Information Security Governance Models: Empowering the Organization

ISACA GRC Conference
October 20, 2011
Orlando, Florida

Introductions

Matt Hynes

Senior Manager
Advisory Practice
Minneapolis, MN

- BBA from University of Notre Dame, MBA from New York University
- CISSP, CISA, CISM, CIPP
- US leader for Ernst & Young's Security Program Management (SPM) services
- Specializations
  - Information Security Organizational Design & Strategy
  - IT/Business Alignment

Justin Greis

Senior Manager
Advisory Practice
Chicago, IL

- BS and MBA from Indiana University (Accounting/IS)
- CISSP, CISA, CISM, CGEIT, CRISC, CIPP, GIAC/GSEC, PMP, ITIL
- Professor of Information Systems at Indiana University, Bloomington, Kelley School of Business
- Specializations
  - Information Security
  - IT Strategy, Governance & Effectiveness
  - Program & Project Management

Information security touches every aspect of business.

The Information Security Challenge

- Managing information security risk across the enterprise is a complex task that requires the input and coordination from many stakeholders throughout the corporation.
- **Security touches every aspect of business** and IT, therefore it becomes a part of everyone's collective responsibility.
- How do we bring the **right groups** and **stakeholders together** into a cohesive team to **make informed, risk-based decisions** using all available information **at the right time?**

Managing the Stakeholders

- Stakeholder selection can be a challenge since **everyone plays a role in protecting corporate information.**
- **Departmental boundaries** and **scope** often play a role in creating an effective information security committee.
- Each stakeholder must play a distinct role in the committee and make valuable contributions.

Organizing the Team

- There is **no "right" or "wrong" way to organize your governance committee;** it depends on many factors that may influence your selection.
- **The "right" structure is heavily reliant upon the culture of the organization and its ability to work together.**

Agenda

1. The Challenge of Information Security Today
2. The Organization: Mapping Power and Control
3. Governance Models and Committees
4. Aligning Your Organization For Success

Executive Summary

Governance committees are foundational to running an effective information security program. They promote open communication, increase effectiveness of the control environment, build consensus on the vision of the program and empower the company by establishing a shared vision of IT risk and security.

However, each organization chooses a different security governance structure to address its unique requirements. While there is no right or wrong way to organize a one's governance committee, the following deck explores three generalized models for consideration. These models are not mutually exclusive; they can be implemented together or in part to form a hybrid structure that works for a particular company.

It is not possible to recommend an appropriate model without a deep understanding of the company and its needs; however, this deck is intended to draw out discussion of the important decision criteria and key considerations when designing a governance model.

Let's do a little experiment…

Justin's $50 Mistake

ISACA
Trust in, and value from, information systems

Here is our scenario…

Stored in a secure lock-box

Sitting out on a table.

Guarded by someone who will alert me when the money is stolen.

Guarded by someone who will ward off thieves and alert authorities.

Protected by a motion detector alarm designed to automatically alert me of a theft.

Consider the following…

What is the risk?

ISACA
Trust in, and value from, information systems

Let's Take a Walk

Let's give it a try.

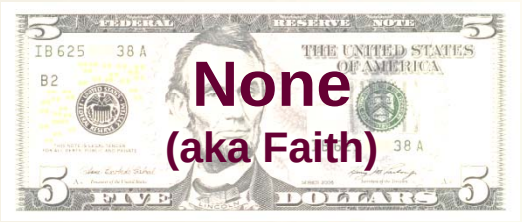
Where's the Money?

What happened?

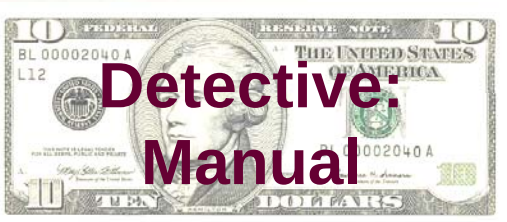
ISACA
Trust in, and value from, information systems

What controls were applied?

Stored in a secure lock-box



Sitting out on a table.

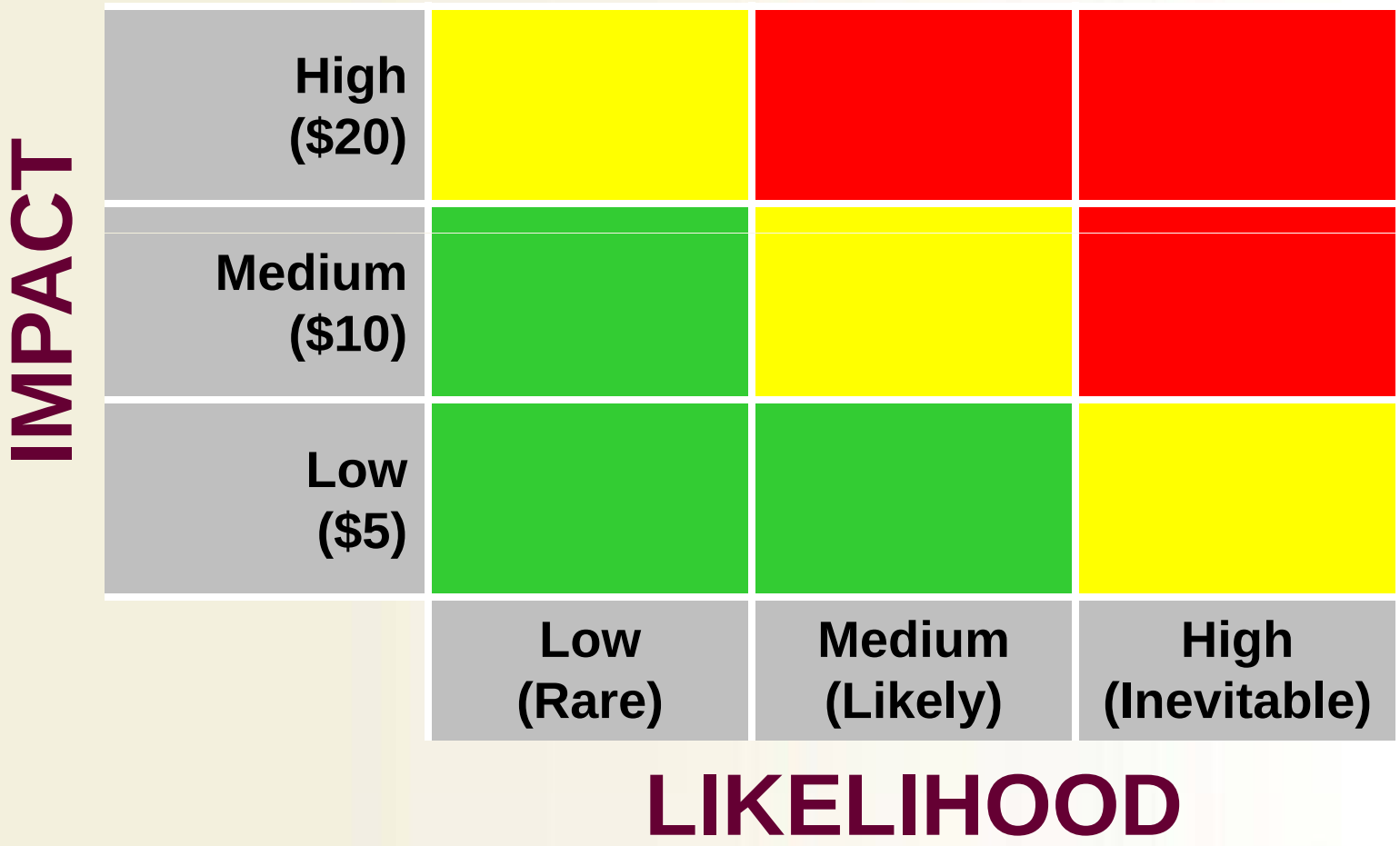


Guarded by someone who will alert me when the money is stolen.

Guarded by someone who will ward off thieves and alert authorities.

Protected by a motion detector alarm designed to automatically alert me of a theft.

What is our risk profile?



How can we apply governance to enhance the process?

- You are all a part of the **ISACA GRC Cash Council**. Our mission is to **protect the assets of the company**.
- In this meeting we must discuss:
  - **What** happened to my $50?!?!?!
  - **Why** did this happen…
  - **How** can we make this process better?
- Once you come up with your recommendations, implement it so we can test it out.
- Let's try the exercise again.

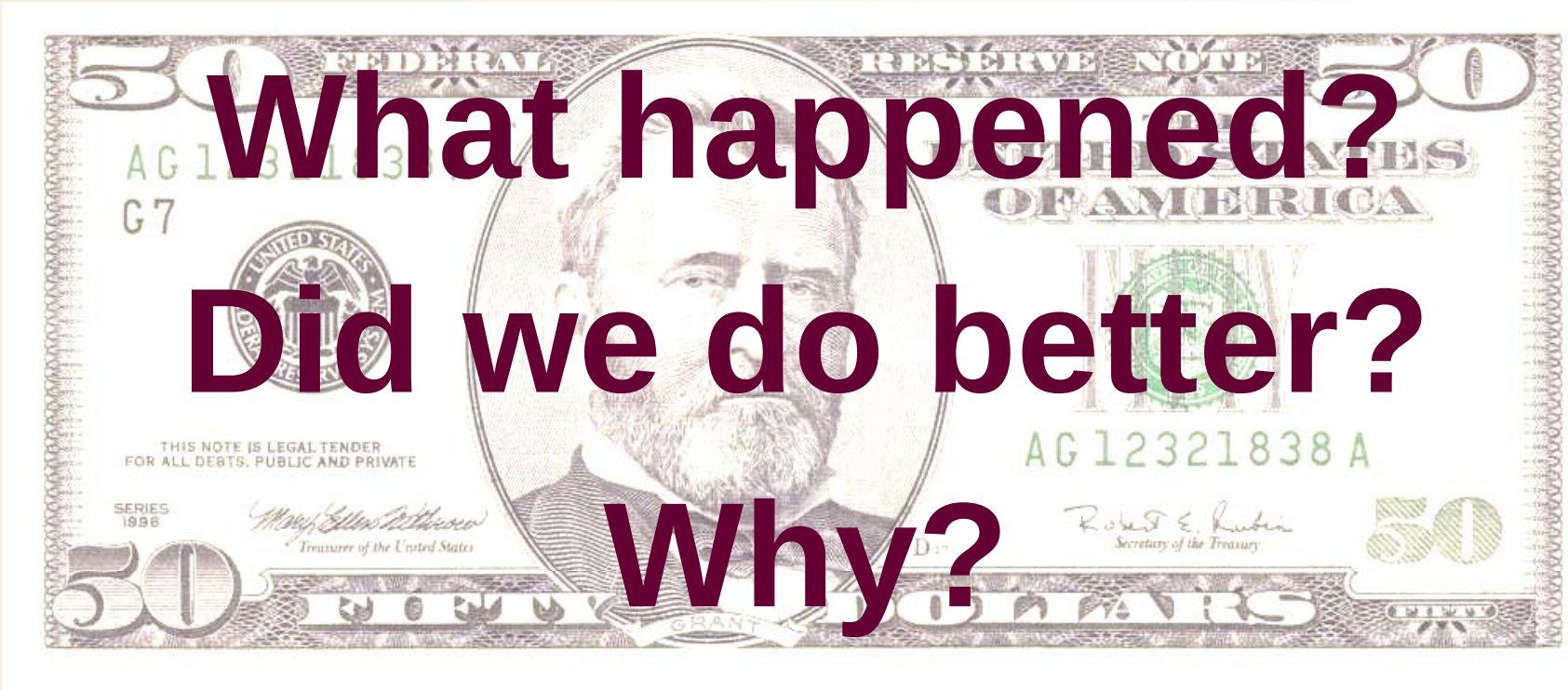
ISACA
Trust in, and value from, information systems

Let's Take a Walk…

Let's try again.

ISACA
Trust in, and value from, information systems

Where's my money?



What happened?

Did we do better?

Why?

