December 2018

Effective Cyber Risk Management & Trends in Cyber Risk Quantification

SIFMA IAS Seminar | December 3, 2018 | New York

pwc

www.pwc.com
Strictly private and confidential

Agenda

Introductions	*Mike Hodges*
The Fundamentals: *PwC's Cyber Risk Management Program*	*Eric Lantz*
Emerging Capabilities: *Trends in Cyber Risk Quantification*	*Charlie Leonard*
Questions and Answers	*All*

The digital revolution is transforming industries without exception – and catching many off guard. Demand and competition are subject to radical and rapid changes.

In addition to changing company and market dynamics, the digital revolution also changes the concept of digital and technology risk.

Companies are being driven to change the way they manage risk

Increased role of Boards and the CEO in cyber risk oversight is driving demand for better methods to measure and articulate business and economic impacts of cyber risks

Cyber security breaches erode companies' share prices permanently and have resulted in **billions of dollars in market valuation being erased** since 2013[1] – as new regulations require better breach reporting financial markets will respond

Companies are becoming digital and current approaches to cyber risk management must **evolve from subjective, checklist and compliance driven methods to data-driven risk models**

Top Questions Boards and Executives are asking risk and cyber leadership:

1. What are our top cyber risks and how much exposure do they represent?
2. Where are we allocating resources and dollars? Are we investing too little or too much?
3. How effective are our investments in risk reduction (return on security investments)?

[1] CGI-Oxford Economics Study: Cyber-Value Connection

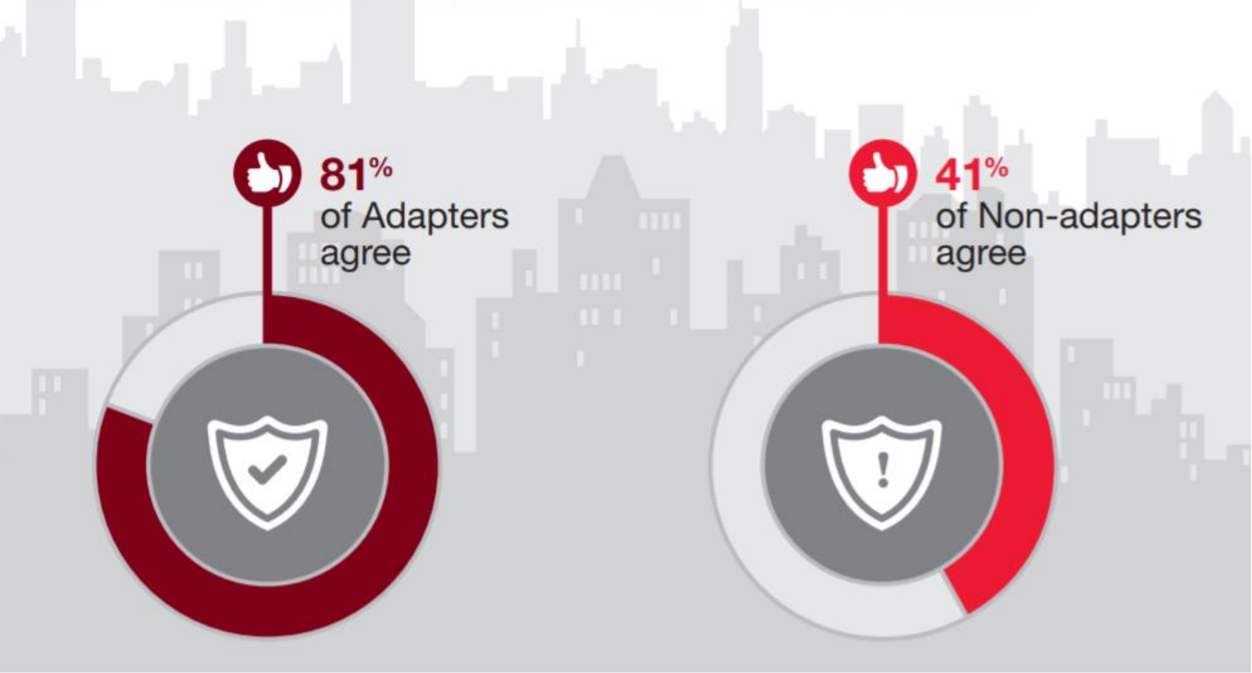
They are realizing benefits from leading the way in digital transformation

Executives who:

1. call their organizations more innovative than those of their peers, and
2. consider their risk management programs to be more effective

...are **three times more likely** than their less-effective and less-innovative peers to anticipate revenue growth

Figure 1: The risk management functions helps increase the odds of success



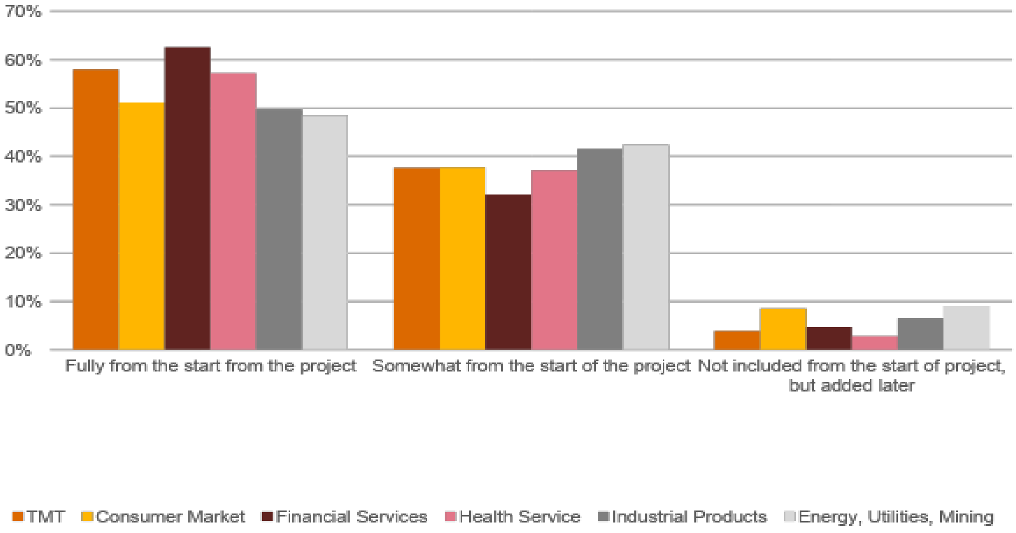
They are doing more to engage risk and security early in the transformation

91%

of enterprise-wide digital transformation include security and/or privacy personnel as stakeholders

53%

include proactive management of cyber and privacy risks by design in the project plan and budget "fully from the start"



q1060: Earlier you said that your company is currently involved in an enterprise-wide digital transformation project. To what extent is proactive management of cyber and privacy risks included by design in the project plan and budget?

