | Risk & Compliance | Business engagement | Technology enablement | Delivery & Operations |
|---|---|---|---|---|
| Act as the senior security leader to own the strategy and be accountable for its delivery to the Board | Set policies and targets that align with the business security risk tolerance and measure their effectiveness | Enable the business to operate within the defined security risk tolerances | Help invest in advanced technology to increase security posture | Oversee secure business and IT operations |

*Leadership skills are paramount as security and technical skills wane in importance**

*Source: Evolve To Become The 2018 CISO Or Face Extinction, Forrester, 2014

# It is imperative to define security roles and responsibilities in a documented and approved RACI[1] model

- RACI models clearly delineate the roles of who approves a decision and who is responsible for the process behind the decision.
- Accurate RACI models are critical for international organizations
- The development and approval of a RACI is a critical step in the journey to mature the Security Function.
- Leverage a 3rd party security service provider to facilitate and accelerate the RACI development process.

EXAMPLE

| PROCESS | Board of Directors (BOD) | CEO | CIO (ATEC) | CRO (ACR) | CSO (DSC) | Internal Controls & Compliance (DCIC) | Business Unit Leaders | Legal Department | Internal Audit | IT Department Leaders | Manager Security Governance (SPS) | Manager Security Operations (SSI) | Security Architects | SOC Manager |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **ESTABLISH** | | | | | | | | | | | | | | |
| Establish Security Strategy and Objectives | C | A | C | R | R | I | C | C | I | C | I | I | I | I |
| Establish Information Security Risk Boundaries and Tolerances | C | A | C | R | R | I | C | C | I | I | I | I | I | I |
| Establish the Information Security Culture | C | A | C | C | R | C | R | C | I | C | I | R | I | I |
| Establish criteria to evaluate risk | I | I | C | A | R | R | C | C | I | C | C | C | C | C |
| Identify critical business assests, threats, risks, potential vulnerabilities and impacts. | I | I | I | A | R | R | C | C | I | C | I | I | I | I |
| Indentify options for the treatment of risks | | | C | A | R | R | C | C | I | C | R | R | R | I |
| Establish Responsibility & Ownership for Information Assets | | I | C | R | R | R | A | C | I | C | C | I | I | I |
| Identify and Confirm Information Security Compliance requirements | | I | C | A | R | R | C | R | C | C | C | I | I | I |
| Develop information security policies to support confidentiality, integrity, availability, and accountability | I | I | C | A | R | C | C | C | I | C | R | C | C | C |
| Develop information security standards and guidelines to support confidentiality, integrity, availability, and | | | C | C | A | C | I | C | I | I | R | I | C | I |

[1]RACI (Responsible, Accountable, Consulted, Informed)

# There are three conceptual models for shaping the security organization – Functional, Divisional and Matrix

### *Functional Models*

Functional purpose of each organizational unit (e.g. IT, marketing, sales) are the basis to create functional units

Typically results in a centralized and hierarchical organization models

Suitable for small or homogeneous organizations, or those with little geographical footprint

### *Divisional Models*

Product Lines, Markets, Geography, etc. are the basis to create organizational divisions

Typically results in a federated and hierarchical organization models

Suitable for organizations with wide geographical coverage, disparate product sets or markets

Also suitable following mergers and acquisitions

### *Matrix Models*

Uses a combination of Functional and Divisional models

Typically results in a federated and flat organization models with multiple reporting lines between roles

Suitable for organizations with functions spanning across the organization or shared between divisions

# Functional models are traditional and place the responsibility for security operations within the IT organisation

Security organizations based on a functional model split IT Security and Information Security Governance responsibilities. Cyber security operational responsibilities are within the IT Function