Take away…

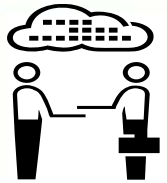
A company's ability to protect its assets are only as good as the governance model it uses to protect its assets.

Information Security Models: Empowering the Organization

THE CHALLENGE OF INFORMATION SECURITY TODAY

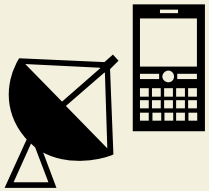
Insights on information security.

60% of organizations see increased risk from using social networking, cloud computing and personal mobile devices at work.



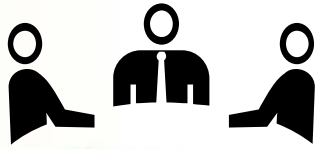
While only 52% of organizations indicate data leakage is a top “new” increased risk.

87% of organizations believe the damage to reputation and brand is the most significant issue related to data loss.



Yet, only **10%** of respondents indicated that examining new and emerging trends is a very important activity for the information security function.

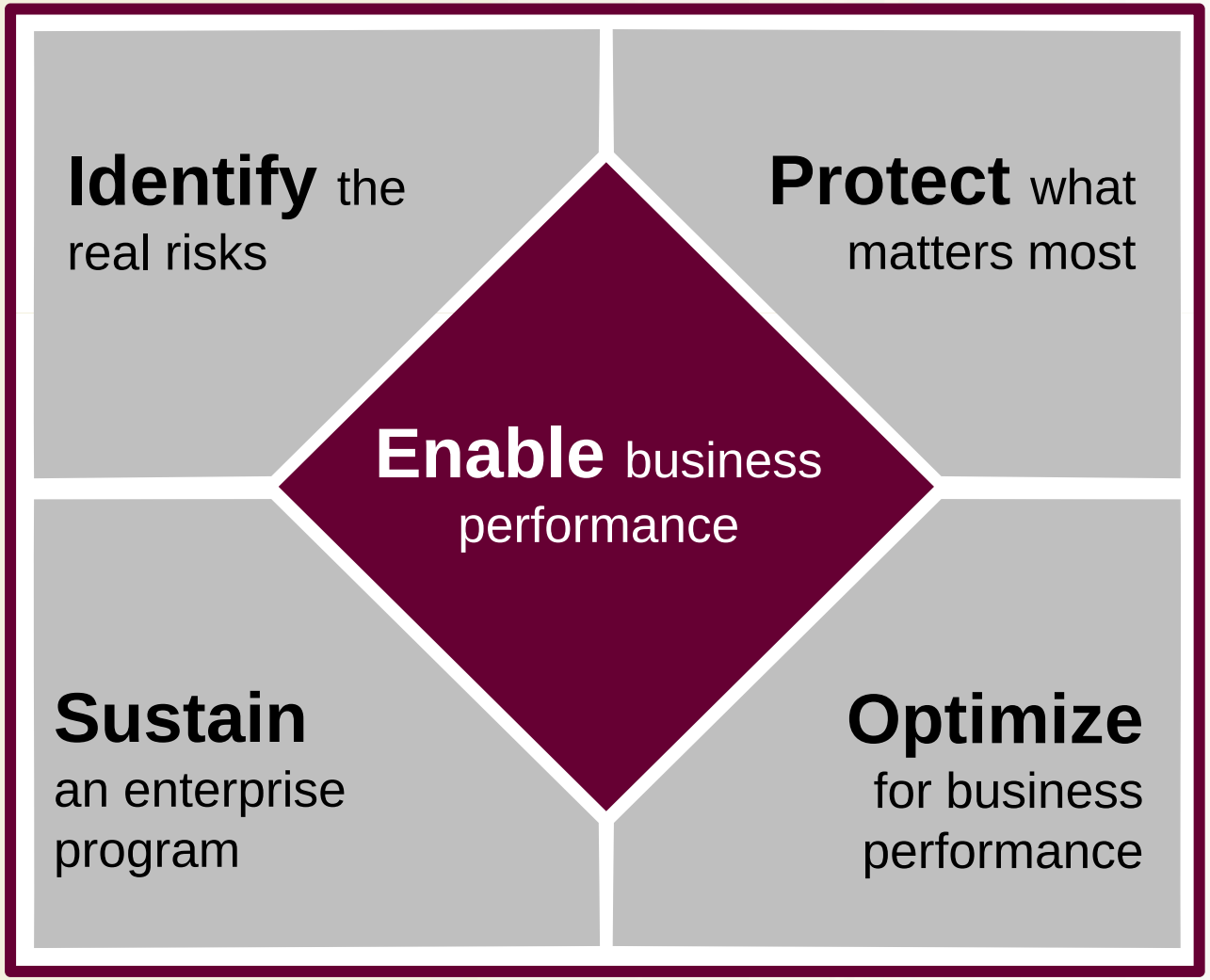
However, 61% are not making policy adjustments or increasing security awareness to address these new threats.



In 2011, there are four major trends that significantly impact information security.

1	**Advanced Persistent Threat**	• Long-term pattern of targeted, sophisticated attacks aimed at governments, companies and political activists. • Organized, politically/economically motivated groups of cyber criminals. • Specifically designed to evade traditional security measures.
2	**Social Media**	• We now connect with each other in two worlds: the physical world and the virtual world. • Originally designed for personal and pleasurable use, social media has introduced new efficiencies and risk to legacy business communications.
3	**Cloud Computing**	• It is no longer necessary to maintain your own set of hardware and software to run your business. • Cloud service providers have made it possible to run almost every aspect of your business using their infrastructure.
4	**Mobile Devices**	• New devices such as iPhones, Blackberries, iPads, and other tablets have increased the efficiency of our work. • But as devices shrink in size and become more sophisticated in what they can do, the risk of data loss or breach increases as well.

Transform your security program to improve business performance.



Five questions for the C-suite

1. **Do you know how much damage a security breach can do to your reputation or brand?**
2. **Are internal and external threats considered when aligning your security strategy to your risk management efforts?**
3. **How do you align key risk priorities in relation to your spending?**
4. **Do you understand your risk appetite and how it allows you to take controlled risks?**
5. **How does your IT risk management strategy support your overall business strategy?**

Today's security programs are ineffective.

- According to Ernst & Young's 2011 Global Information Security Survey (GISS), **less than half of respondents think their information security function is meeting the needs of their organization (49%)**

- Why? The data suggests three reasons:
  1. An **over-reliance on technology** to solve today's problems
  2. A **lack of strategic planning** and
  3. Organizations that are **not aligned** with the current threat landscape.

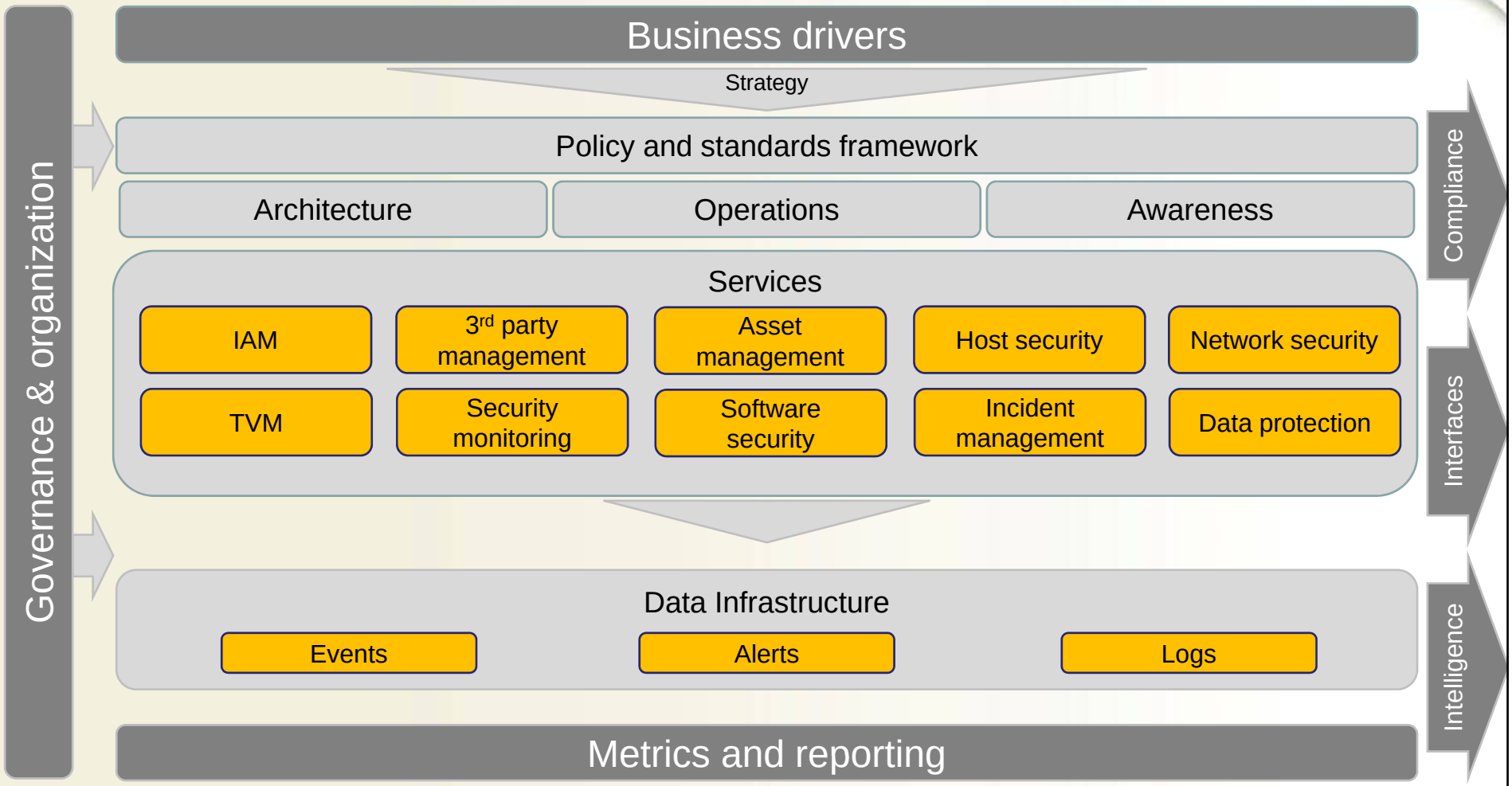
One root cause: failing to plan strategically.

- 46% of organizations **do not have a long term security plan**
- Only 24% of organizations **think they have a strategy** that addresses today's risks
- And although 67% of respondents say that the external risk environment is increasing, **only 1/3 have updated their strategy in the past 12 months**.

What can be done?

- **Get back to the basics.** Stop spending money on the latest tools, and focus on the fundamentals: patching vulnerabilities; strengthening system configurations; and properly configuring software.
- **Develop a strategic plan.** Having a clearly articulated strategic plan shows company leadership that the organization has a vision for improving security, which is not being directed merely by the latest headlines.
- **Use a common sense approach.** Understand your assets, assess your current capability, define how to close capability gaps, and then develop the 3-year plan to close the gaps.

Where does it fit?



Information Security Models: Empowering the Organization

THE ORGANIZATION: MAPPING POWER AND CONTROL

There are three ways to effectively control an organization.

- **Resources**
  - Control over money, resources and assets determines what the organization buys or invests in.