These efforts present challenges and opportunities for auditors

Technical Prowess
How can IA attract and retain the right skills to provide an effective Third Line of Defense?

IA Program
How can IA find the right balance between scope, coverage, and frequency while minimizing "audit fatigue" in Operations due to continuous Risk Oversight?

Focus
How can IA balance the demands of expanding audit activities beyond 1st Line of Defense cyber risk control testing, maintain focus on the effectiveness of the overall cyber risk program, and challenge the 2nd Line of Defense?

Stakeholders
How can IA meet regulators' are expectations and audit committee demands for more effective cyber risk audits?

The Fundamentals

PwC's Cyber Risk Management Program

Organizations continue to struggle with common pitfalls

Pitfalls

Strategy

- Evolving cyber function from risk assessors to risk managers
- Applying risk management discipline to strategic cyber planning

Methods

- Modelling dependencies between threats, assets and capabilities
- Frameworks and/or compliance driven approach to evaluating risks and prioritizing investments

Reporting

- Articulating cyber and value connection in business friendly terms
- Meaningful metrics and actionable risk intelligence that answer the "so what" question and drive actions

Response

Elevate cyber function to be an enabler of Business Strategy using a robust, yet agile risk framework

Data driven risk management, leveraging threat-asset-capability relational data model and probabilistic Value at Risk techniques

Quantify risks into tangible metrics that can be used for informed decision making

Pain points in effectively managing and overseeing cyber risk

It is challenging to achieve ***a common understanding*** *of* ***cyber risk management*** *efforts that spans the* ***3 lines of defense***

No. 1

Cyber risk tolerance and risk appetite is not established or understood

No. 2

Security strategy does not align with business objectives or risk appetite

No. 3

Enterprise risk parlance is not used to articulate cyber risks

No. 4

The Board and Executive Leadership has limited visibility into impact of cyber risks

No. 5

Risk management “ownership” is not established

No. 6

Roles and responsibilities across the three lines are often ambiguous

No. 7

Controls are not designed to address risk but to manage compliance

No. 8

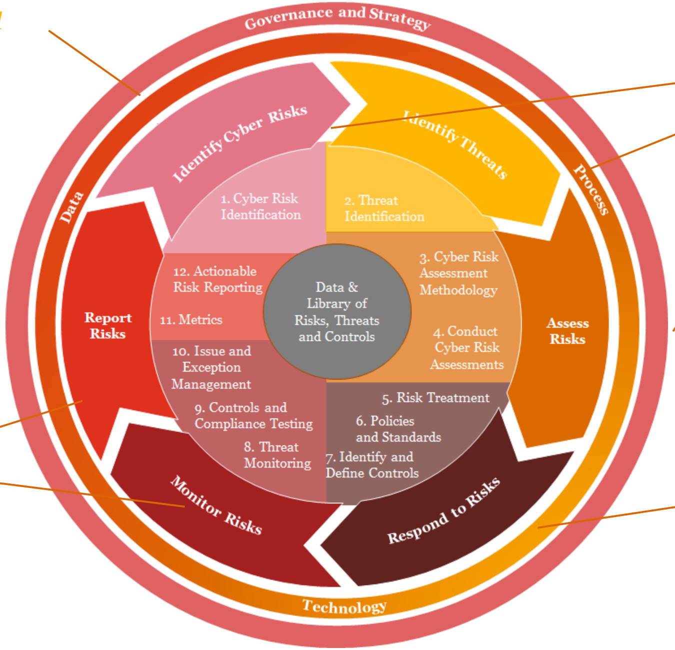
Audit fatigue due to proliferation of compliance requirements

PwC's Cyber Risk Management Program Components

Cyber Risk Governance, Strategy and Operating Model

The foundation of the Cyber Risk Management Program is defined and aligned to the enterprise risk appetite and strategy. Some of the key activities include:

- Defining the operating model
- Setting cyber risk appetite for the enterprise or lines of business
- Establishing risk committees
- Defining Cyber Risk Management policies & standards for second line of defense



Governance and Strategy
Data
Process
Technology
Identify Cyber Risks
Identify Threats
Assess Risks
Respond to Risks
Monitor Risks
Report Risks
1. Cyber Risk Identification
2. Threat Identification
3. Cyber Risk Assessment Methodology
4. Conduct Cyber Risk Assessments
5. Risk Treatment
6. Policies and Standards
7. Identify and Define Controls
8. Threat Monitoring
9. Controls and Compliance Testing
10. Issue and Exception Management
11. Metrics
12. Actionable Risk Reporting
Data & Library of Risks, Threats and Controls

Cyber Risk Identification and Assessment

Cyber risks and threats that could potentially impact the enterprise are identified, as well as the controls that are in place to mitigate them. Some of the key activities include:

- Risk identification and threat profiling
- Determining inherent risk, identifying and evaluating controls and residual risk estimation

Cyber Risk Monitoring and Reporting

A formal and repeatable process is established to monitor key performance indicators and report their evolution to the board of directors or appropriate risk committees. Some of the key activities include:

- Design a cyber risk dashboard and reporting platform
- Define second line of defense key performance indicators and establish a mapping to the enterprise key risk indicators