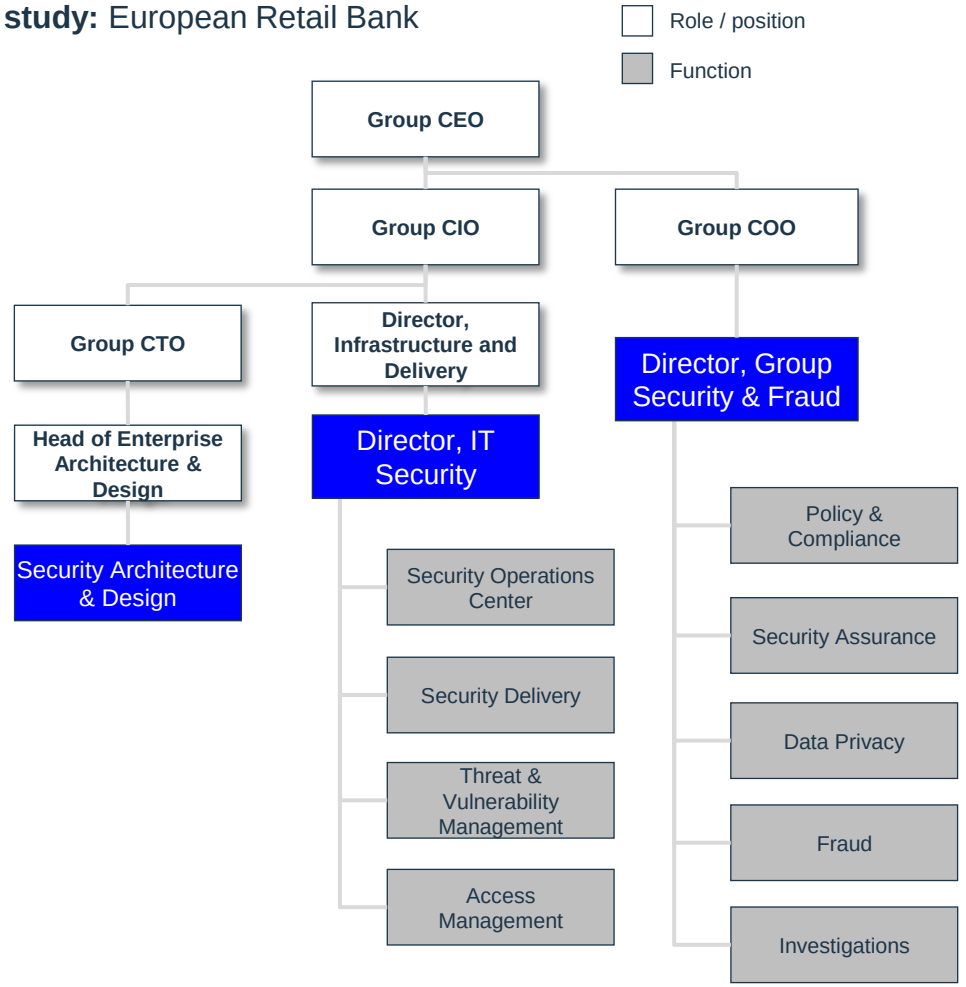
## Pros

- Clear roles and responsibilities for security
- Clear separation of duties between policy definition (governance) and delivery
- IT organization has clear accountability for meeting regulatory security requirements

## Cons

- May result in silo mentality between IT and Business Risk Management
- The IT Security Governance functions are not the priority within the IT organization
- Establishes conflict of interest risk within CIO organization; CIO may make risk decisions independently

**Case study:** European Retail Bank



# Divisional models are suited for organizations with disparate needs across different regions

Security organizations based on a region-based divisional model splits security responsibilities by region. Each region my operate independently with some governance provided from the Group.