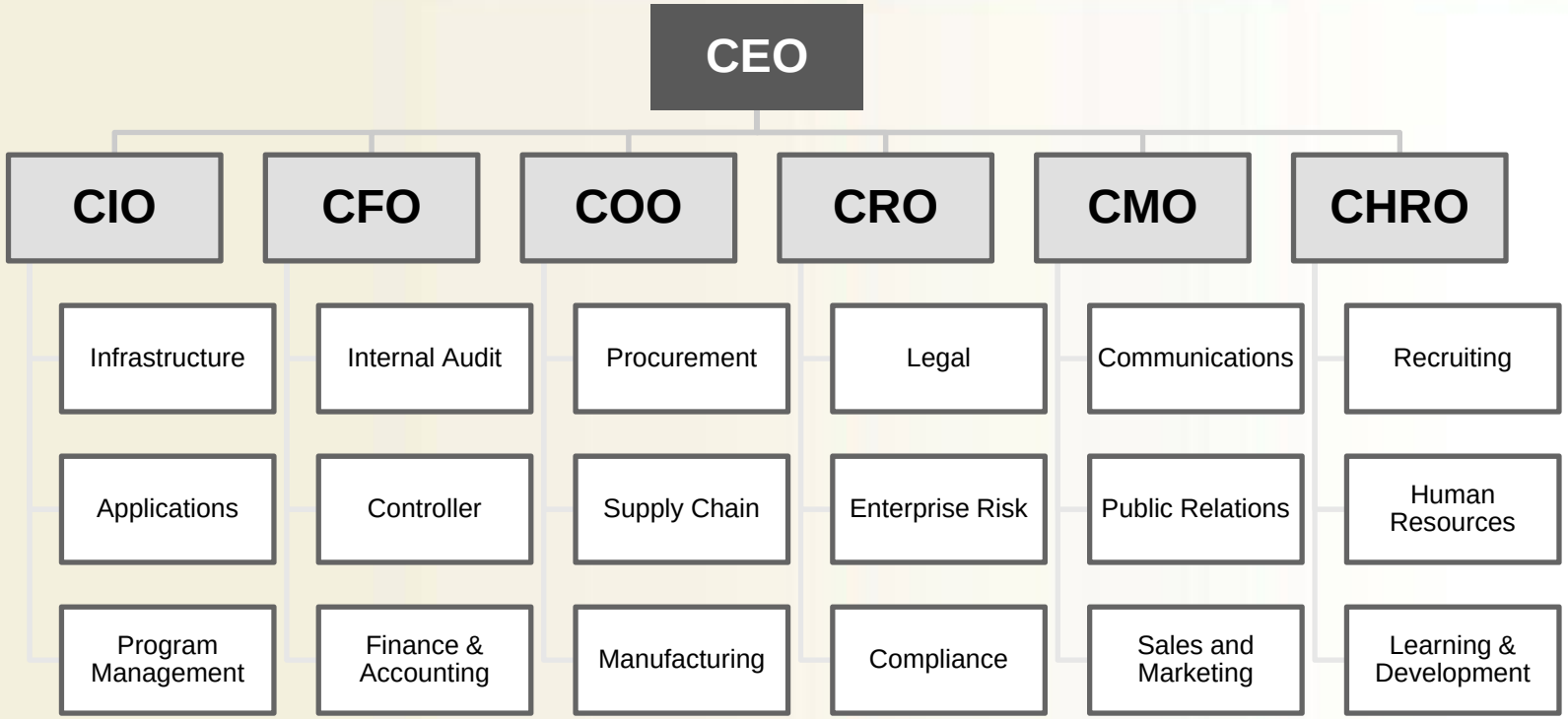
- **Strategy**
  - Directives set by executive leadership or regulatory bodies controls how the organization sets its vision.

- **Authority**
  - Scope of control can be limited based on an organization's authority and limit its ability to make autonomous decisions.

When designing an information security organization, we want it to be…

- Integrated
- Collaborative
- Risk-based
- Enable the business
- Cost effective
- Forward-thinking
- Metrics-driven
- Planned strategically
- Tactically focused and executed

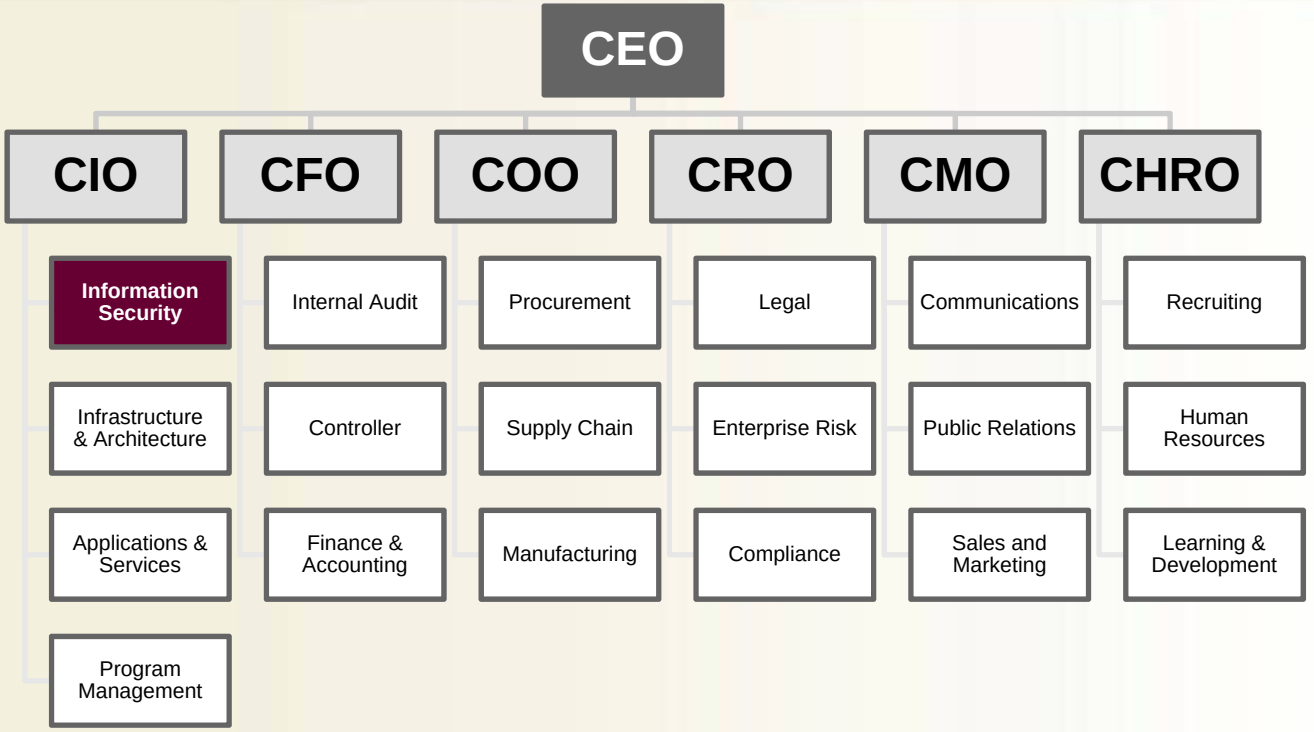
Let's look at a the typical functions and roles within a large corporation…



Q ***Where* does *information security* fit in the organization?**

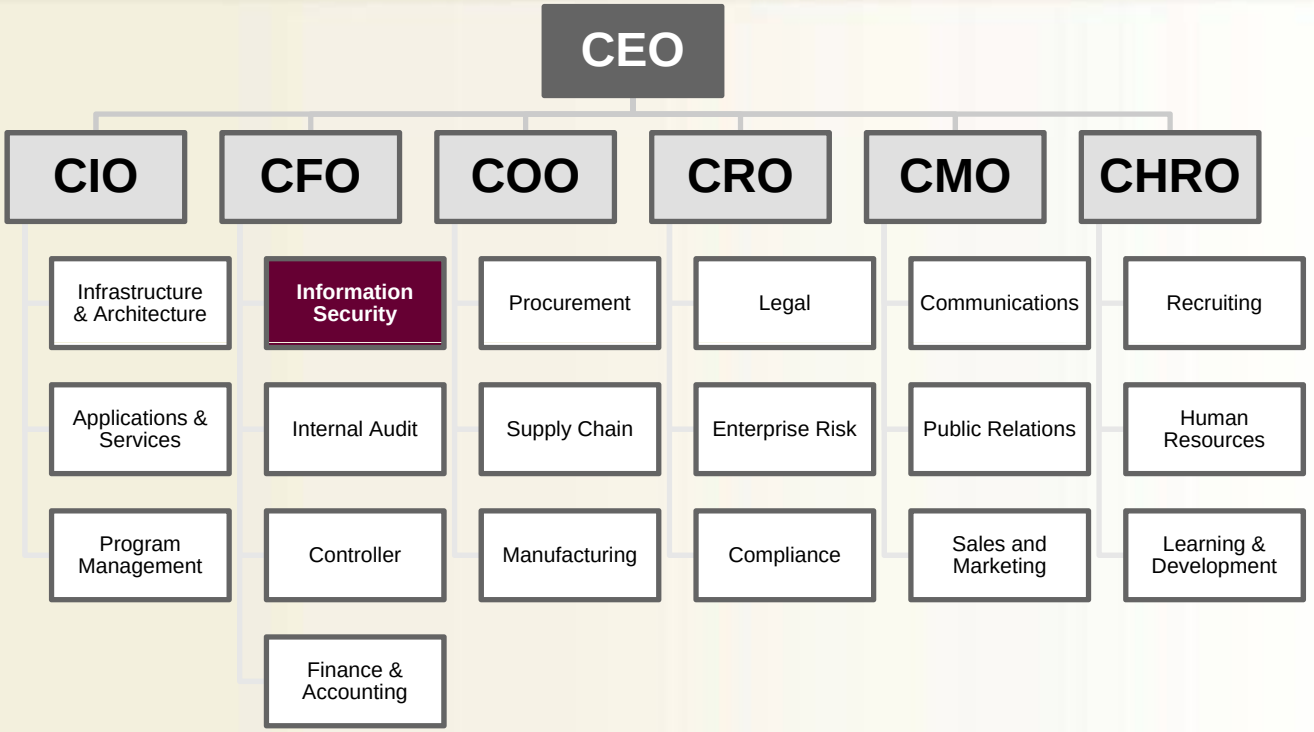
A **It varies from company-to-company. But wherever it is located, it has a major impact on the resources, strategy and authority of the enterprise.**

Information security reports to the CIO…



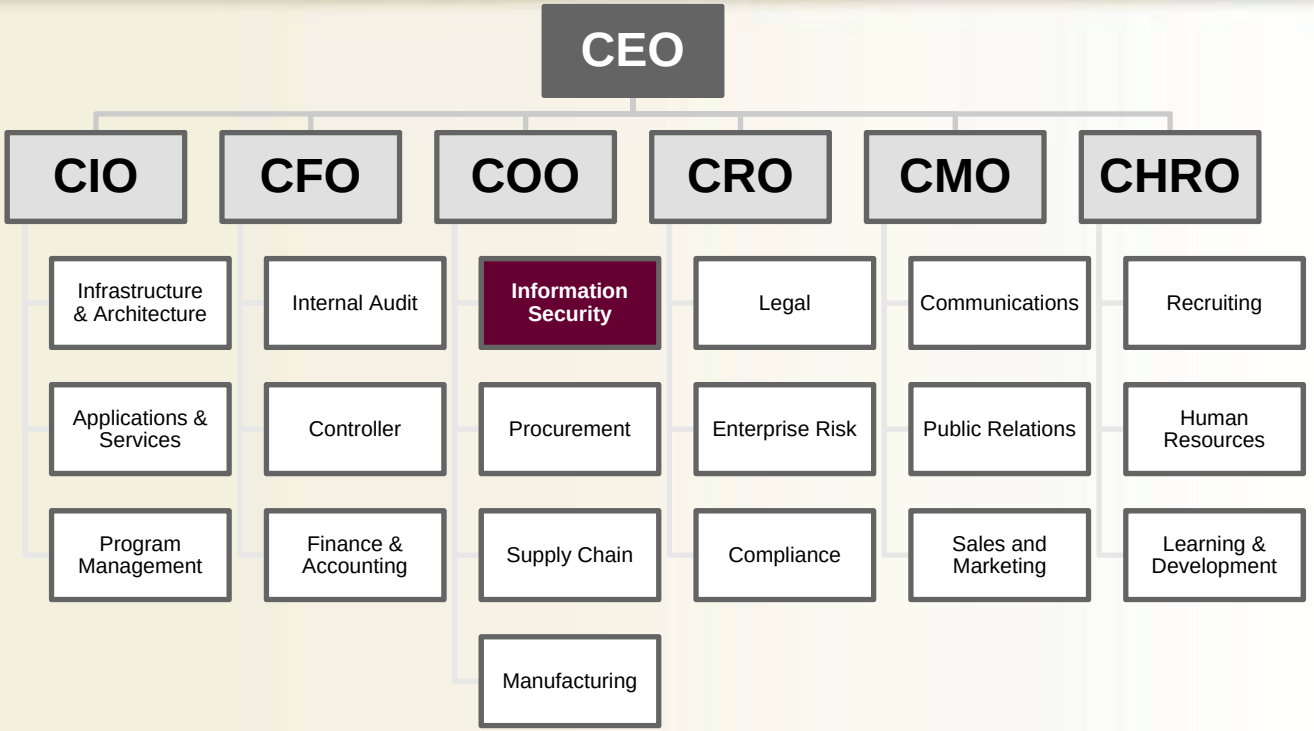
Pros	Cons
• IT resources are readily available • Solutions can be easily integrated and addressed with technology • Security embedded in key IT processes	• Risks may not receive necessary attention • Resources split between all IT functions • Very siloed authority of the technology functions