Cyber Risk Response

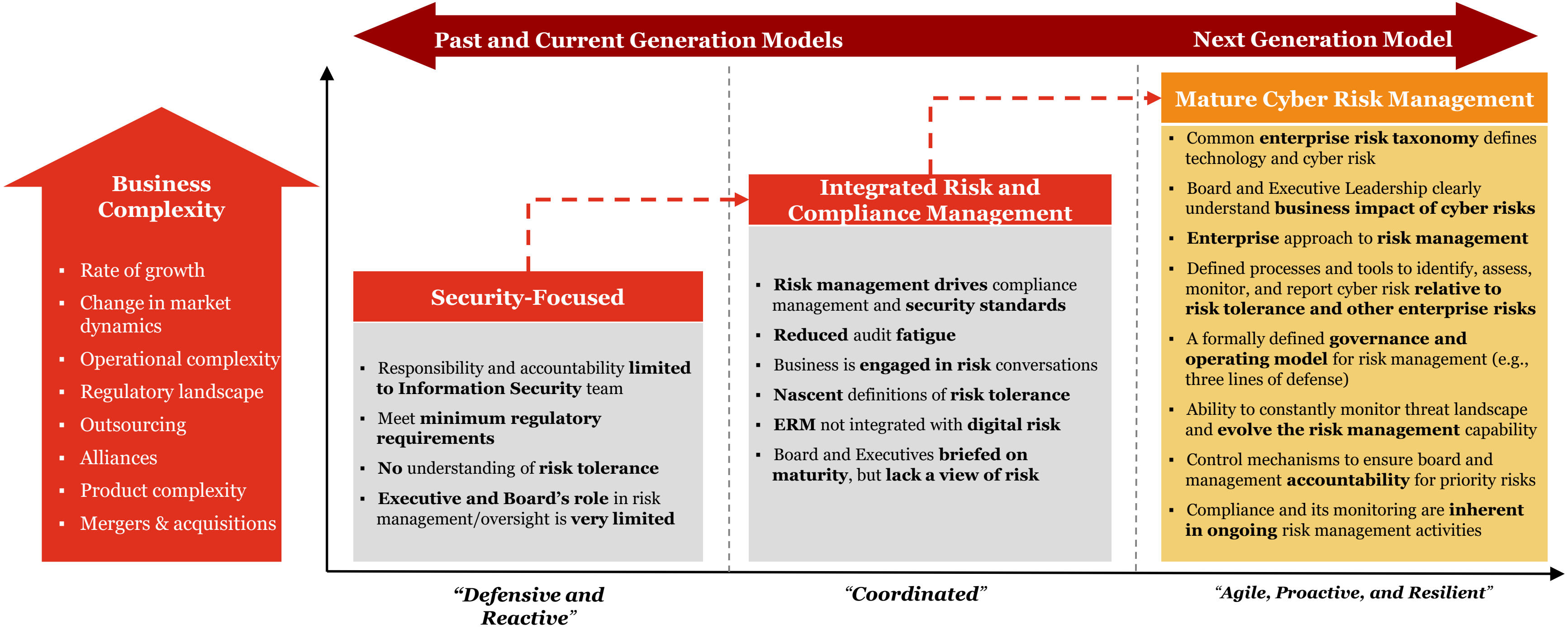
A plan is defined to treat risk and manage risk exposure. Some of the key activities include:

- Analyze risk appetite vs current risk exposure to determine the appropriate risk treatment decision (i.e. treat, terminate, transfer, tolerate)
- Identify mitigation actions and implement according to determined plan

Establishing an effective Cyber Risk Management Program enables organizations to consistently identify, assess, respond to, monitor, and report on existing and emerging cyber risks.

Evolving Approaches in Managing Cyber Risks

Beyond the financial services sector most organizations have limited enterprise risk management capabilities. Hence, Cyber Risk Management is still evolving from a traditional security-focused function to managing cyber risks with an enterprise risk lens.



Past and Current Generation Models

Next Generation Model

Business Complexity

- Rate of growth
- Change in market dynamics
- Operational complexity
- Regulatory landscape
- Outsourcing
- Alliances
- Product complexity
- Mergers & acquisitions

Security-Focused

- Responsibility and accountability **limited to Information Security** team
- Meet **minimum regulatory requirements**
- **No** understanding of **risk tolerance**
- **Executive and Board's role** in risk management/oversight is **very limited**

"Defensive and Reactive"

Integrated Risk and Compliance Management

- **Risk management drives** compliance management and **security standards**
- **Reduced** audit **fatigue**
- Business is **engaged in risk** conversations
- **Nascent** definitions of **risk tolerance**
- **ERM** not integrated with **digital risk**
- Board and Executives **briefed on maturity**, but **lack a view of risk**

"Coordinated"

Mature Cyber Risk Management

- Common **enterprise risk taxonomy** defines technology and cyber risk
- Board and Executive Leadership clearly understand **business impact of cyber risks**
- **Enterprise** approach to **risk management**
- Defined processes and tools to identify, assess, monitor, and report cyber risk **relative to risk tolerance and other enterprise risks**
- A formally defined **governance and operating model** for risk management (e.g., three lines of defense)
- Ability to constantly monitor threat landscape and **evolve the risk management** capability
- Control mechanisms to ensure board and management **accountability** for priority risks
- Compliance and its monitoring are **inherent in ongoing** risk management activities

"Agile, Proactive, and Resilient"

Cyber Risk Governance and Operating Models – Contrasts in Maturity

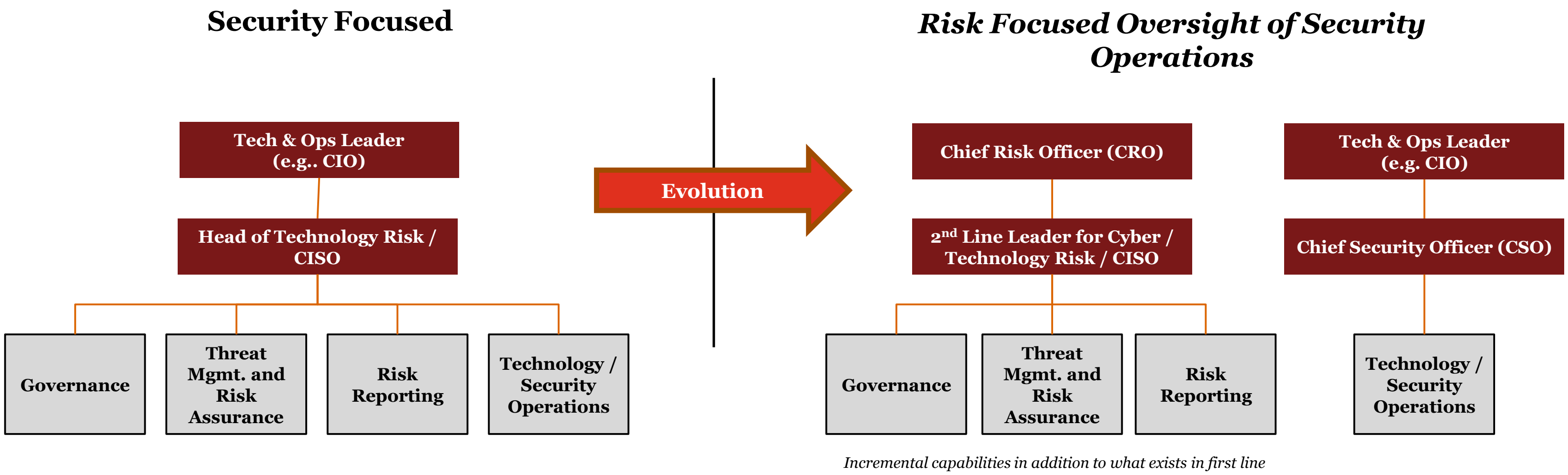
In heavily-regulated industries (e.g., Financial Services), allocating key functional attributes and responsibilities across three distinct lines of defense promotes transparency and accountability for cyber risk ownership, oversight, and assurance.

Board and Committee(s) Oversight

	1st Line of Defense CIO/CISO and Business Units	**2nd Line of Defense Independent Risk Management**	**3rd Line of Defense Internal Audit**
Mature Model in Heavily Regulated Industry	▪ Owns the risks ▪ Operates the controls ▪ Monitors risk, threats and controls on an ongoing basis	▪ Independently oversees risks ▪ Owns framework ▪ Sets policy ▪ Provides credible challenge ▪ Independently aggregates and reports on material cyber risks	• Independently tests controls • Evaluates program adherence by first **and** second lines of defense • Evaluate overall cyber risk management effectiveness
	1st Line of Defense CIO/CISO and Business Units	**2nd Line of Defense Independent Risk Management**	**3rd Line of Defense Internal Audit**
Less Mature Model in Less Regulated Industries	▪ Owns the risks ▪ Operates the controls ▪ Sets policy ▪ Monitors risk, threats and controls on an ongoing basis ▪ Reports on IS program		• Independently tests controls • Evaluates program adherence by first line of defense

Cyber Risk Operating Model – Structural Evolution in Financial Services

The traditional role and organizational positioning of Chief Information Security Officers (CISOs) is evolving, especially in regulated industries and more complex organizations, and may be determined or complemented by the establishment of a second line independent cyber risk function and officer independent from the Chief Information Officer (CIO) and the CISO. Most organizations are in the process of implementing a second line of defense for Cyber Risk Management:


Security Focused
Tech & Ops Leader (e.g.. CIO)
Head of Technology Risk / CISO
Governance
Threat Mgmt. and Risk Assurance
Risk Reporting
Technology / Security Operations
Evolution
Risk Focused Oversight of Security Operations
Chief Risk Officer (CRO)
2nd Line Leader for Cyber / Technology Risk / CISO
Tech & Ops Leader (e.g. CIO)
Chief Security Officer (CSO)
Governance
Threat Mgmt. and Risk Assurance
Risk Reporting
Technology / Security Operations

Incremental capabilities in addition to what exists in first line

PwC’s Cyber Risk Management Program - Benefits

Efficiency through improved ***focus on cyber*** *risks with* ***enterprise risk implication***

Enhanced ***awareness*** *by those ultimately accountable –* ***Board of Directors***

Clearer ***accountability*** *and roles and responsibilities between* ***risk ownership*** *and* ***risk oversight***

Preservation of profits *and market cap*

Increased *stakeholder and regulator* ***confidence****, and all that entails for* ***brand and reputation***

Value-added, actionable ***cyber risk intelligence*** *– Executive Management’s* ***decision making***

Independent, ***credible challenge*** *of operations by officers/functions* ***outside CIO’s span of control***

Emerging Capabilities

Trends in Cyber Risk Quantification

Companies are investing in technology that accelerates risk oversight

Successful risk management functions are investing in these areas for greater efficiency, visibility, and risk mitigation

1. Analytics, Visualization and Insights

Advanced analytics, modelling and quantification of cyber risks

Decision-oriented risk visualization tools

2. Data Fusion and Platform

Data lakes and integrated data model to tackle siloed data

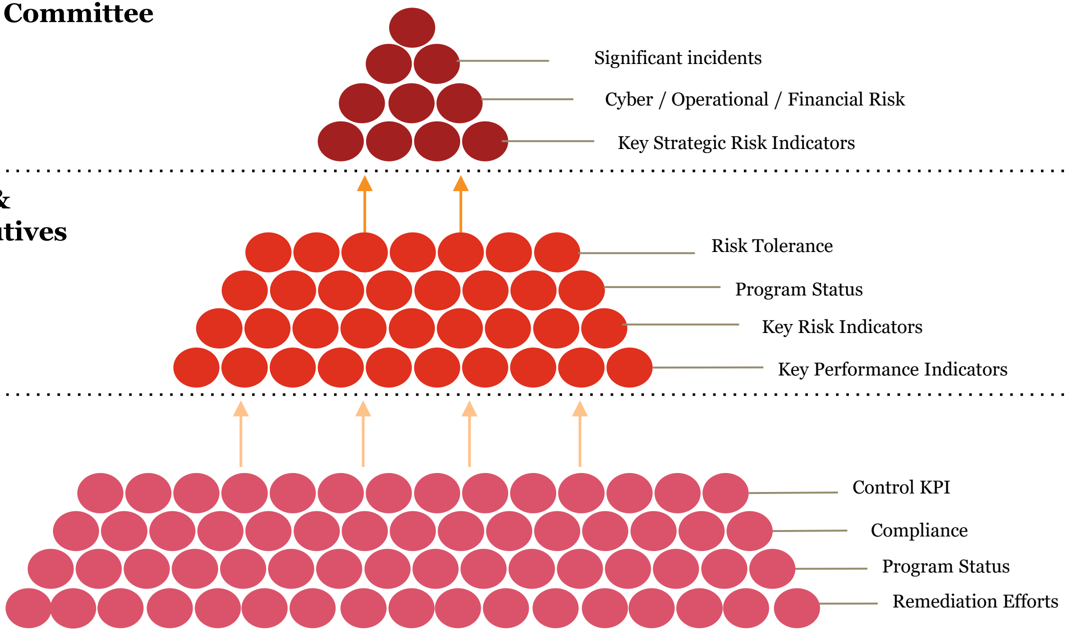
Applying artificial intelligence and machine learning to data sets

3. Data Sources and Processes

Integrating threat modelling, threat hunting and risk assessment capabilities

Orchestration / Automation of risk and compliance processes and controls

They are building an enterprise view of risk with aggregated metrics



Board & Executive Committee

Significant incidents

Cyber / Operational / Financial Risk

Key Strategic Risk Indicators

Cyber Risk Oversight

Lines of Business & Accountable Executives

Risk Tolerance

Program Status

Key Risk Indicators

Key Performance Indicators

Cyber Risk Ownership

Risk & Security Operations Teams

Control KPI

Compliance

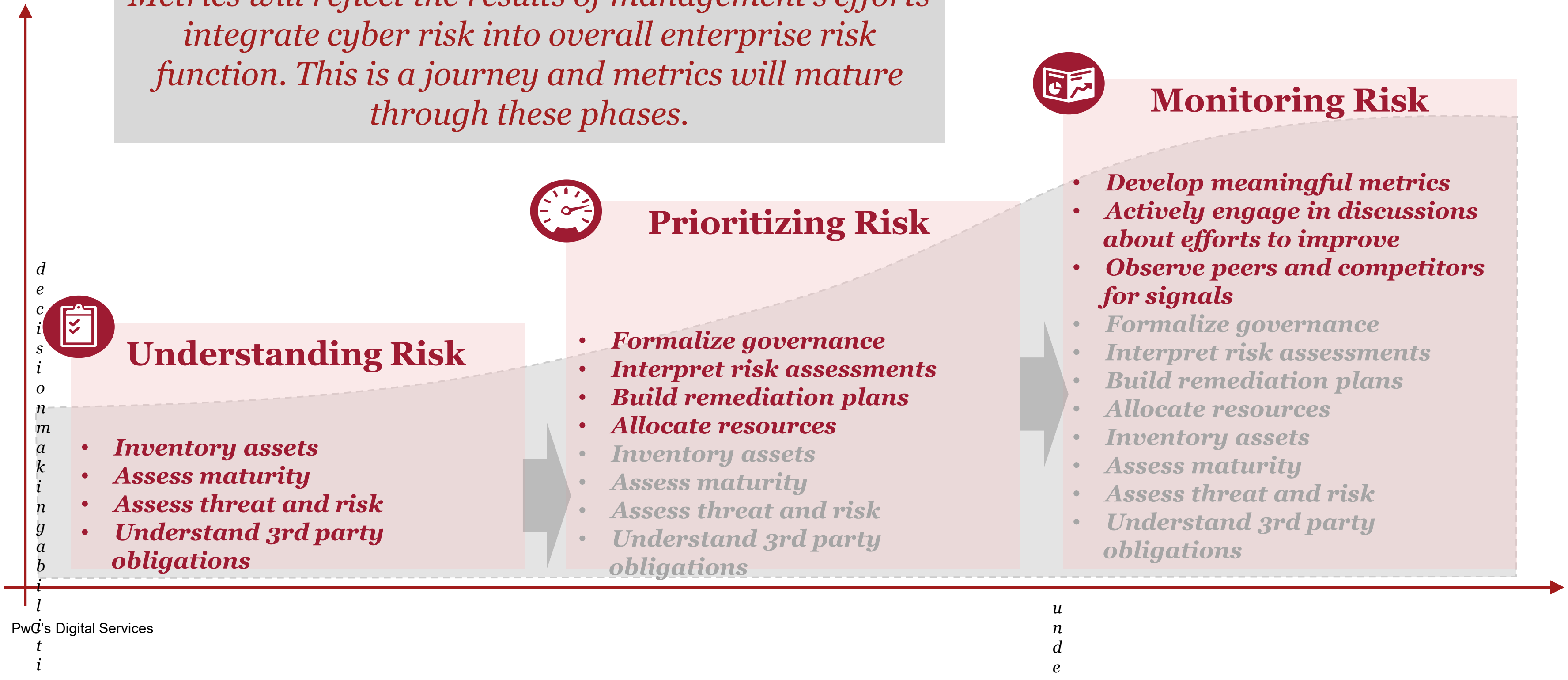
Program Status

Remediation Efforts

Cyber Risk Operations

They are maturing the way that risk oversight operates and communicates

Metrics will reflect the results of management's efforts integrate cyber risk into overall enterprise risk function. This is a journey and metrics will mature through these phases.



Understanding Risk

- *Inventory assets*
- *Assess maturity*
- *Assess threat and risk*
- *Understand 3rd party obligations*

Prioritizing Risk

- *Formalize governance*
- *Interpret risk assessments*
- *Build remediation plans*
- *Allocate resources*
- *Inventory assets*
- *Assess maturity*
- *Assess threat and risk*
- *Understand 3rd party obligations*

Monitoring Risk

- *Develop meaningful metrics*
- *Actively engage in discussions about efforts to improve*
- *Observe peers and competitors for signals*
- *Formalize governance*
- *Interpret risk assessments*
- *Build remediation plans*
- *Allocate resources*
- *Inventory assets*
- *Assess maturity*
- *Assess threat and risk*
- *Understand 3rd party obligations*

They are reaping the benefits of enhanced knowledge and visibility

Message

Promote the value & effectiveness of your cybersecurity program to executives – in simple business and economic terms

Risk Portfolio

Understand your aggregate portfolio of cyber risk and track how well your cyber capabilities are performing in managing your Value at Risk

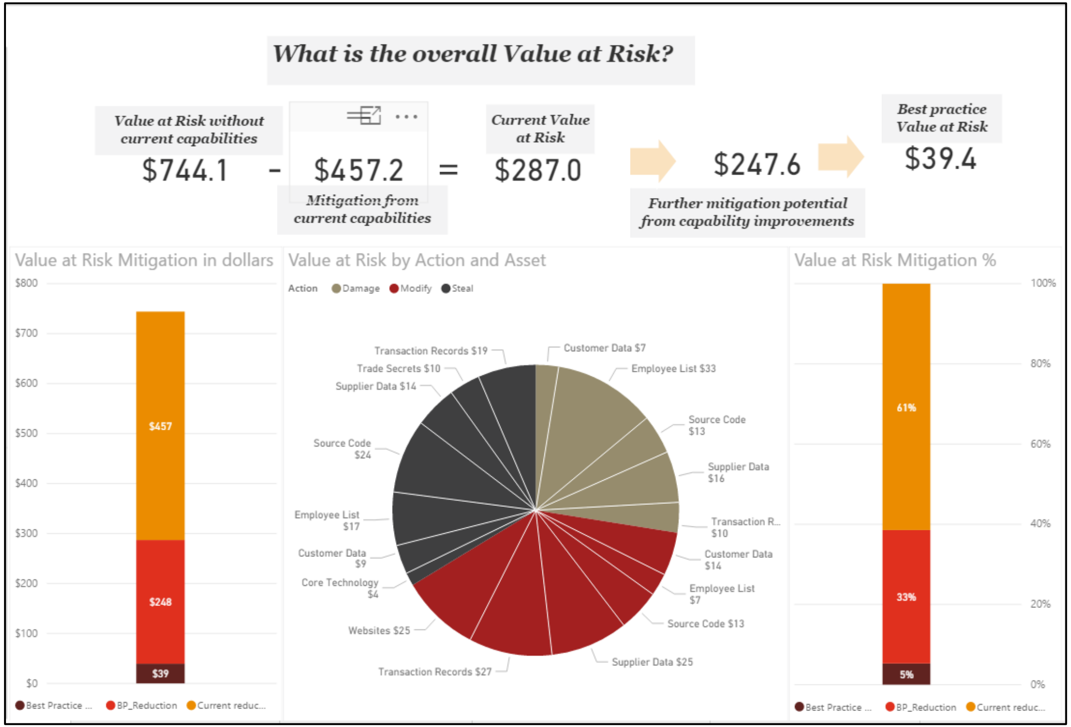
Capability Optimization

Transform information into insights to help you manage diminishing returns in your cyber capabilities

Capital Agility

Develop a defendable cyber investment strategy that allows you to effectively allocate limited resources and funds and respond to unexpected resource constraints

They are using digitized inputs to make value-based strategic decisions



What is the overall Value at Risk?

Value at Risk without current capabilities $744.1 - $457.2 *Mitigation from current capabilities* = *Current Value at Risk* $287.0 → $247.6 *Further mitigation potential from capability improvements* → *Best practice Value at Risk* $39.4

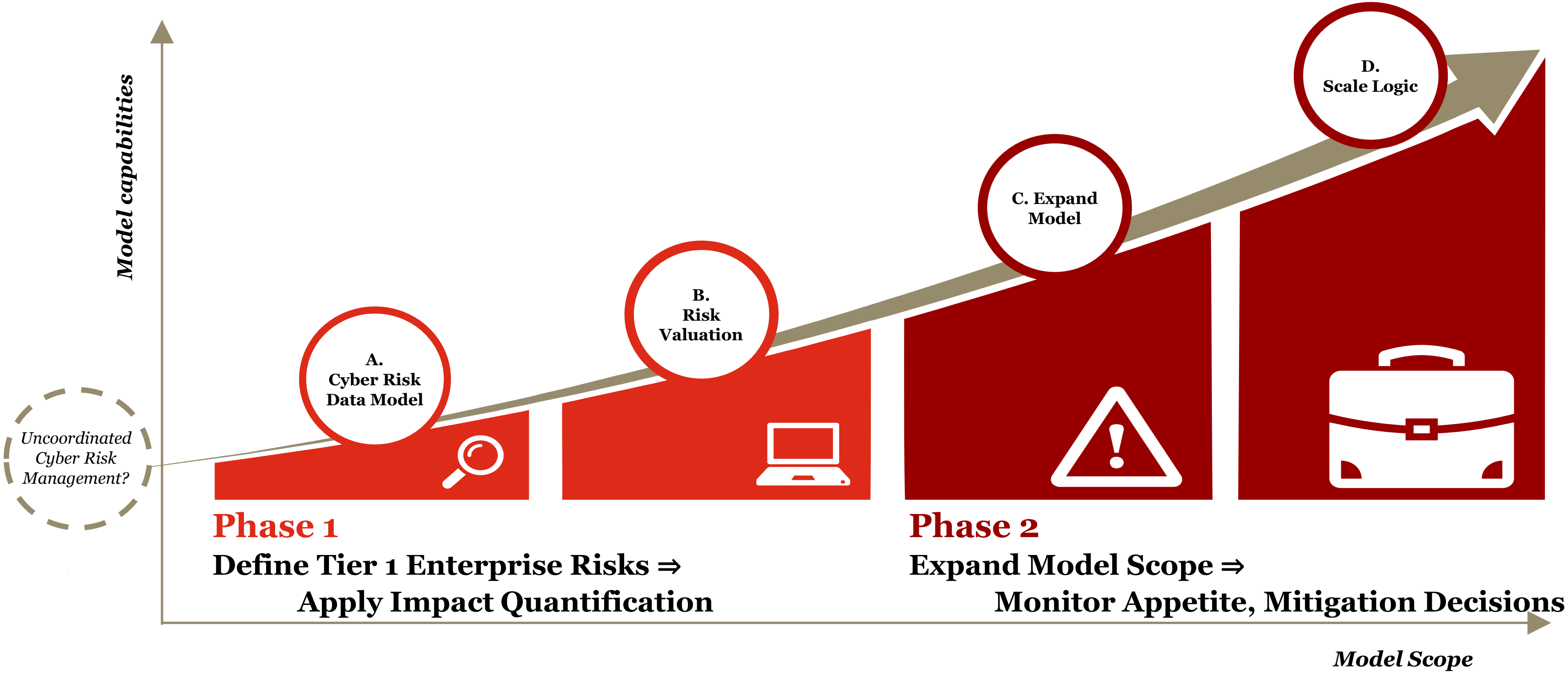
Digital Risk models based on:

- Current security posture
- Asset prioritization
- Threat prioritization

Are able to give insights like:

- Value at risk across the business portfolio
- Investment evaluation
  - ○ Risk reduction benefits
  - ○ Security posture gain
- Capability relevancy assessment
- Business objectives alignment
- Capability improvement ideation
- Risk metrics analysis

They are making decisions faster and achieving greater impact



Phase 1

Define Tier 1 Enterprise Risks ⇒ Apply Impact Quantification

Phase 2

Expand Model Scope ⇒ Monitor Appetite, Mitigation Decisions

What should auditors be thinking about; how can they take action?

Return to Fundamentals	***Emerging Capabilities***
What are you doing to address the current state of fundamentals?	*How are you laying the groundwork for successful embrace of emerging capabilities?*

Thank you.

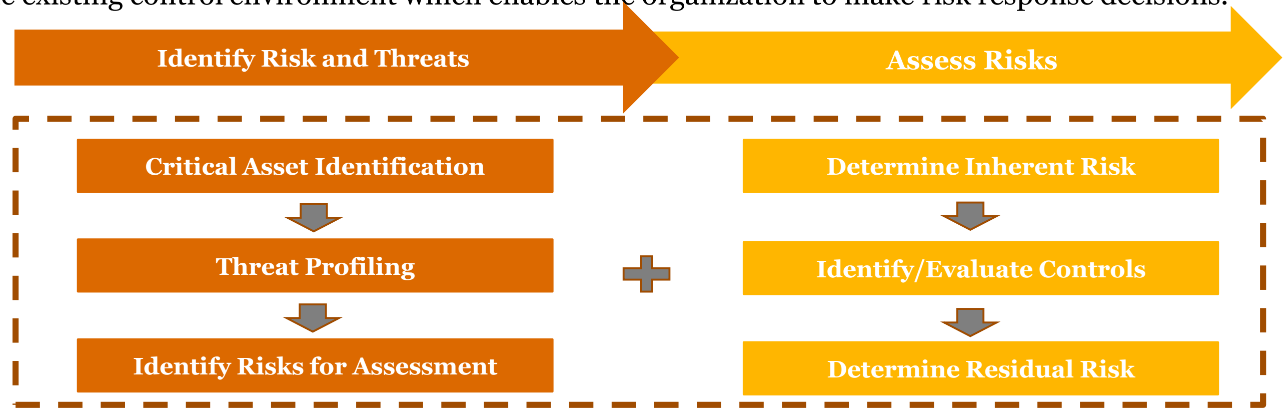
Questions?

pwc

Appendix

Cyber Risk & Threat Identification and Assessment

The first step to develop a Cyber Risk Management program is to identify the risks and threats that are realities of doing business in today's environment. Once risks and threats have been identified for your organization, those risks must be assessed to understand the existing control environment which enables the organization to make risk response decisions.



Identify Risk and Threats

Critical Asset Identification

Threat Profiling

Identify Risks for Assessment

Assess Risks

Determine Inherent Risk

Identify/Evaluate Controls

Determine Residual Risk

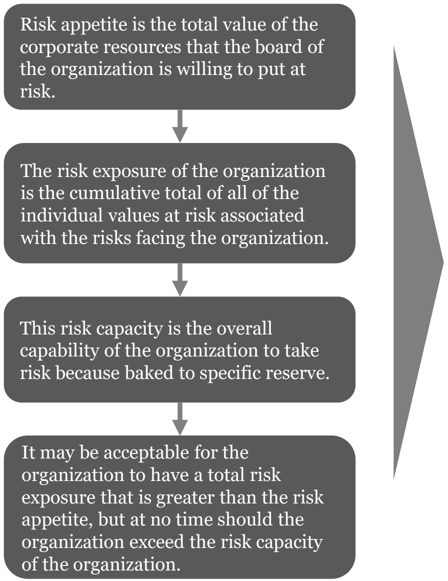
- Focus on the alignment of critical assets with relevant business risks and cyber threats:
  - What are the "Crown Jewels"?
  - Who/what are the potential threat actors, motives, and vectors?
  - What are our business risks (i.e., data breach, fraud)?

- Focus on the alignment of identified risks with relevant cyber controls:
  - What are the potential impacts (i.e., monetary, legal)?
  - What controls are in place to mitigate the risks?
  - Is the residual risk in line with our risk tolerance?

Cyber Risk Response

Formally setting a risk appetite for the enterprise and / or lines of business will help organizations understand and respond to adverse changes to their risk profile. This will help drive decision making including deployment of new controls and more successful risk mitigation strategies.

Risk appetite vs. risk exposure influences risk treatment decision…



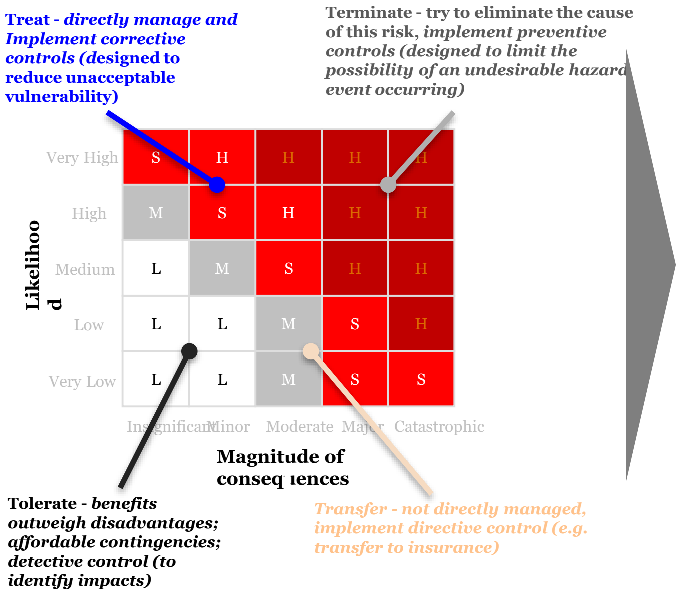
Risk appetite is the total value of the corporate resources that the board of the organization is willing to put at risk.

The risk exposure of the organization is the cumulative total of all of the individual values at risk associated with the risks facing the organization.

This risk capacity is the overall capability of the organization to take risk because baked to specific reserve.

It may be acceptable for the organization to have a total risk exposure that is greater than the risk appetite, but at no time should the organization exceed the risk capacity of the organization.

… that is based also on the specific level of considered risk.



Treat - *directly manage and Implement corrective controls* (designed to reduce unacceptable vulnerability)

Terminate - try to eliminate the cause of this risk, *implement preventive controls (designed to limit the possibility of an undesirable hazard event occurring)*

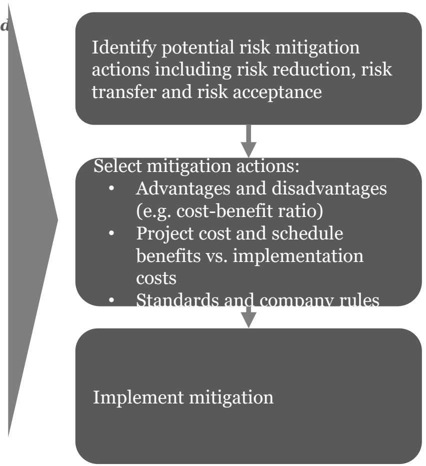
Likelihoo d	Insignificant	Minor	Moderate	Major	Catastrophic
Very High	S	H	H	H	H
High	M	S	H	H	H
Medium	L	M	S	H	H
Low	L	L	M	S	H
Very Low	L	L	M	S	S

Magnitude of conseq ıences

Tolerate - *benefits outweigh disadvantages; affordable contingencies; detective control (to identify impacts)*

Transfer - not directly managed, implement directive control (e.g. transfer to insurance)

Typically identifying mitigation action requires specific actions.



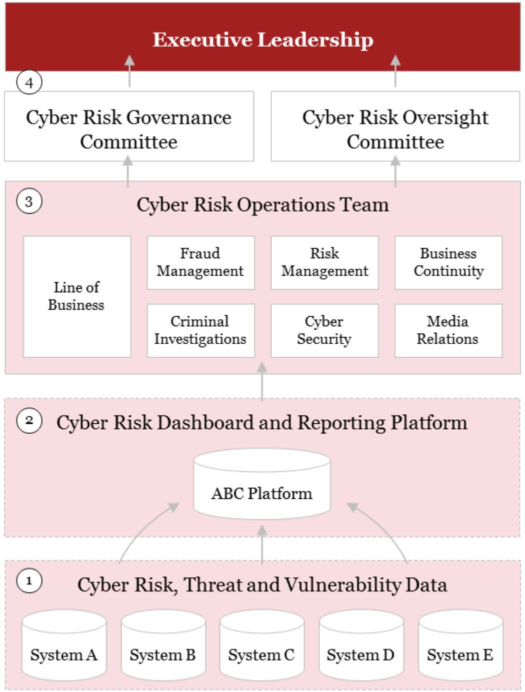
Identify potential risk mitigation actions including risk reduction, risk transfer and risk acceptance

Select mitigation actions:
- Advantages and disadvantages (e.g. cost-benefit ratio)
- Project cost and schedule benefits vs. implementation costs
- Standards and company rules

Implement mitigation

Cyber Risk Monitoring and Reporting

To make the right decisions, Executive Leadership and the Board of Directors must have the necessary information at its fingertips. An effective Cyber Risk Dashboard and Reporting Capability enables an organization to monitor and dynamically respond to changes in its cyber risk profile.



Executive Leadership

4

Cyber Risk Governance Committee

Cyber Risk Oversight Committee

3 Cyber Risk Operations Team

Line of Business

Fraud Management

Risk Management

Business Continuity

Criminal Investigations

Cyber Security

Media Relations

2 Cyber Risk Dashboard and Reporting Platform

ABC Platform

1 Cyber Risk, Threat and Vulnerability Data

System A

System B

System C

System D

System E

1. Disparate sources of data are aggregated in a dedicated Cyber Risk Dashboard and Reporting Platform.

1. The platform is used by members of the Cyber Risk Operations Team to perform scheduled and ad-hoc reporting on a variety of key topics (e.g., recent cyber incidents, their duration, the assets that were targeted, related external events etc.).

1. The Operations Team provides ongoing reports to the Cyber Risk Governance and Oversight Committees.

1. Reports provided the Cyber Risk Oversight Committee contain the status of various activities being performed to address cyber threats and improve cyber resiliency across the organization.

1. The Cyber Risk Governance and Cyber Risk Oversight Committees provide periodic reporting to Executive Leadership.

Cyber Risk, Threats and Controls Library

An integrated risk and controls library enables continuous risk management and cross-functional coordination (i.e., within Security and between Security, Risk Organizations, and Business Units).

Integrated Risk, Threats and Controls Library

Risk

- Risk Category
- Risk Sub-Category
- Business Risk Event
- Risk Scenario
- Threat Vector

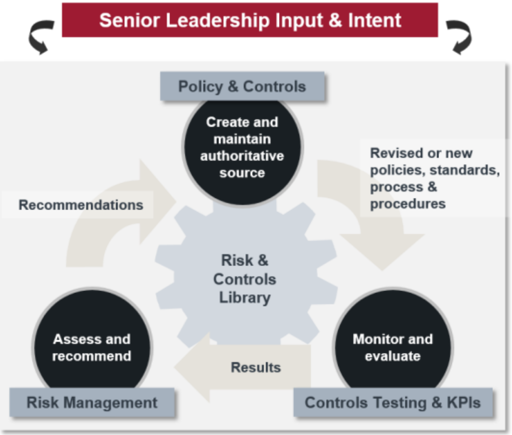
+

Controls

Rationalized Control Objective	Control Activity	Test Procedures and Evidence Request List
Control Owner	Control Scope	Control Execution & Monitoring Frequency
Standard	Policy	Framework

Example Control Domains

Architecture and Operations	Third Party Management
Threat and Vulnerability Management	Incident and Crisis Management
Information and Asset Protection	Risk, Compliance, and Policy Management
Identity and Access Management	Strategy, Governance, and Management
Business Continuity	Physical and Environmental Security


Senior Leadership Input & Intent
Policy & Controls
Create and maintain authoritative source
Recommendations
Revised or new policies, standards, process & procedures
Risk & Controls Library
Assess and recommend
Results
Monitor and evaluate
Risk Management
Controls Testing & KPIs