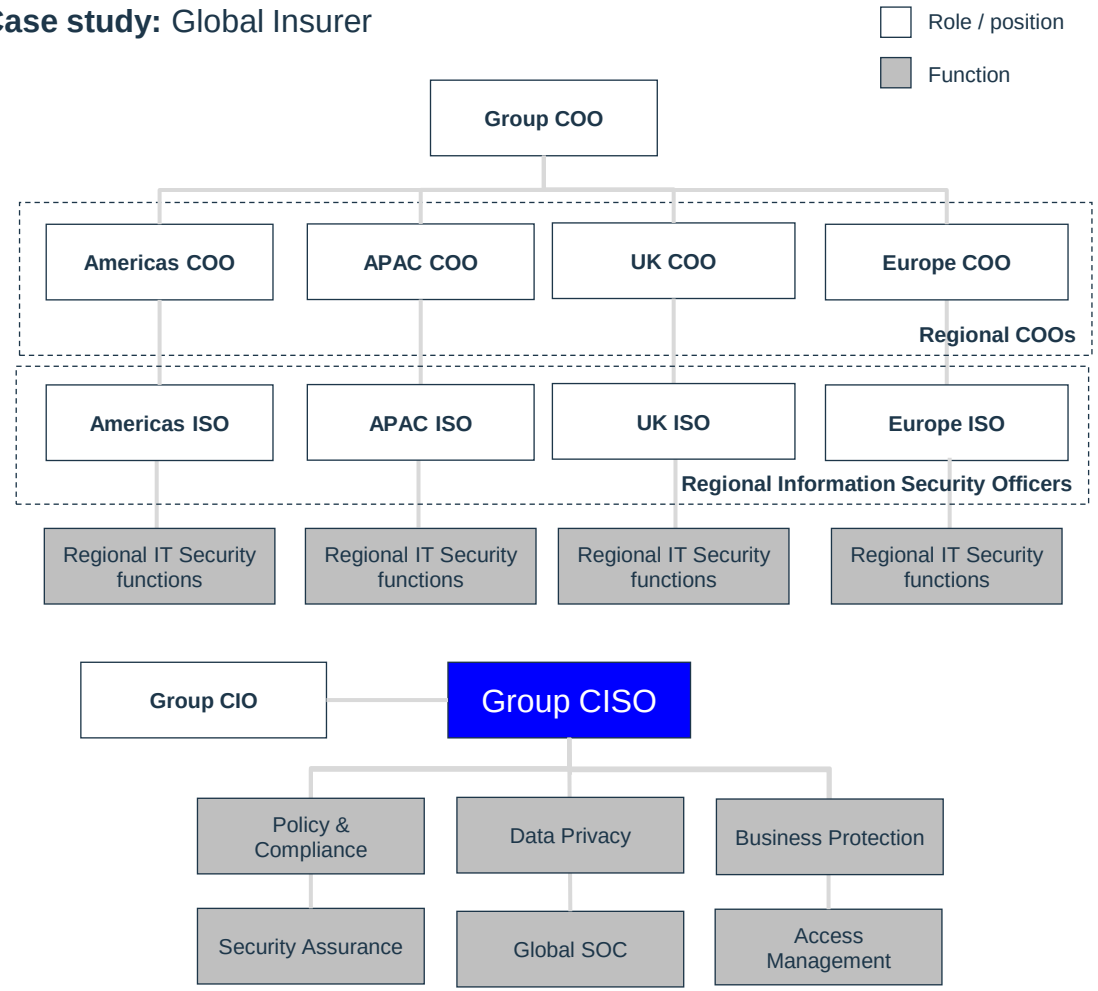
**Pros**

- Tailored approach for each region, e.g. accounting for different regulations
- Local leadership supported by global oversight

**Cons**

- Inconsistent implementation of security
- Potential conflict between the Group and Regions because the Region is held Accountable for security
- Difficult to implement cross-regional capability, e.g. Global SOC
- Establishes conflict of interest risk within CIO organization; CIO may make risk decisions independently

**Case study:** Global Insurer



# Matrix models may enable better alignment with functions but can be complex to govern

Security organizations based on a matrix model operates virtual security teams, which are fragmented across the organization in specialised areas (e.g. Architecture).