Information security reports to the CFO…



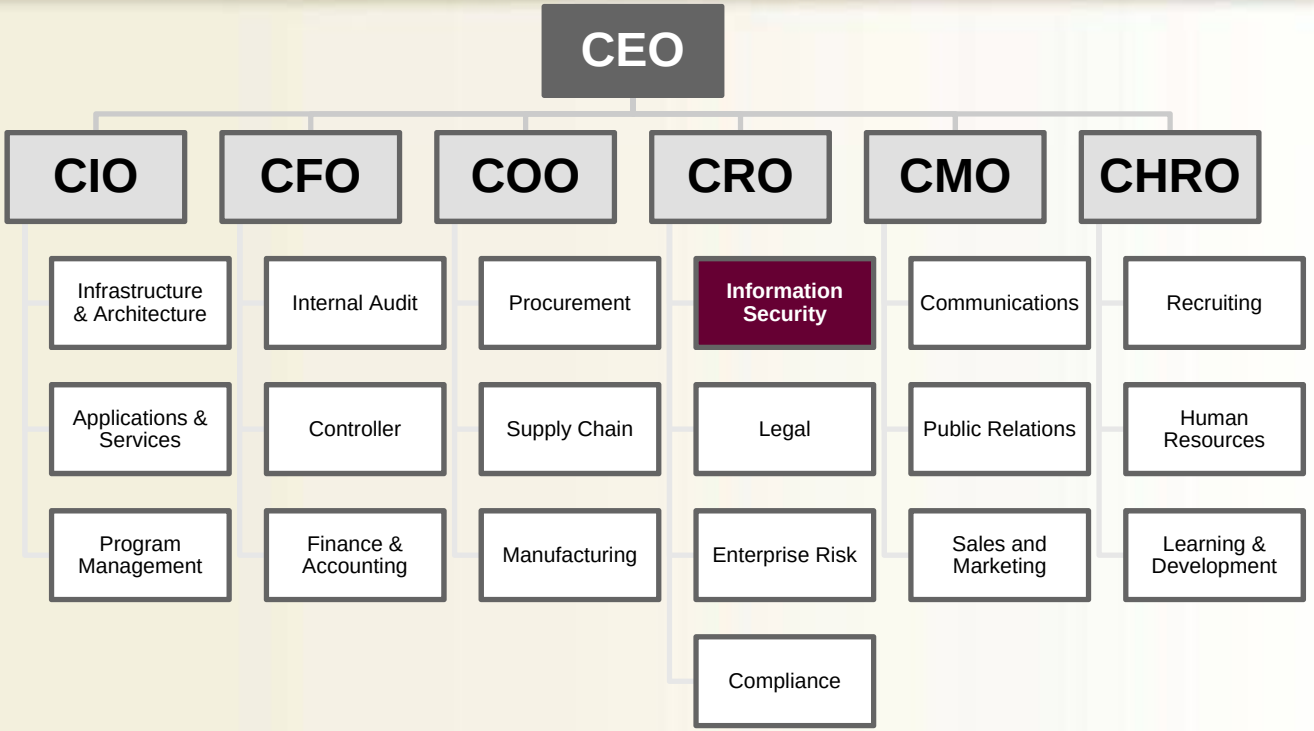
Pros	Cons
• Business and financially oriented view of security • Security integrated with audit and controls • Heavy focus on compliance	• Finances are controlled by CFO who may not understand the security issues • Strong emphasis on verification and audit rather than enabling the business

Information security reports to the COO…



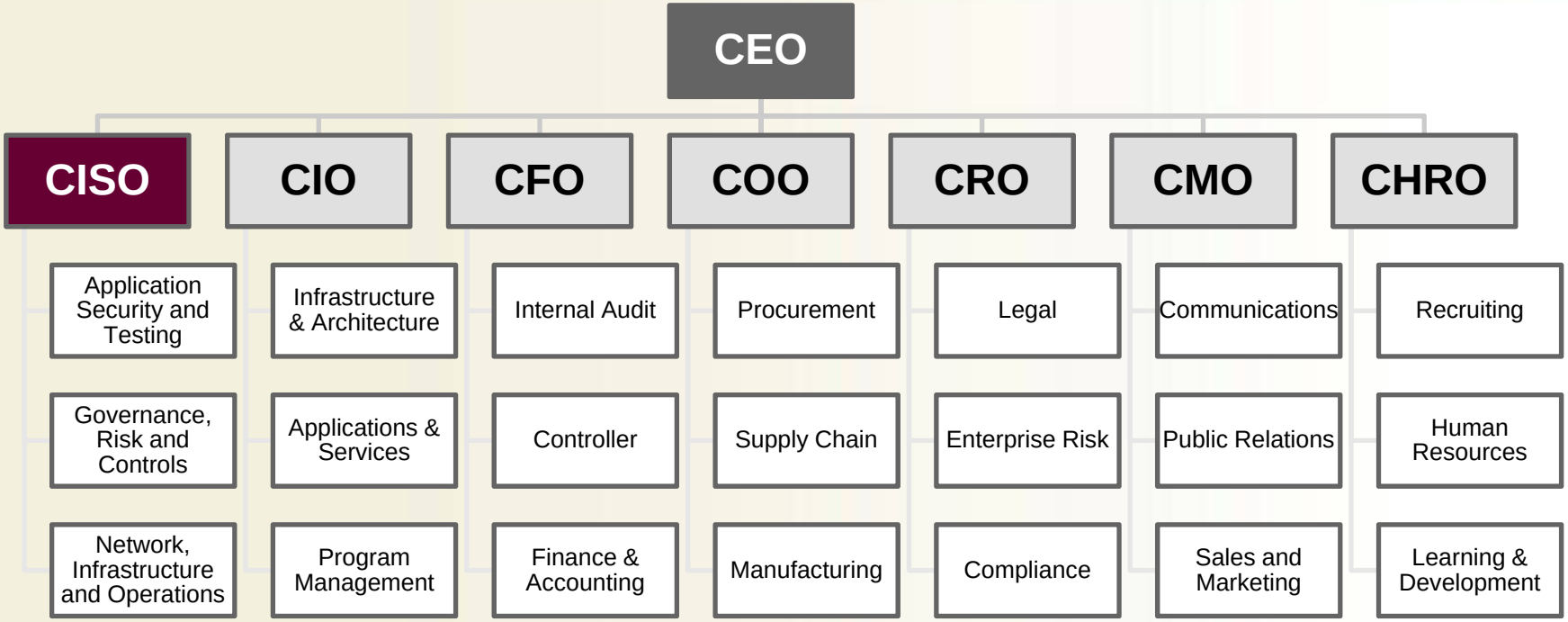
Pros	Cons
• Security embedded into key business processes • Strong focus on operational security • Emphasis on efficiency and production	• Pressured to “run lean” • May not be able to act strategically • Budgeting and planning focuses on operations rather than emerging threats

Information security reports to the CRO…



Pros	Cons
• Heavy emphasis on risk and compliance • Very good for regulated industries • Maintains independence from other core business functions	• May not be fully integrated with business or IT functions

Information security reports to the CEO…



Pros	Cons
• Autonomous and independent • Board and executive level attention to security issues • Access to emerging technology and strategy	• Integration may be a challenge • Reporting and dashboarding may present a challenge

Promoting integration across the enterprise…

Integration of security across the enterprise is a challenge. Enforcing standardization and a common security architecture is especially difficult for large organizations…

Security Liaisons *Evangelists* *Champions*

Security Architects and Engineers

Training, Education and Awareness

Rewarding and Discouraging Behaviors

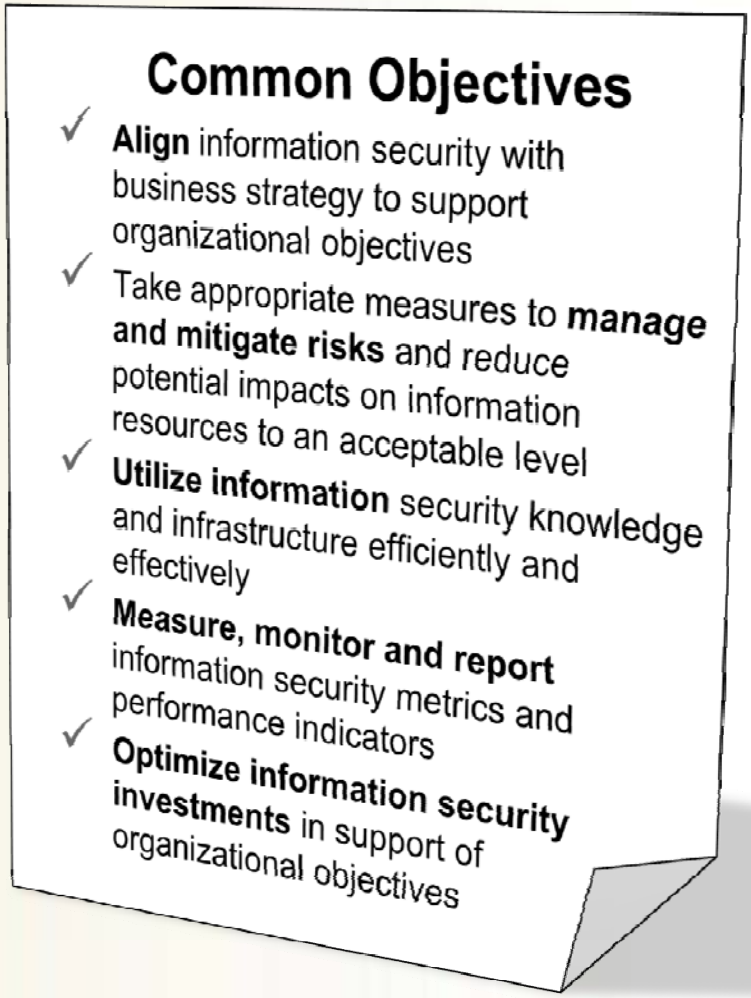
Security Councils

Information Security Models: Empowering the Organization

GOVERNANCE MODELS AND COMMITTEES

Governance committee objectives

- All information security governance committee models have a common set of objectives.
- These objectives are carried out differently depending on:
  - Level of Executive Involvement *(or Power)*
  - Decision Authority *(or Ability to Enable Change)*
- Objectives are typically common, but the means of achieving those objectives can vary.
  - *Example: Some organizations separate security core functions (e.g. policy, incident response, architecture, etc.) from mission critical solution delivery (e.g. IAM, network operations, etc.)*



Source: Adapted from IT Governance Institute, Board Briefing on IT Governance

Governance model characteristics

Power and ability to enable change are two factors that determine the characteristics of a governance model.

Power	Change	
↓	↓	***"Doers"***

Composed of functional leaders experts who actually execute the ideas they come up with.