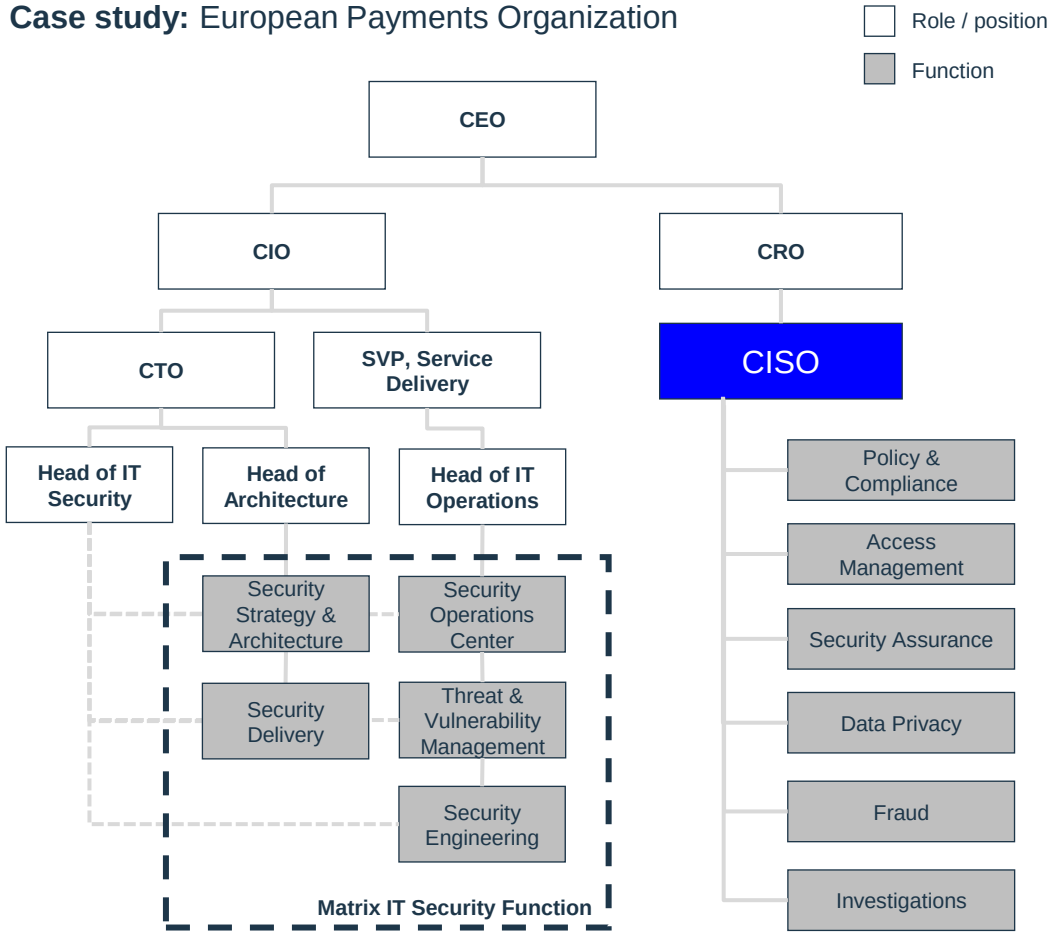
**Pros**

- Specialized security teams (e.g. Security Architecture) benefit from working closely with other teams
- Can be more flexible in bringing together different skills across the organization

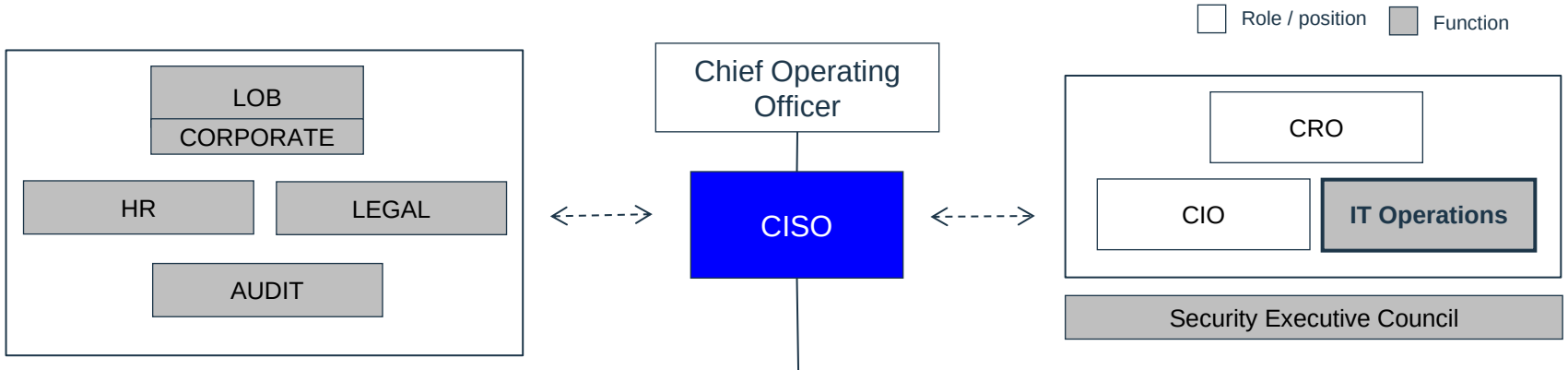
**Cons**

- Complex governance model
- Less clear roles and responsibilities
- Less clear accountability
- Establishes conflict of interest risk within CIO organization; CIO may make risk decisions independently