↑	↓	***"Advisors"***

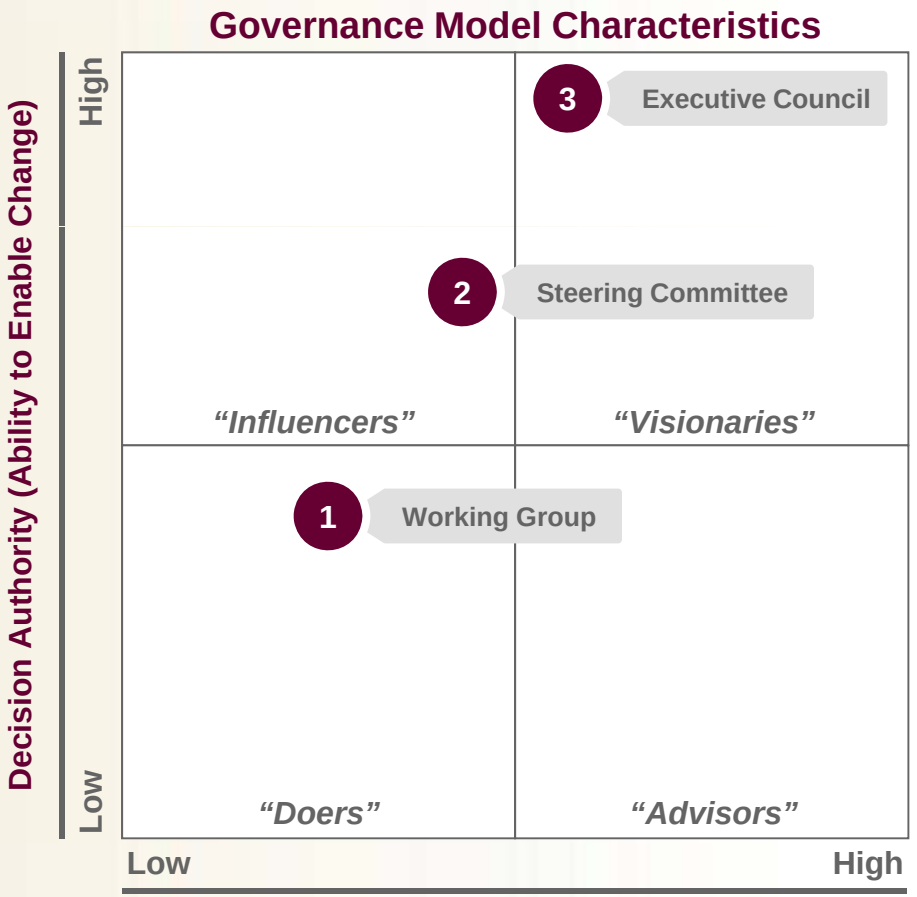
Composed of subject matter experts who advise on solution design, provide input into issues, or provide specific direction on a topic or set of topics.

↓	↑	***"Influencers"***

Key resources who play critical change roles in the organization. May not be in executive leadership but serve as champions of issues.

↑	↑	***"Visionaries"***

Leaders of the organization who can both lead change and set tone at the top and direction.



Governance Model 1: Working Group

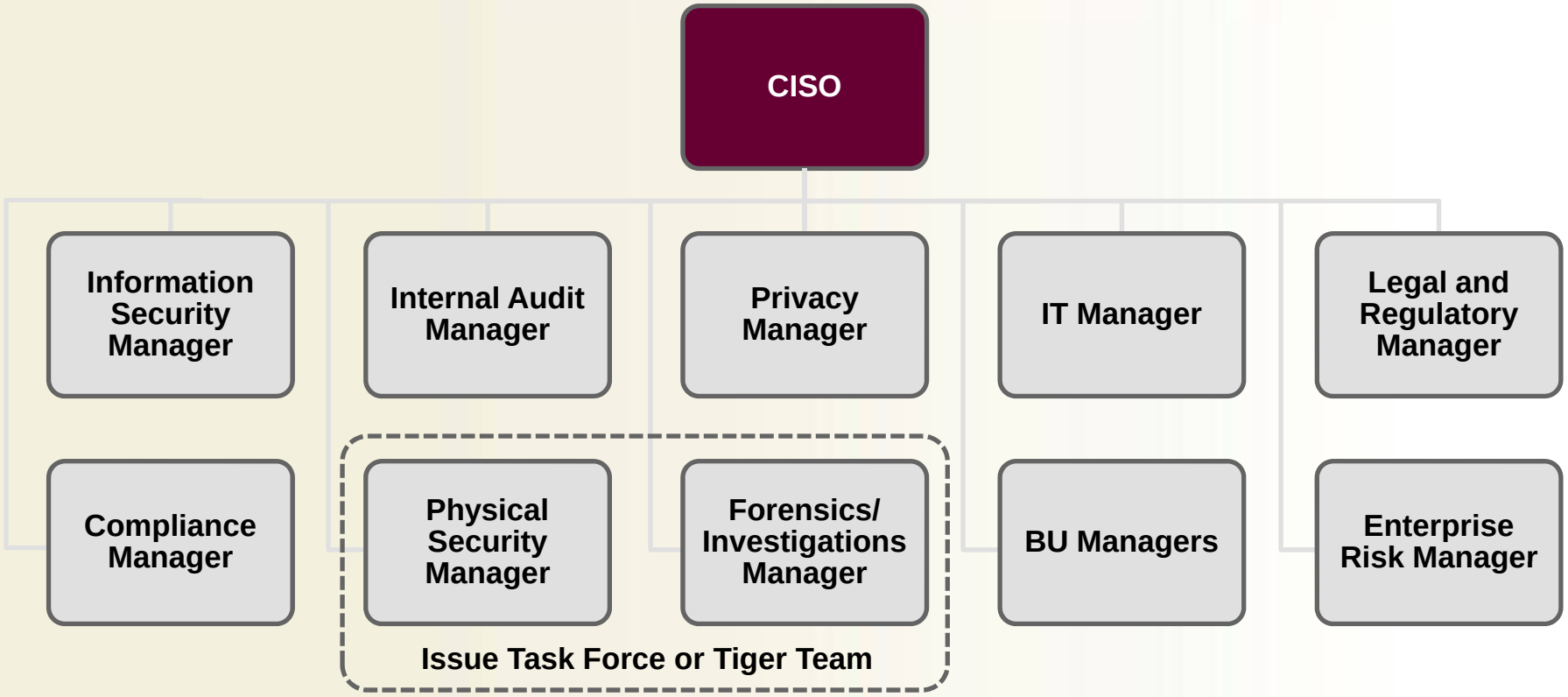
1. **Working Group**
   Operational management team with execution responsibility
2. **Steering Committee**
   Leadership team that sets collaborative vision and delegates action to its teams
3. **Executive Council**
   Executive-level team that sets direction, allocates resources, and provides oversight

This model focuses on operational issues of the organization. It is typically used as a task-force to address specific issues or take on difficult matters requiring specialized attention. This group meets often to collaborate, bring issues forward and recommend solutions to their functional areas. This group often does not have significant budget authority but can recommend solutions and innovation to their respective leaders.

Model Characteristics	
Collaboration	*High*
Communication Style	*Dialog or Two-Way*
Budget Authority	*Limited*
Issue Focus	*Narrow focus on operational issues*
Meeting Frequency	*Often (i.e. weekly or bi-weekly)*
Decision Authority	*Recommend*
Transformation Effectiveness	*Low*
Strategic Focus	*Low*

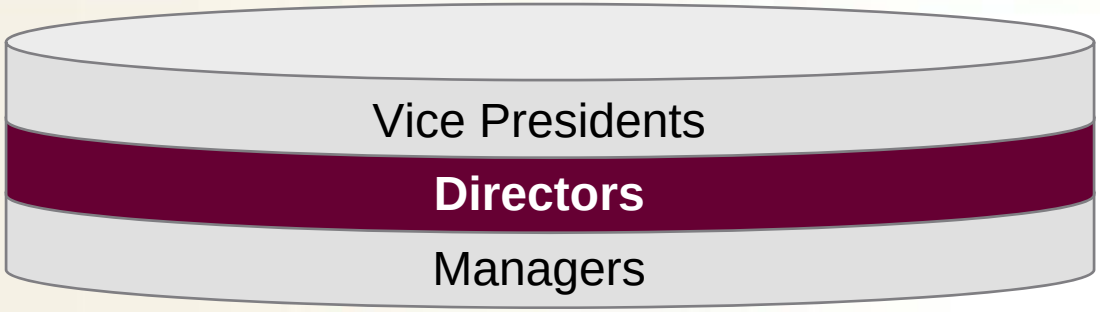
Governance Model 1: Working Group

Example Organizational Chart



Governance Model 2: Steering Committee

1. **Working Group**
   Operational management team with execution responsibility
2. **Steering Committee**
   Leadership team that sets collaborative vision and delegates action to its teams
3. **Executive Council**
   Executive-level team that sets direction, allocates resources, and provides oversight



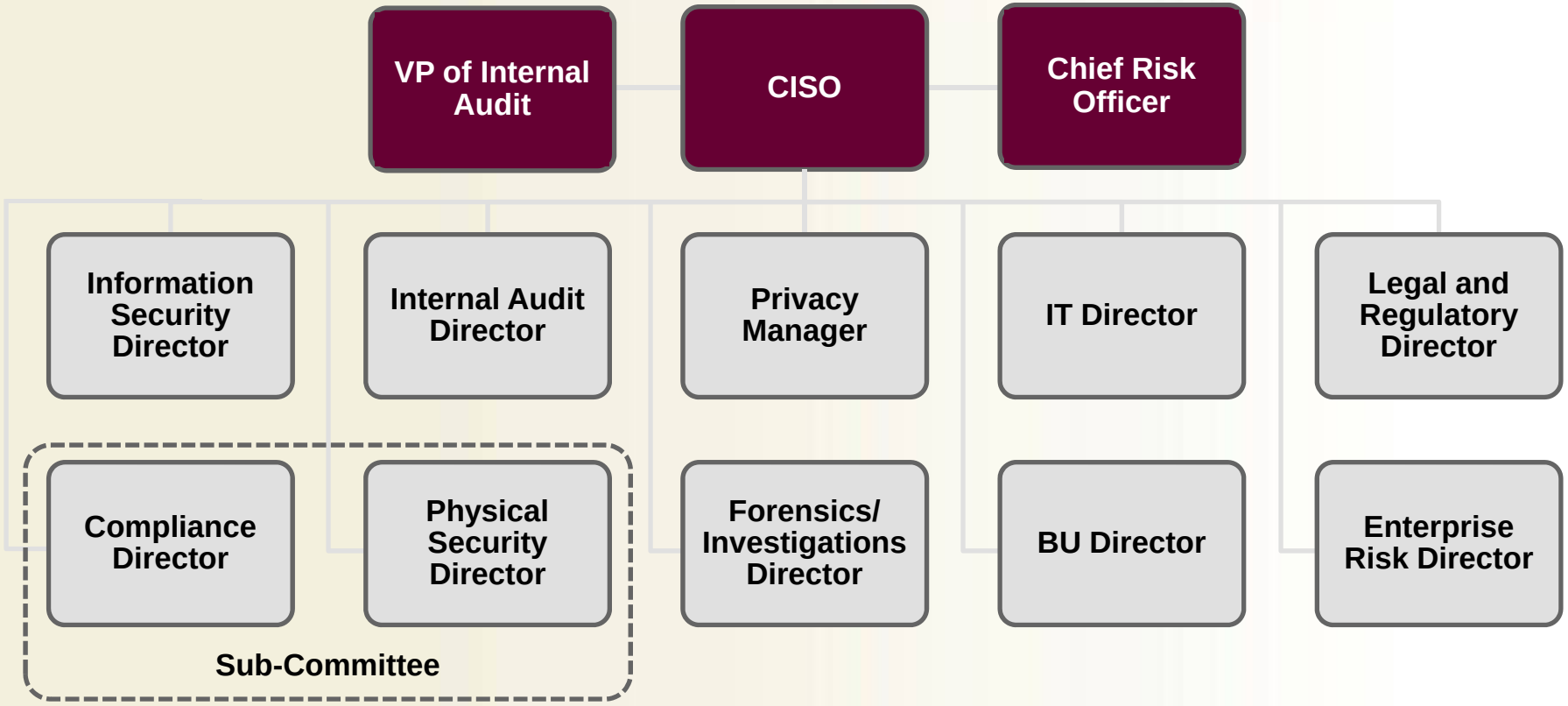
This model leverages its membership to manage risk collectively. Each member represents his/her functional area or department to bring its unique point-of-view to the group. The committee is typically high enough to make decisions and affect change, but low enough to still require executive approval for major decisions and direction.

Model Characteristics

Collaboration	*Medium - High*
Communication Style	*Mixed (Dialog and Edicts)*
Budget Authority	*Collective planning process*
Issue Focus	*Broad focus on participant issues*
Meeting Frequency	*Monthly*
Decision Authority	*Functionally aligned decisions*
Transformation Effectiveness	*Limited to specific departments*
Strategic Focus	*Limited to specific departments*

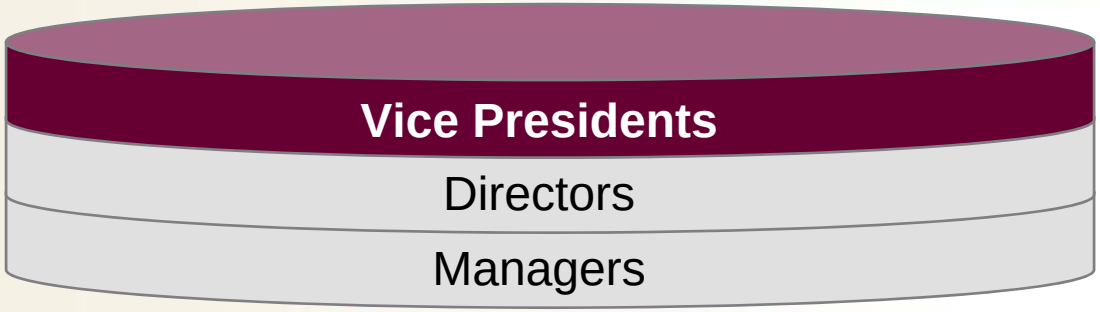
Governance Model 2: Steering Committee

Example Organizational Chart



Governance Model 3: Executive Council

1. **Working Group**
   Operational management team with execution responsibility
2. **Steering Committee**
   Leadership team that sets collaborative vision and delegates action to its teams
3. **Executive Council**
   Executive-level team that sets direction, allocates resources, and provides oversight



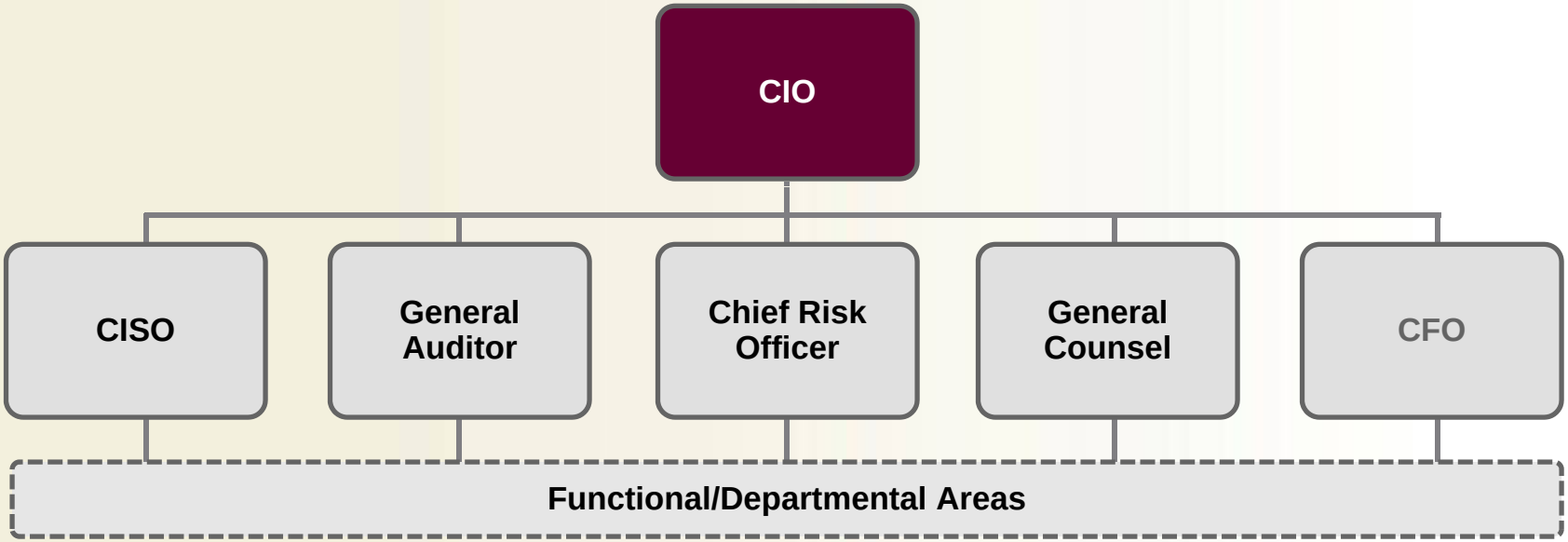
This model leverages its company executives to manage the highest risks to the enterprise. The purpose of this group is to set direction and provide feedback about the overall performance and objectives of the organization. This strategic body typically does not execute or support operational processes; rather, is more concerned with macro-level risks affecting the company and its information assets.

Model Characteristics

Collaboration	*Depends on group; typically medium*
Communication Style	*Depends on group; typically two-way*
Budget Authority	*High*
Issue Focus	*Broad, strategic issues*
Meeting Frequency	*Quarterly or bi-monthly*
Decision Authority	*Authorized to make decisions*
Transformation Effectiveness	*High*
Strategic Focus	*High*

Governance Model 3: Executive Council

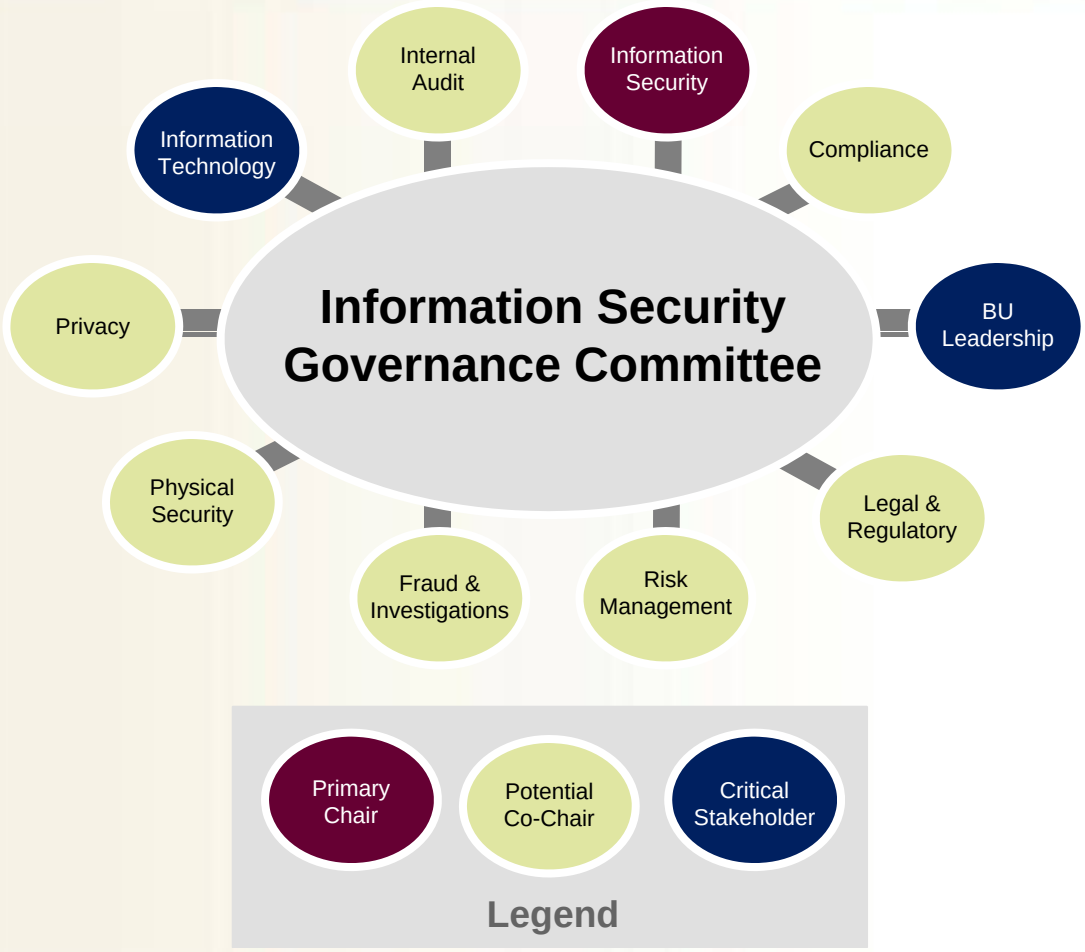
Example Organizational Chart



Member | Chair

Chairs and Leadership

- Information security should serve as a primary chair of leadership team
- Any functional area with a mission focusing on risk can serve as a potential co-chair
- Chairs are focused on:
  - Establish charter and committee mission
  - Setting agenda
  - Preparing for the meetings
  - Making assignments
  - Holding members responsible/accountable
  - Administering the meeting
  - Reporting progress/issues to executive management
- Oversee voting and tie-breaking, as needed
- Caution not to have too many chairs on the committee in order to keep focus of the committee on information security
- Some members are critical stakeholders and should not be considered chairs



How do I chose the right governance model?

- What **types of issues** do you want to discuss at your governance committee meeting?
- What is the desired **communication style** of the group?
- Will the committee have **budget authority**?
- What **input** are you looking for from the group?
- What **outcomes** will come out of the group?
- Will the group form **sub-committees** or **task forces**?
- **How often** would you like to meet?
- **To whom** will the group **report**?
- Who **reports into** this group?
- Who **resolves conflict** when consensus cannot be reached?
- Who will **chair/co-chair** the group?
- How is **independence** maintained between independent audit parties? Are there non-voting members?
- How will **progress be tracked and reported**?

Information Security Models: Empowering the Organization

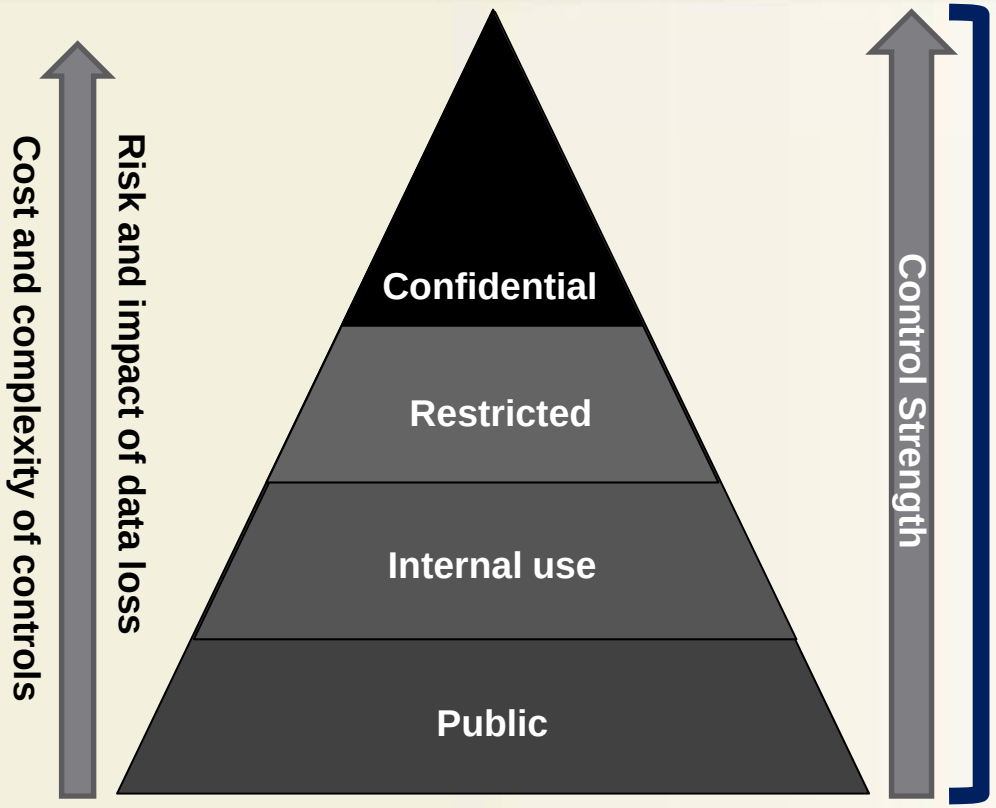
ALIGNING YOUR ORGANIZATION FOR SUCCESS

Our view on information security: It's time for a rethink…

- Traditional **security models are outdated**; need to take a new approach
- Focus on the **most important information and applications**
- **Attacks are inevitable**, so **plan and react accordingly**
- Back to basics; the **fundamentals** are still important
- **Spend wisely**; consider alternative sourcing models
- Get **governance** right; involve the Executive Leadership Team
- **Engage the business**
- **Embrace technology** rather than banning it

Information Protection

Protection Cost to Value



Targeted controls

- Encryption
- Targeted Security Awareness
- Data Loss Prevention
- Secure network spaces
- User access and appropriateness
- Full logging and monitoring
- Multifactor access controls
- Rapid response capability
- Emerging Technologies
- Virtual Desktop Infrastructure

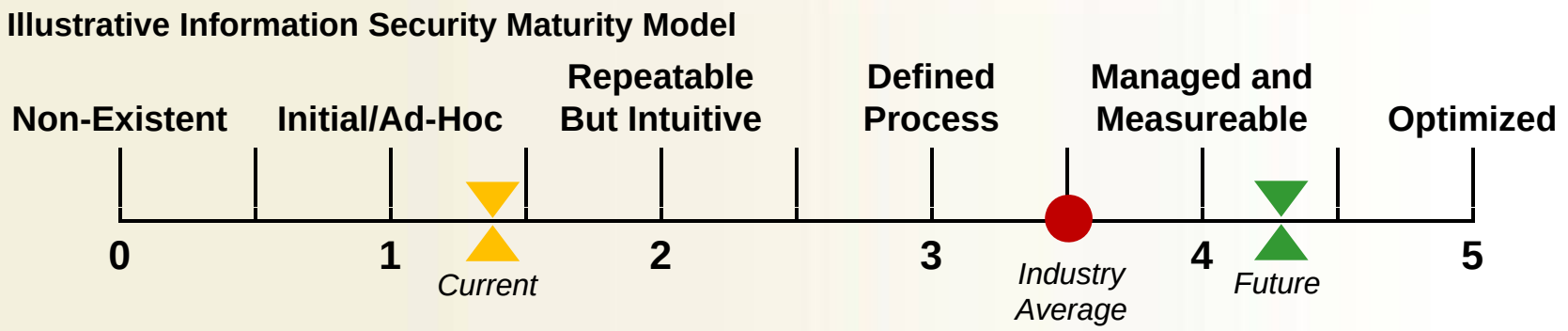
Foundation controls

- Security awareness
- Security intelligence
- SOC (Security Operations Center)
- CIRT
- Patch management
- Anti virus
- User access management
- Perimeter security
- End point security (laptop)
- Governance and oversight
- Configuration management
- Heuristic threat detection and forensics

Control strength must align to the value of the information and potential impact of loss.

Information Security Governance Maturity

Information security governance maturity can be measured on a scale and benchmarked over time.



Note: See appendix for maturity model definitions

- Information security governance maturity factors a number of inputs to determine how well a governance structure is operating
- Definitions and criteria can be adapted based on the scope and objectives of the group as outlined in the charter
- It is helpful to perform annual assessment of the governance structures to ensure it is meetings its goals and objectives and to benchmark performance over time
- Industry averages can be compared by looking at peer groups to see how well they operate their governance committees

What can you do next?

- Understand the **unique needs** of your business
- **Build consensus** around a model that works for your organization
- **Chose aspects** of the above models that work given the IT and business environment
- **Implement desired model** and **determine strategy**:
  1. Create charter
  2. Create governance framework
  3. Develop information security strategy
  4. Develop information security roadmap
  5. Prioritize initiatives for execution
  6. Select projects and allocate funding

Collaborate, Cooperate and Communicate

Thank You

Contact Information

Justin Greis
Senior Manager
Chicago, Illinois

Phone: +1 (312) 342-4202
E-Mail: justin.greis@ey.com

Matt Hynes
Senior Manager
Minneapolis, Minnesota

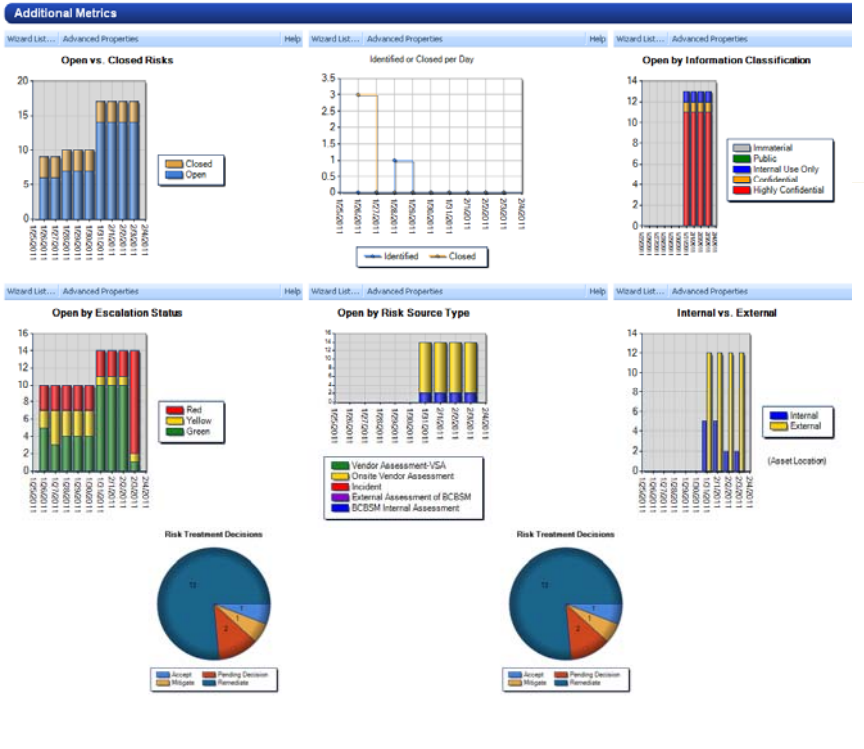
Phone: +1 (612) 229-4417
E-Mail: matt.hynes@ey.com

Information Security Models: Empowering the Organization

APPENDIX

Example Meeting Agenda and Dashboard

Example Risk Dashboard



Meeting Agenda

Introduction	CISO
Approval of Minutes	CISO
Risk Report	Enterprise Risk
1. Dashboard Review	
2. Key Metrics	
Threat Report	Information Security
Compliance and Controls	Internal Audit
Policies and Standards	Information Security
1. Policy/Standards Updates	
2. Policy Exception Review	
Project Updates	
1. Project 1	[Name]
2. Project 2	[Name]
3. Project 3	[Name]
Topic Presentation	
Open Forum	
Conclusion	

ISACA
Trust in, and value from, information systems

Example Project Status Reporting

Project Status Report

Status Report for Period Ending: DD/MM/YYYY

Summary

Project Name:		Project ID:	
Project Sponsor:		Project Start Date:	End Date:
Project Manager(s):		Weekly Executive Summary	
Status Report Distribution:			

Cost Health:	Y	<-- Select one
Scope Health:	R	<-- Select one
Schedule Health:	G	<-- Select one

Resource Health:	G	<-- Select one

Metri

#	Metric Description
1	
2	
3	
4	
5	

Project Accomplishm

	Major Accomplishments for this Reporting Period
1	
2	
3	
4	
5	

Milestone & Projec

#	Milestone Name
1.0	**Phase 1**
1.1	Milestone 1
1.2	Milestone 2
2.0	**Phase 2**
2.1	Milestone 3
2.2	Milestone 4

Issues & Risks

Issues				
#	Description	Resolution	Due Date	Status
1				
New Issues for this Reporting Period				
#	Description	Resolution	Due Date	Status
	No issues identified for this reporting period.			
Risks				
#	Description	Mitigation Plan	ID Date	Status
1				
New Risks for this Reporting Period				
#	Description	Mitigation Plan	ID Date	Status
	No risks identified for this reporting period.			

Decision Management

	Decision			Outcome/ Resolution	
#	Required Decision Description	By Whom	Date	Outcome/ Resolution Description	Date
1					

Change Management

		Dates		
#	Change Description	Requested	Response	Status
1				

Work Products/Deliverables Acceptance

		Dates		
#	Deliverable/Milestone Description	Delivered	Accepted	Status/Comments
1				
2				

Note

Lavender highlights indicate change in plan from previous status report/plan.

Prepared by:	[Name] - [Date]
Reviewed by:	[Name] - [Date]

Consistent project status reporting lays the foundation for basic information on which management decisions can be made

Example Project Health Dashboard

Workstream/Project	Overall	Cost	Scope	Schedule	Resource	Technology	Vendor
Workstream 1							
Project 1	↔ Green	↔ Green	↔ Green	↔ Green	↔ Green	↔ Green	↔ Green
Project 2	↓ Yellow	↓ Yellow	↓ Yellow	↓ Yellow	↓ Yellow	↓ Yellow	↓ Yellow
Project 3	↓ Red	↓ Red	↓ Red	↑ Yellow	↑ Yellow	↑ Yellow	↑ Yellow
Workstream 2							
Project 4	↑ Yellow	↑ Green	↓ Red	↔ Green	↑ Yellow	↓ Yellow	↔ Green
Project 5	↔ Green	↔ Green	↑ Green	↔ Green	↔ Green	↔ Green	↔ Green
Project 6	↔ Green	↔ Green	↔ Green	↔ Green	↔ Green	↔ Green	↔ Green
Workstream 3							
Project 7	↔ Green	↔ Green	↑ Green	↔ Green	↔ Green	↔ Green	↔ Green
Project 8	↔ Green	↔ Green	↑ Green	↔ Green	↔ Green	↔ Green	↔ Green
Project 9	↔ Green	↔ Green	↑ Green	↔ Green	↔ Green	↔ Green	↔ Green
Project 10	↓ Red	↓ Red	↓ Red	↔ Green	↔ Green	↔ Green	↔ Green
Project 11	↔ Green	↔ Green	↑ Green	↔ Green	↔ Green	↔ Green	↔ Green
Project 12	↔ Green	↔ Green	↑ Green	↔ Green	↔ Green	↔ Green	↔ Green
Project 13	↔ Green	↔ Green	↑ Green	↔ Green	↔ Green	↔ Green	↔ Green
Project 14	↔ Green	↔ Green	↑ Green	↔ Green	↔ Green	↔ Green	↔ Green

Health Movement Key

↑ *Milestone health has improved since last reporting period*
↓ *Milestone health has decreased since last reporting period*
↔ *Milestone health has not changed since last reporting period*

Green *On Target* Yellow *At Risk* Red *Critical Issues*

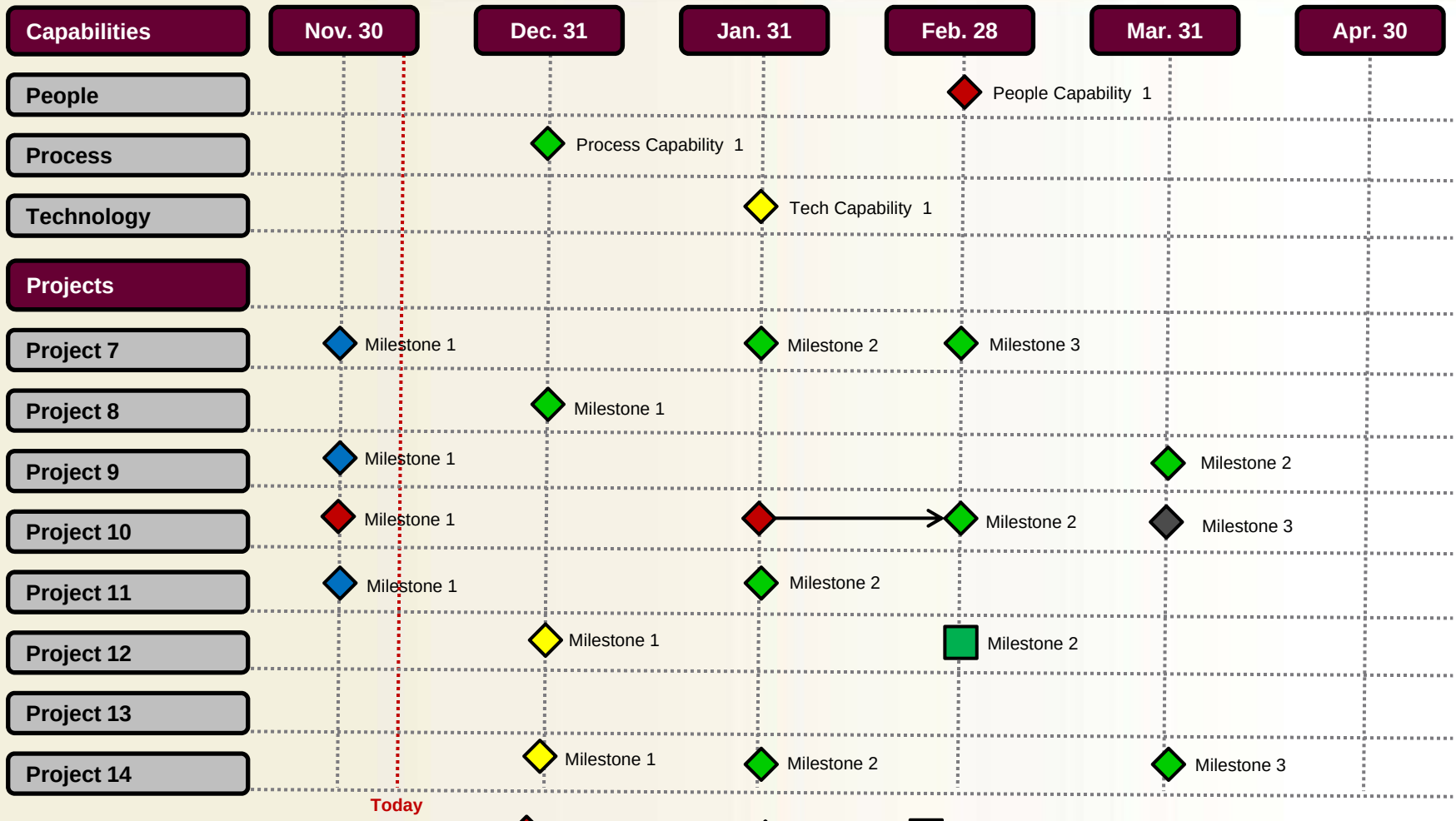
Health Status Key

Example Project Health Trend Dashboard

Workstream/Project	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7
Workstream 1							
Project 1	Green	Green	Green	Green	Green	Green	Green
Project 2	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow	Yellow
Project 3	Red	Red	Red	Yellow	Yellow	Yellow	Yellow
Workstream 2							
Project 4	Yellow	Green	Red	Green	Yellow	Yellow	Green
Project 5	Green	Green	Green	Green	Green	Green	Green
Project 6	Green	Green	Green	Green	Green	Green	Green
Workstream 3							
Project 7	Green	Green	Green	Green	Green	Green	Green
Project 8	Green	Green	Green	Green	Green	Green	Green
Project 9	Green	Green	Green	Green	Green	Green	Green
Project 10	Red	Red	Red	Green	Green	Green	Green
Project 11	Green	Green	Green	Green	Green	Green	Green
Project 12	Green	Green	Green	Green	Green	Green	Green
Project 13	Green	Green	Green	Green	Green	Green	Green
Project 14	Green	Green	Green	Green	Green	Green	Green

Health Trend Status Key Green *On Target* Yellow *At Risk* Red *Critical Issues*

Example Milestone Dashboard



Notes: [1] Footnote text, [2] Footnote text, [3] Footnote text, [4] Footnote text, [5] Footnote text, [6] Footnote text

Information Security Governance Maturity Definitions (Page 1 of 3)

- **Non-Existent (0)**
  - Risk assessment for processes and business decisions does not occur. The organization does not consider the business impacts associated with security vulnerabilities and development project uncertainties. Risk management has not been identified as relevant to acquiring IT solutions and delivering IT services.
  - The organization does not recognize the need for information security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of information security are not implemented. There is no information security reporting and no response process to information security breaches. There is a complete lack of a recognizable system security administration process.
  - There is no understanding of the risks, vulnerabilities and threats to IT operations or the impact of loss of IT services to the business. Service continuity is not considered as needing management attention.

- **Initial/Ad-Hoc (1)**
  - The organization considers IT risks in an *ad hoc manner, without following* defined processes or policies. Informal assessments of project risk take place as determined by each project.
  - The organization recognizes the need for information security, but security awareness depends on the individual. Information security is addressed on a reactive basis and is not measured. Information security breaches invoke finger-pointing responses if detected, because responsibilities are unclear. Responses to information security breaches are unpredictable.
  - Responsibilities for continuous service are informal, with limited authority. Management is becoming aware of the risks related to and the need for continuous service.

Information Security Governance Maturity Definitions (Page 2 of 3)

- **Repeatable but Intuitive (2)**
  - There is an emerging understanding that IT risks are important and need to be considered. An approach to risk assessment exists, but the process is still immature and developing.
  - Responsibilities and accountabilities for information security are assigned to an information security co-coordinator with no management authority. Security awareness is fragmented and limited. Information security information is generated, but not analyzed. Security tends to respond reactively to information security incidents and by adopting third-party offerings, without addressing the specific needs of the organization. Security policies are being developed, but inadequate skills and tools are still being used. Information security reporting is incomplete, misleading or not pertinent.
  - Responsibility for continuous service is assigned. The approaches to continuous service are fragmented. Reporting on system availability is incomplete and does not take business impact into account.

- **Defined Process (3)**
  - An organization-wide risk management policy defines when and how to conduct risk assessments. Risk assessment follows a defined process that is documented and available to all staff through training.
  - Security awareness exists and is promoted by management. Security awareness briefings have been standardized and formalized. Information security procedures are defined and fit into a structure for security policies and procedures. Responsibilities for information security are assigned, but are not consistently enforced. An information security plan exists, driving risk analysis and security solutions. Information security reporting is IT-focused, rather than business-focused. *Ad hoc intrusion testing is* performed.
  - Management communicates consistently the need for continuous service. High-availability components and system redundancy are being applied piecemeal. An inventory of critical systems and components is rigorously maintained.

Information Security Governance Maturity Definitions (Page 3 of 3)

- **Managed and Measurable (4)**
  - The assessment of risk is a standard procedure and exceptions to following the procedure would be noticed by IT management. It is likely that IT risk management is a defined management function with senior-level responsibility. Senior management and IT management have determined the levels of risk that the organization will tolerate and have standard measures for risk/return ratios.
  - Responsibilities for information security are clearly assigned, managed and enforced. Information security risk and impact analysis is consistently performed. Security policies and practices are completed, with specific security baselines. Security awareness briefings are mandatory. User identification, authentication and authorization are standardized. Security certification of staff is established. Intrusion testing is a standard and formalized process, leading to improvements. Cost-benefit analysis, supporting the implementation of security measures, is increasingly being utilized. Information security processes are coordinated with the overall organization security function. Information security reporting is linked to business objectives.
  - Responsibilities and standards for continuous service are enforced. System redundancy practices, including use of high-availability components, are consistently deployed.

- **Optimized (5)**
  - Risk management has developed to the stage that a structured, organization-wide process is enforced, followed regularly and managed well.
  - Information security is a joint responsibility of business and IT management and is integrated with enterprise security business objectives. Information security requirements are clearly defined, optimized and included in a verified security plan. Security functions are integrated with applications at the design stage and end users are increasingly accountable for managing security. Information security reporting provides early warning of changing and emerging risk, using automated active monitoring approaches for critical systems. Incidents are promptly addressed, with formalized incident response procedures supported by automated tools.
  - Periodic security assessments evaluate the effectiveness of implementation of the security plan. Information on new threats and vulnerabilities is systematically collected and analyzed, and adequate mitigating controls are promptly communicated and implemented. Intrusion testing, root cause analysis of security incidents and proactive identification of risk are the basis for continuous improvements. Security processes and technologies are integrated organization-wide.
  - Continuous service plans and business continuity plans are integrated, aligned and routinely maintained. Buy-in for continuous service needs is secured from vendors and major suppliers.

Example Governance Model Charter

Purpose

The Information Security Steering Committee (ISSC) assists the Chief Information Security Officer in the oversight of [COMPANY]'s Security Program.

The steering committee provides a means for stakeholders representing diverse perspectives to engage in constructive discussion of [COMPANY]'s information security issues. It provides input into [COMPANY]'s information security strategy and operations. The [COMPANY]'s recommendations will be a significant input into implementing information security strategy, policy, and standards. The ISSC will contribute to the goal of cost-effective use of information security resources and technology to achieve prudent and proportional security of information while enabling [COMPANY]'s business strategy. It is responsible for promoting a culture of appropriate information security practices.

Responsibilities

The Information Security Steering Committee shall:

- Assure alignment of security policies, standards and practices with the business
- Review and approve Information Security Policies, Standards or Guidelines for final approval by [COMPANY] Executive Leadership.
- Assure alignment of the Information Security strategy with the long-term business strategy.
- Identify information security risks and recommend potential solutions.
- Propose topics or issues to be addressed by [COMPANY] Information Security.
- Assure that business and IT initiatives include appropriate information security considerations.
- Provide input into priorities for the allocation of information security resources.
- Review quarterly reports from the CISO of ongoing security monitoring and assessments.
- Consider any sensitive security concerns in ad hoc executive sessions.
- Escalate issues, as required, to the Corporate Compliance Committee, for consideration and resolution.

Example Governance Model Charter

Accountability

The committee will make recommendations to the CISO. It will make recommendations to [COMPANY] executives or other committees as necessary. Committee members serve as a liaison between their respective functional area and Information Security.

Meeting Frequency

The ISCC will meet at least monthly at a regularly scheduled time. Ad hoc meetings will be held as needed.

Attendance

Members of the ISCC are expected to attend all meetings as reasonably as possible. A quorum consisting of 51% of voting members is required to conduct business. Personal attendance is strongly encouraged; however, members may participate by telephone if out of town. Members may send an alternant to represent them at the meeting only if attendance in person or by telephone is not possible due to unforeseen circumstances.

Membership

The success of the ISCC depends on an objective and business-oriented understanding of [COMPANY]'s Information Security issues. An effective mix of members who understand the business operations and can challenge Information Security assumptions is likely to increase the ISCC's success in achieving its goals.

The Chief Information Security Officer will serve as leader and chair of the group. Members will include representatives of selected management with diverse responsibilities. Recommended voting membership shall include, but not be limited to the following:

– [List membership here]

Individually, group members are responsible to bring information security issues to the group as appropriate and to promote a culture that encourages appropriate information security practices.

Minutes and Agenda

The leader will distribute an agenda and any pre-read materials one week in advance of the meeting. The leader will be responsible for maintaining minutes and assignment logs and will determine whether to assign staff support.