**Case study:** European Payments Organization

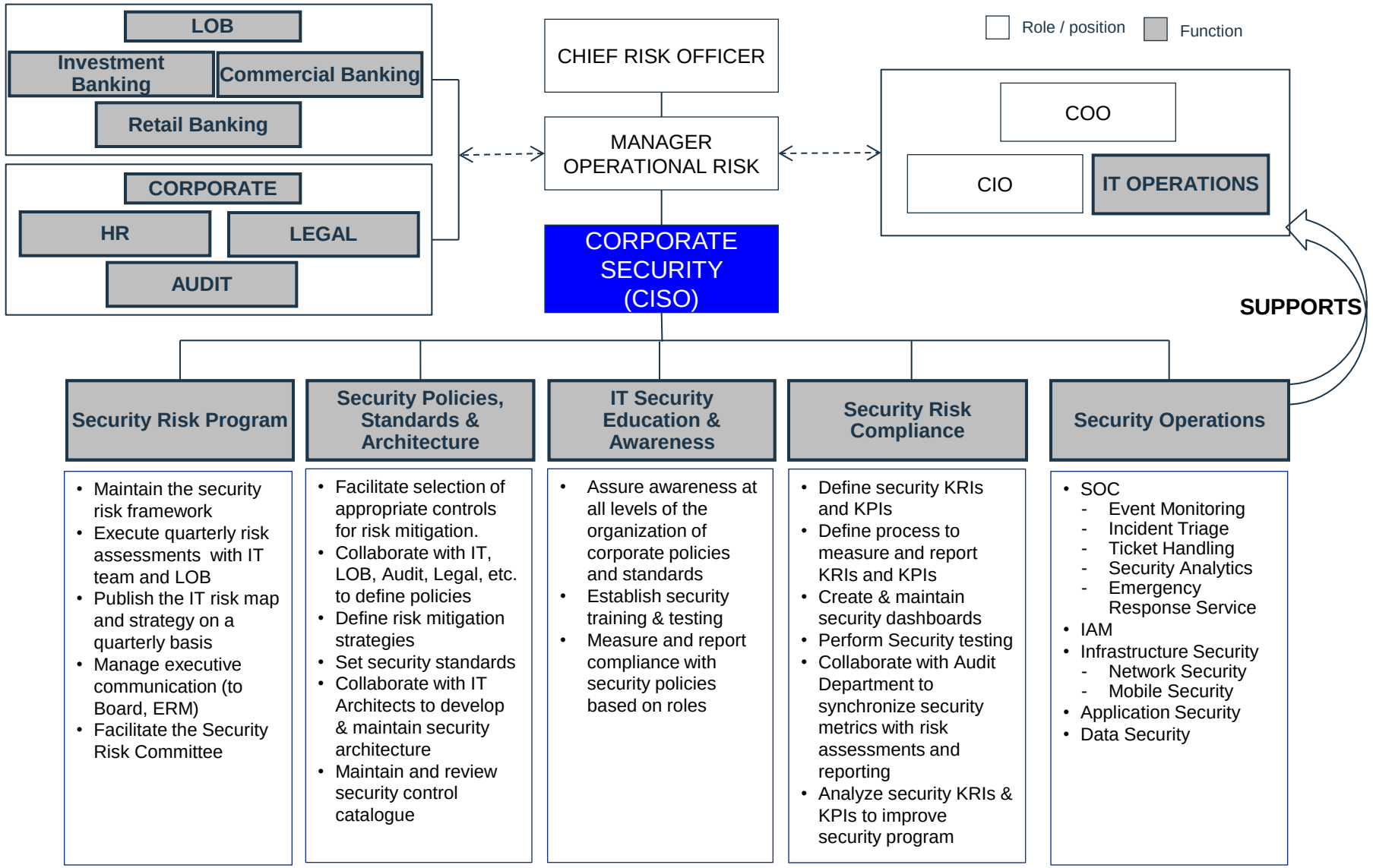


# Reference model – A business-focused CISO supported by a functional organization




| Security Strategy & Risk Oversight | Security Policies & Standards | Security Education & Awareness | Security Risk & Compliance | Security Operations |
|---|---|---|---|---|
| • Maintain the security strategy and risk framework<br>• Execute quarterly risk assessments with IT team and LOB<br>• Manage internal and external executive communication (to Board, ERM, Regulators)<br>• Chair the Cyber Security Committee<br>• Work with external peers on threats affecting the industry and joint response | • Facilitate selection of appropriate controls for risk mitigation<br>• Collaborate with IT, LOB, Audit, Legal, etc. to define policies<br>• Define risk mitigation strategies<br>• Set high level security standards to help drive security architecture and IT security standards<br>• Maintain and review security control catalogue | • Assure awareness at all levels of the organization of corporate policies and standards<br>• Establish security training & testing<br>• Measure and report compliance with security policies based on roles | • Define security KRIs and KPIs<br>• Define process to measure and report KRIs and KPIs<br>• Perform regular and ad hoc security testing<br>• Collaborate with Audit Department to synchronize security metrics with risk assessments and reporting<br>• Analyze security KRIs & KPIs to improve security program | • Security Operations and Intelligence Center<br>- Event Monitoring<br>- Incident Triage<br>- Ticket Handling<br>- Security Analytics<br>- Emergency Response Service<br>• IAM<br>• Infrastructure Security<br>- Network Security<br>- Mobile Security<br>• Application Security<br>• Data Security |

# Example Business Risk Management Organizational Model where security is clearly an element of the company's operational risk program



IBM Security

# THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions



Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM