CYS 403 – Security Risk Management, Governance and Control

Intended Learning Outcomes

- CLO 1: Evaluate the issues and concerns indicative to protecting information, systems and users.

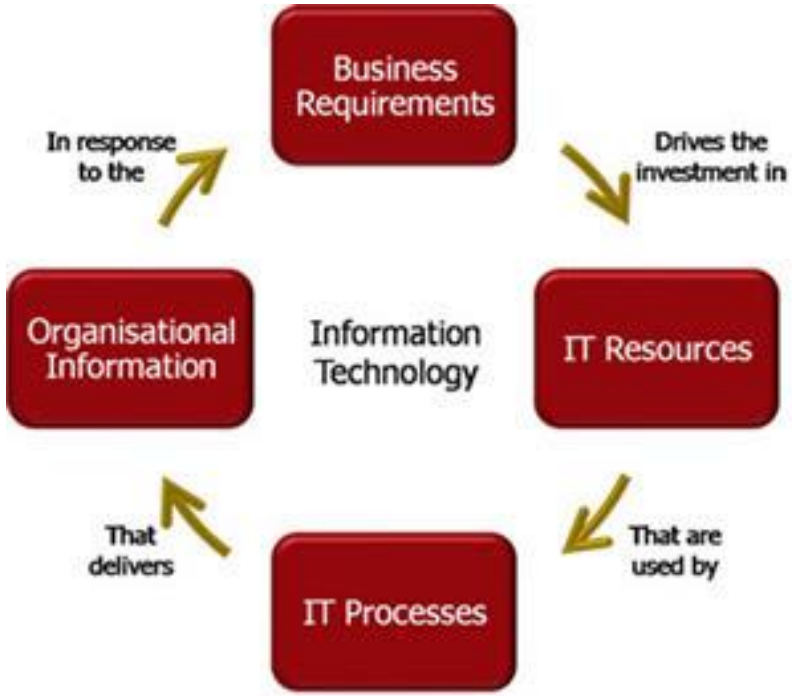
Agenda

- Introduction to Risks in the organization
- Risks in IT context.
- Security as an Investment
- Business-Driven Security Program
- Governance and Control.
- Information Security Policy Basics

Risks in Business

Why Care About Cyber Risk?

- Enterprises are dependent on automation and integration.
- Need to cross IT silos of risk management.
- Important to integrate with existing levels of risk management practices.



IT's Business Focus. Adopted from CobiT®

Why Care About Cyber Risk?

- 91% of Board Members at the most vulnerable companies can't interpret a cybersecurity report. (Nasdaq report)
- The knowledge gap between executives and IT must be bridged.
  - First, identify why cyber risk should be a **business priority** for any executive.
  - The goal isn't to turn CEOs, CFOs and other business leaders into technologists, but for businesses to **adapt to the digital landscape** in which they exist.
  - requires effort from both management and IT to find **middle ground in a relationship** that has often been difficult

Why Care About Cyber Risk?

- Risk and value are two sides of the same coin.
- Risk is inherent to all enterprises.
- BUT, Enterprises need to ensure that opportunities for value creation are not missed by trying to eliminate all risk.

Manage and Capitalize on Risk

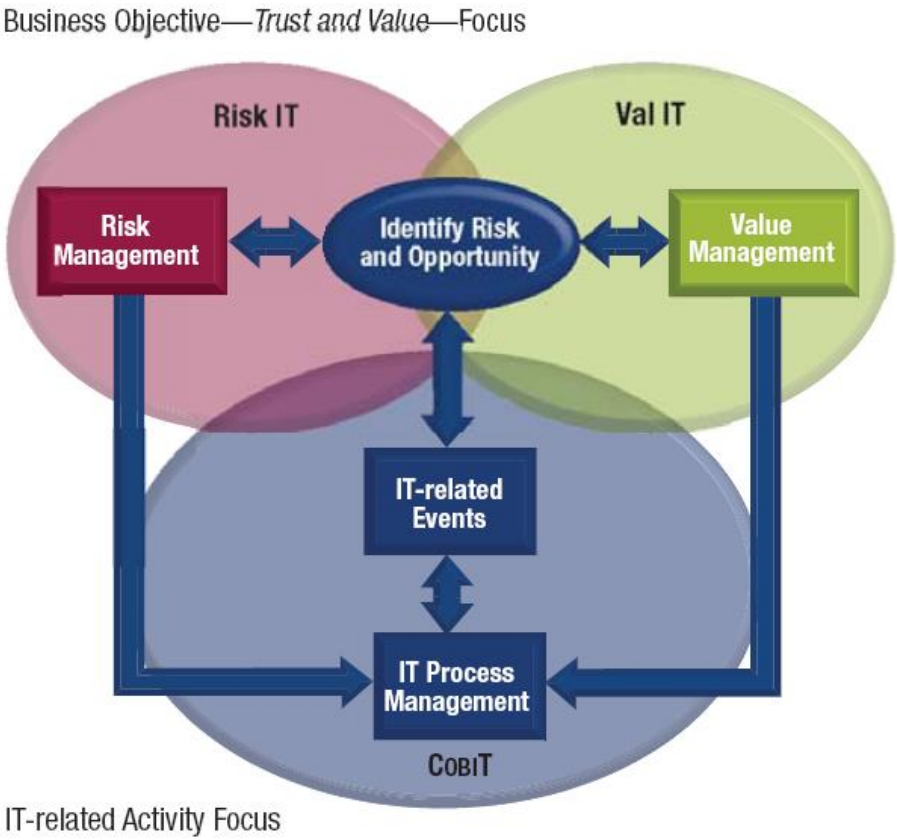
- Enterprises achieve return by taking risks.
- Some try to eliminate the very risks that drive profit.
- Guidance was needed on how to *manage* risk effectively.

IT Risk and IT Value

- VAL IT: is a governance framework that can be used to create business value from IT investments.
- RISK IT: provides an end-to-end, comprehensive view of all risks related to the use of information technology (IT).
- COBIT: is to provide management and business process owners with an information technology (IT) governance model that helps in delivering value from IT and understanding and managing the risks associated with IT.

Risk IT Extends Val IT and COBIT

Risk IT complements and extends COBIT and Val IT to make a more *complete* IT governance guidance resource.

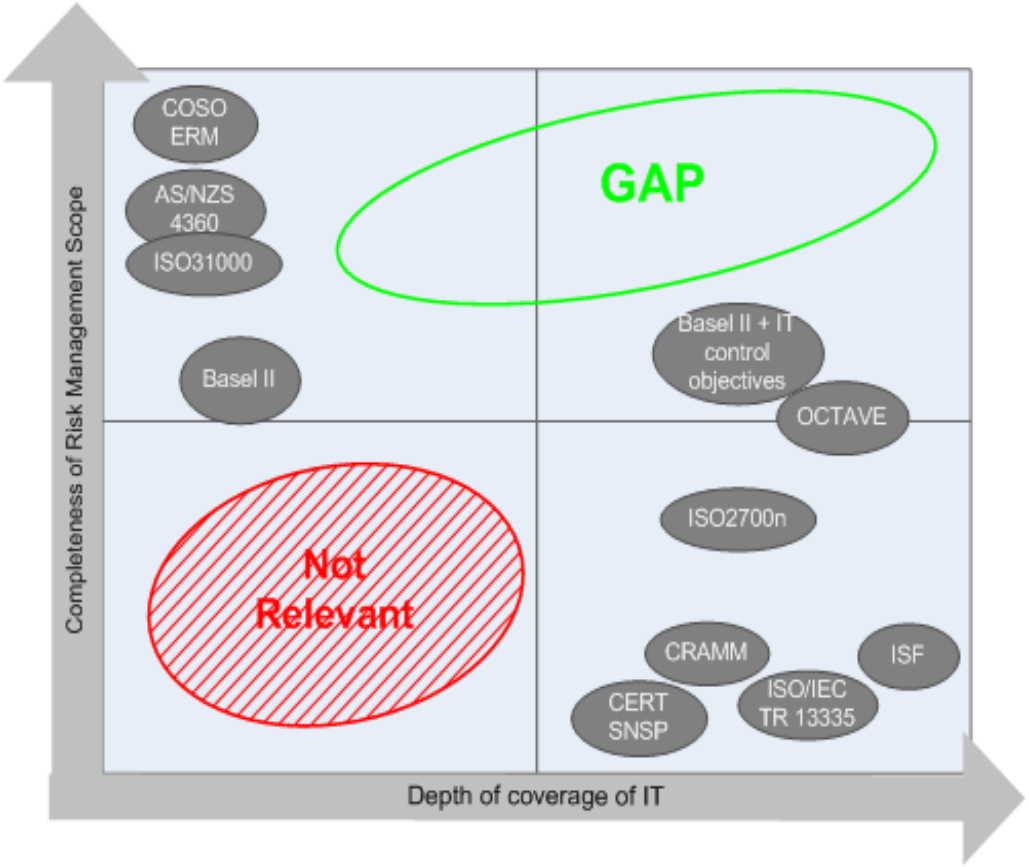


Where IT Risk Fits In

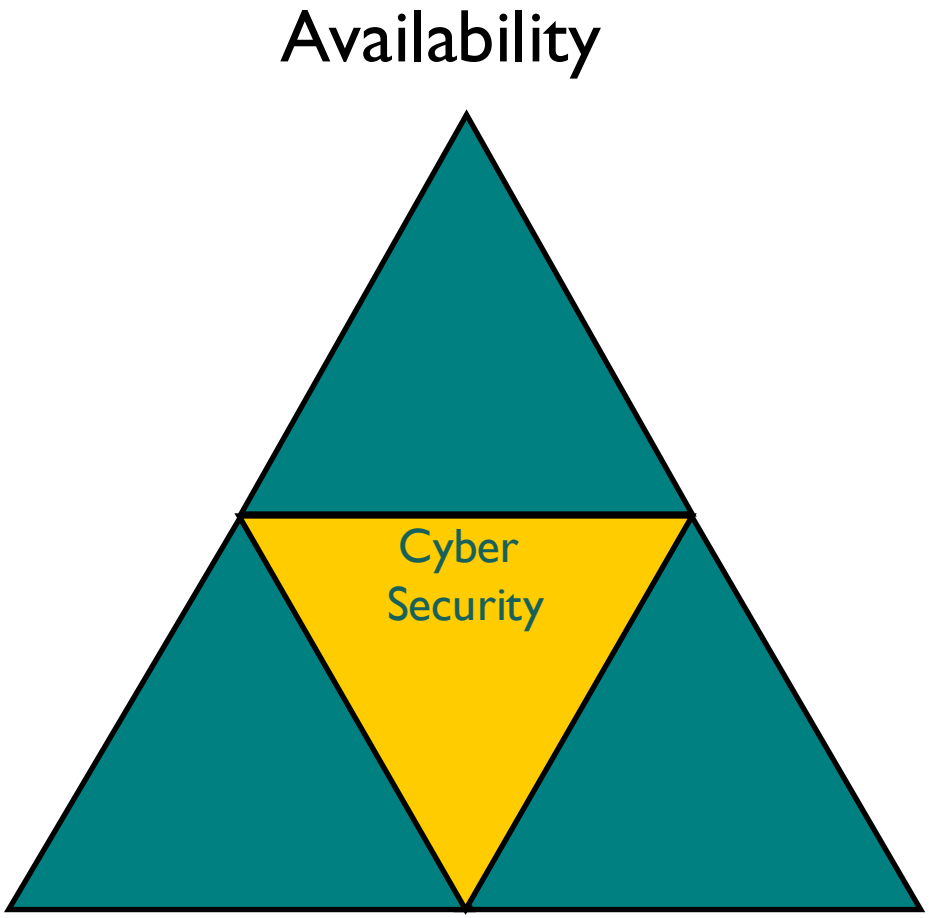
Standards and frameworks are available, but are either too:

- Generic enterprise risk management-oriented
- IT security-oriented

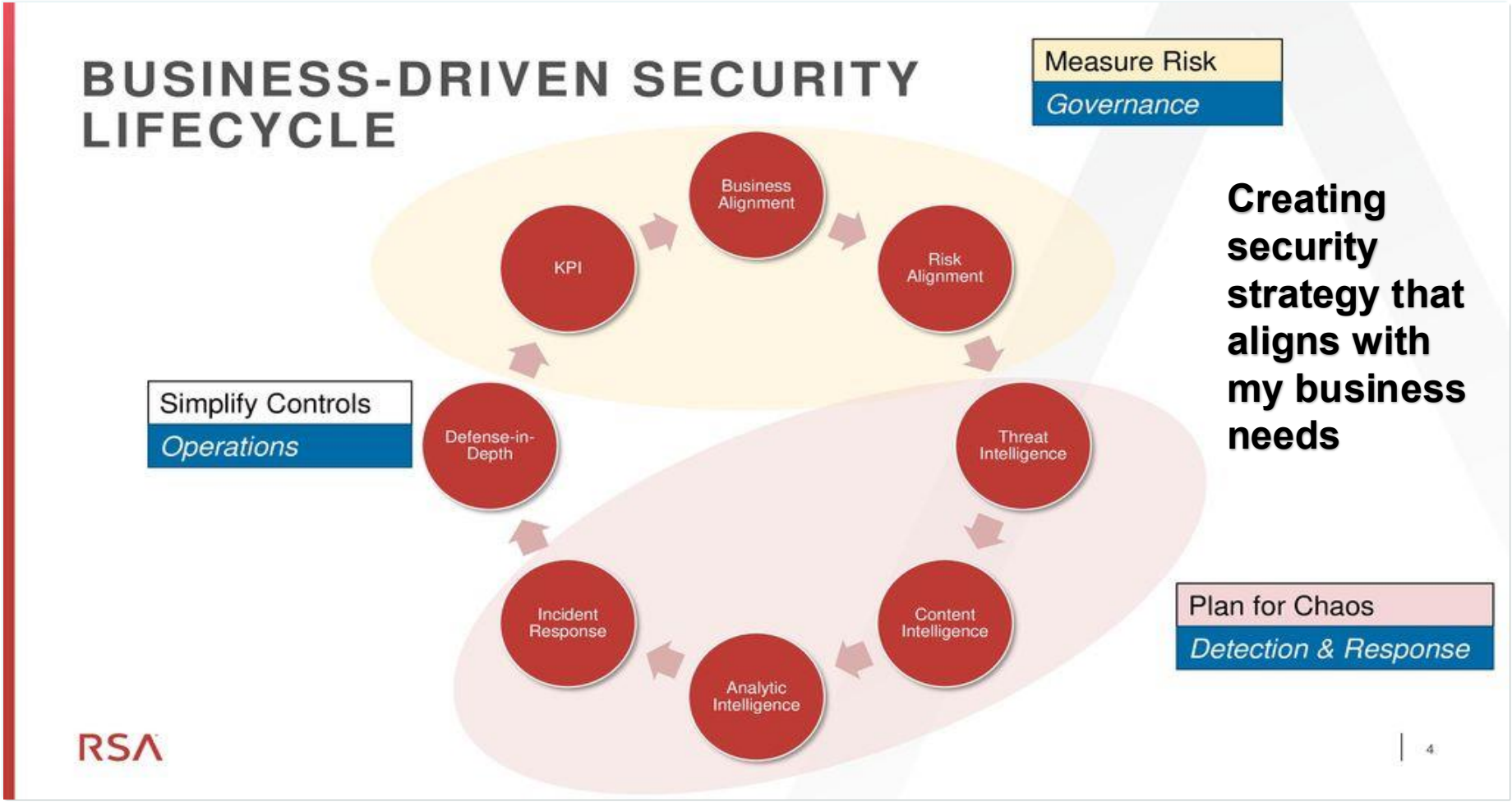
No comprehensive cyber security framework available—until now.



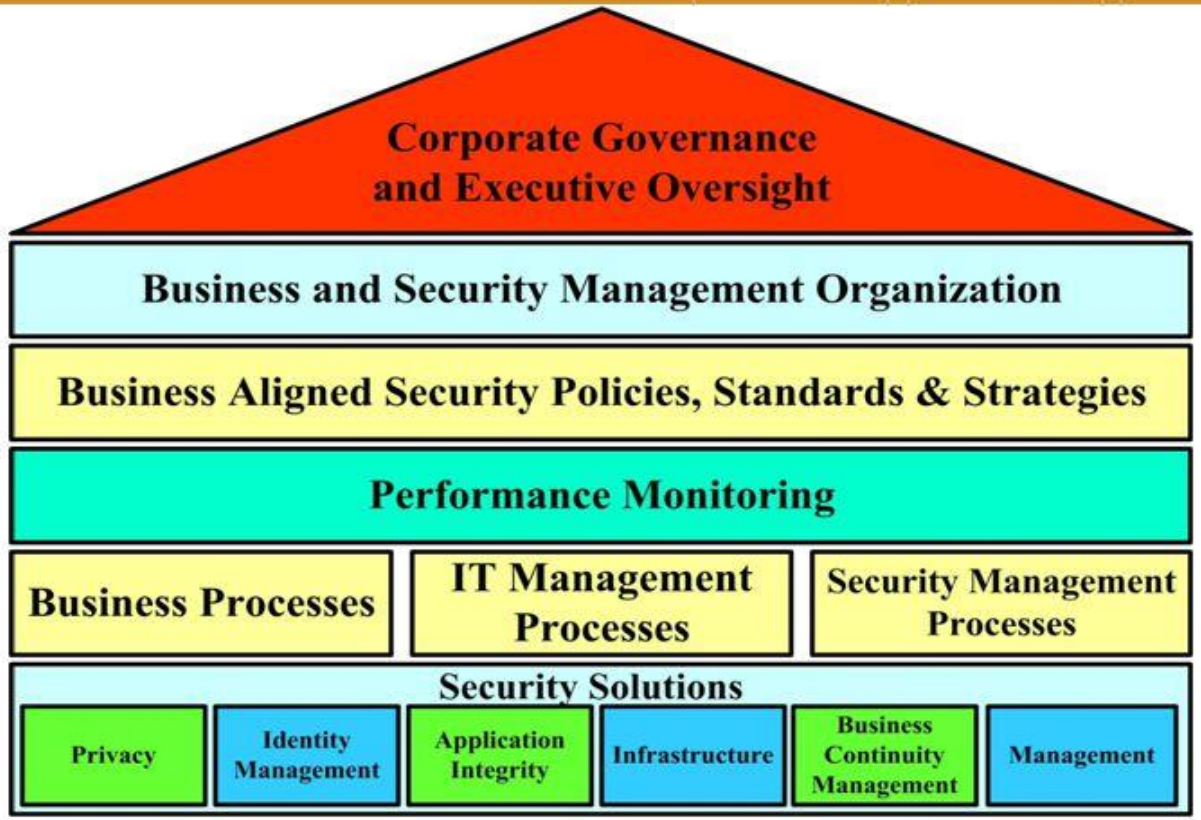
Cybersecurity TRIAD



Business-Driven Security

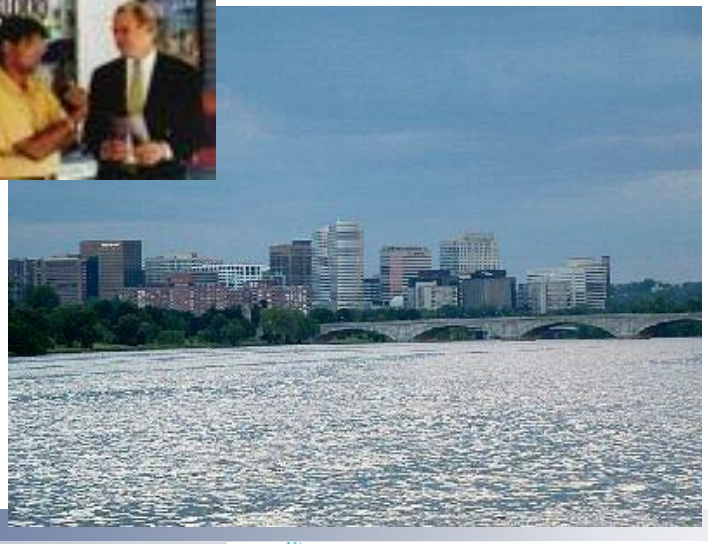


IT Security Requirements Structure



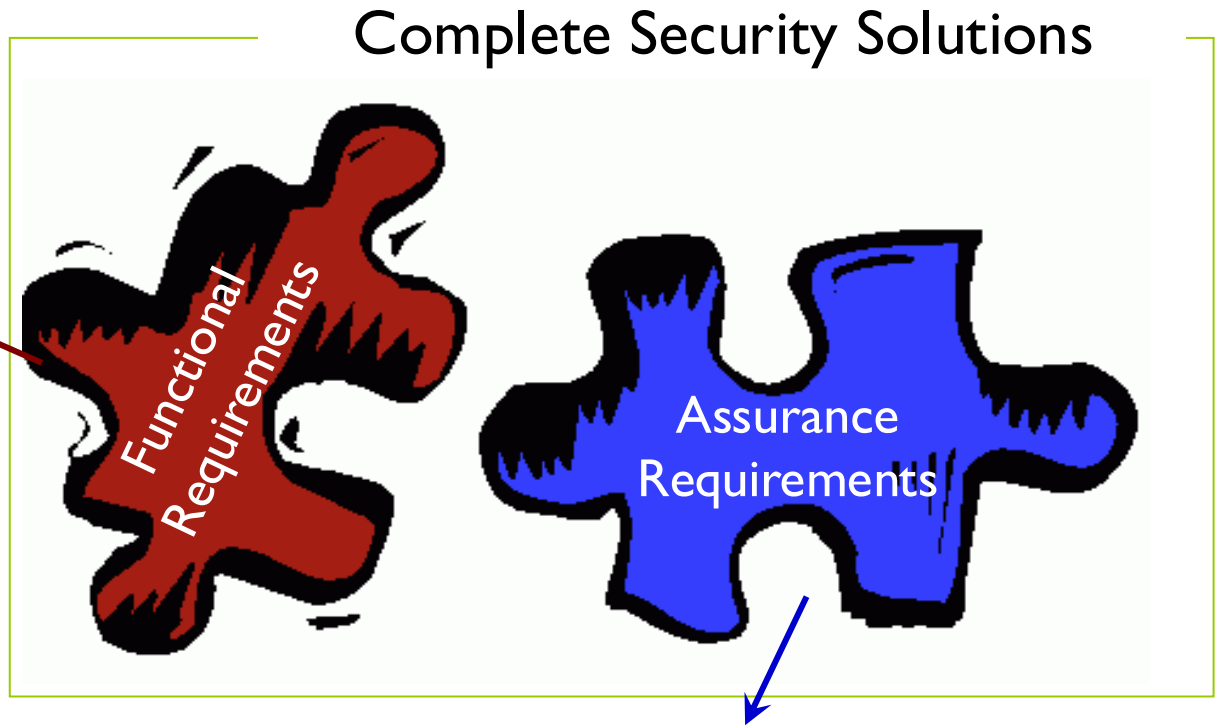
Organizational & Business Requirements

- Focus on the mission of the organization
- Each type of organization has differing security requirements
- Security must make sense and be cost effective



Cybersecurity Security Solutions

- Defines the security behavior of the control measure
- Selected based on risk management process.



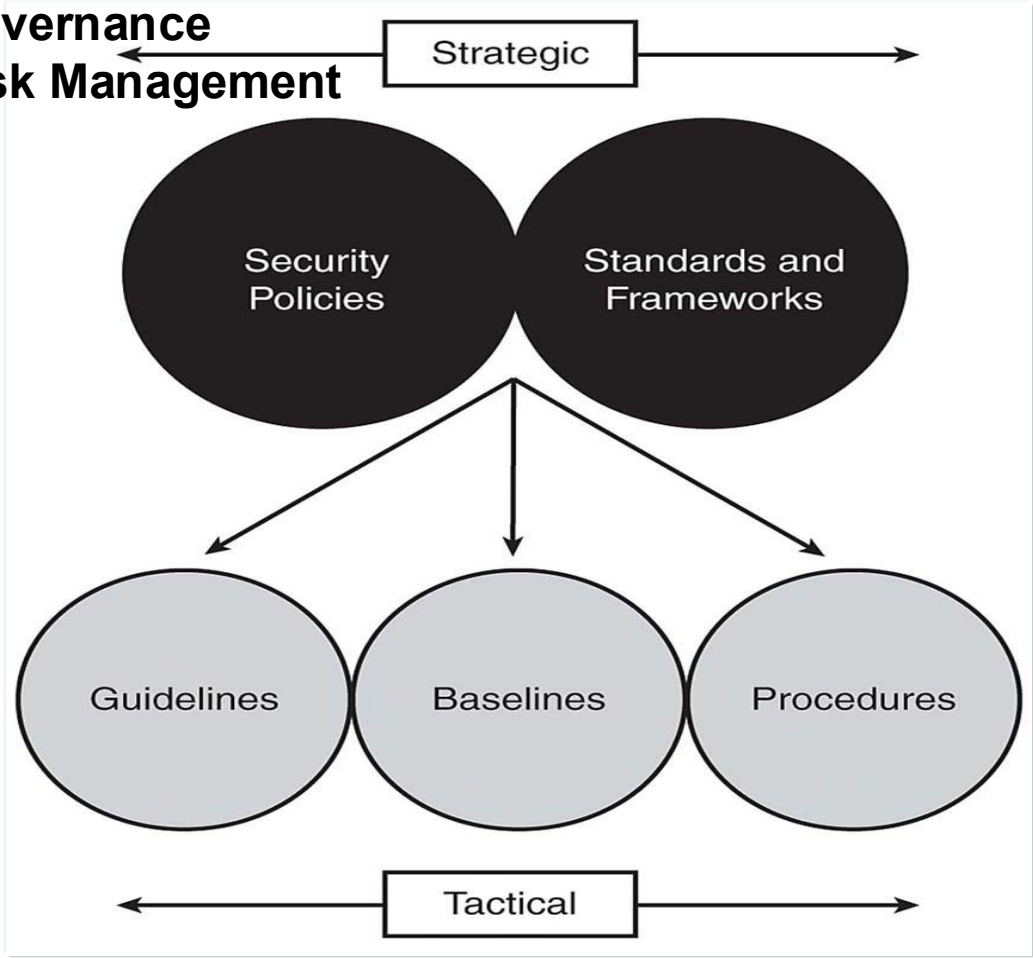
- **Provides confidence that security function is performing as expected**
- **Critical part of the security program**

Cybersecurity Management

- everything an organization does to protect its information systems and computer networks from cyber attacks, intrusions, malware and various types of data breaches.

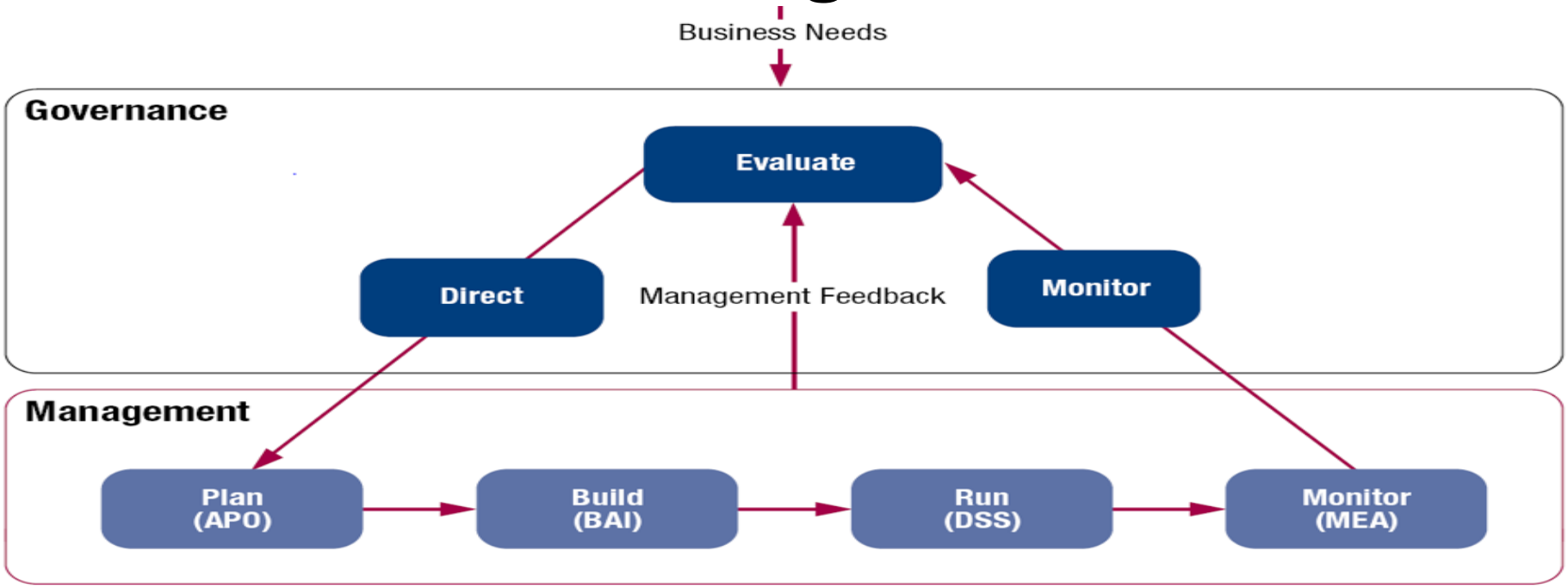
Cybersecurity Management

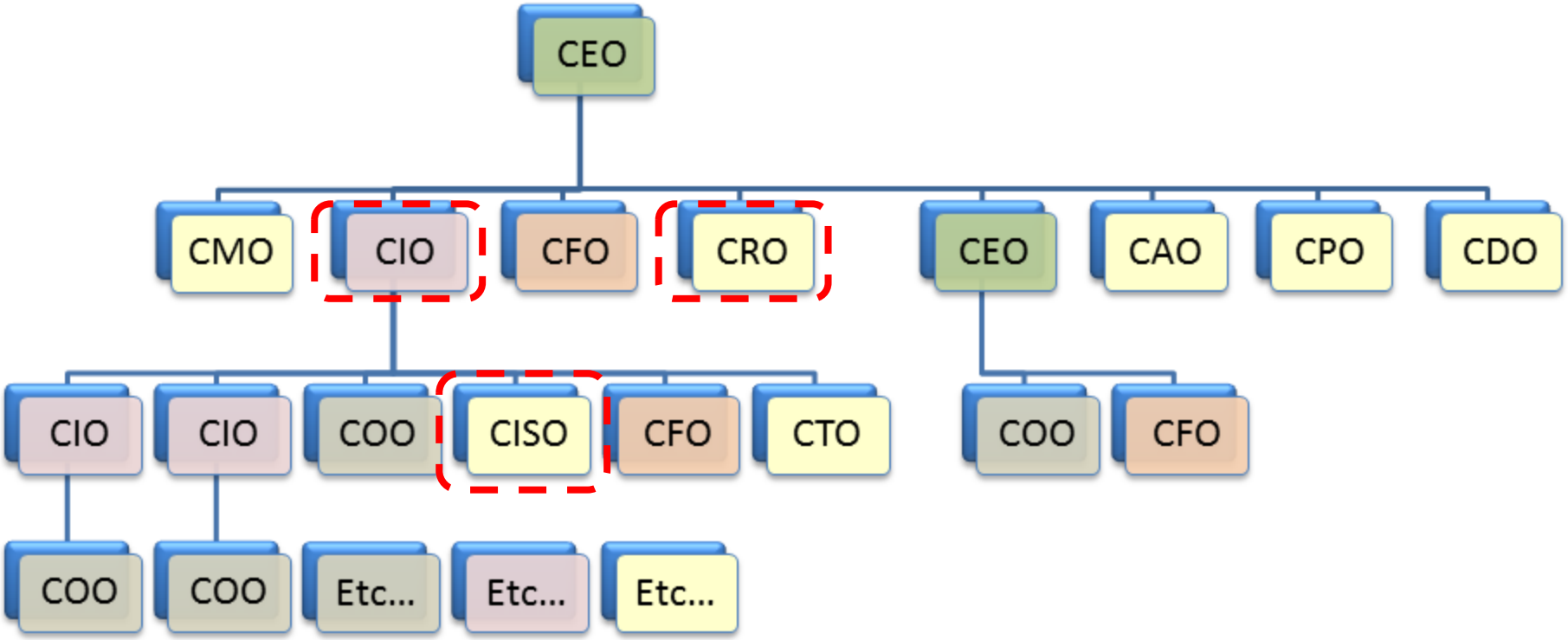
- Cybersecurity Management includes:
  - **Governance**
  - **Risk Management**



Cybersecurity Governance

- Cybersecurity Governance is an integral Part of Overall Corporate Governance
- Governance vs. management





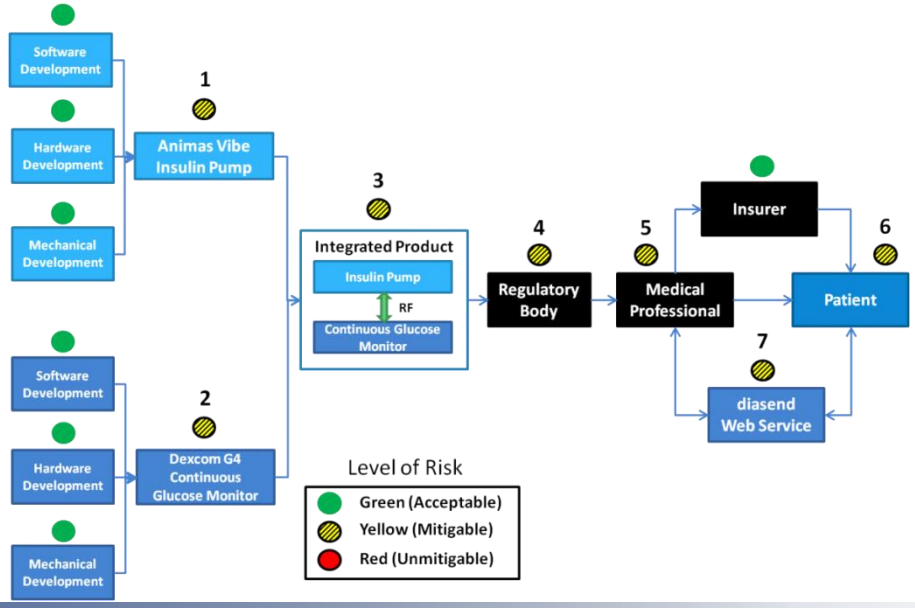
- CEO – Chief Executive Office
- COO – Chief Operating Officer
- CISO – Chief Information Security Officer
- CRO – Chief Risk Officer
- CDO – Chief Digital Officer
- CAO – Chief Admin Officer
- CFO – Chief Finance Officer
- CPO – Chief Procurement Officer
- CTO – Chief Technology Officer
- CMO – Chief Market Officer

Cybersecurity Governance

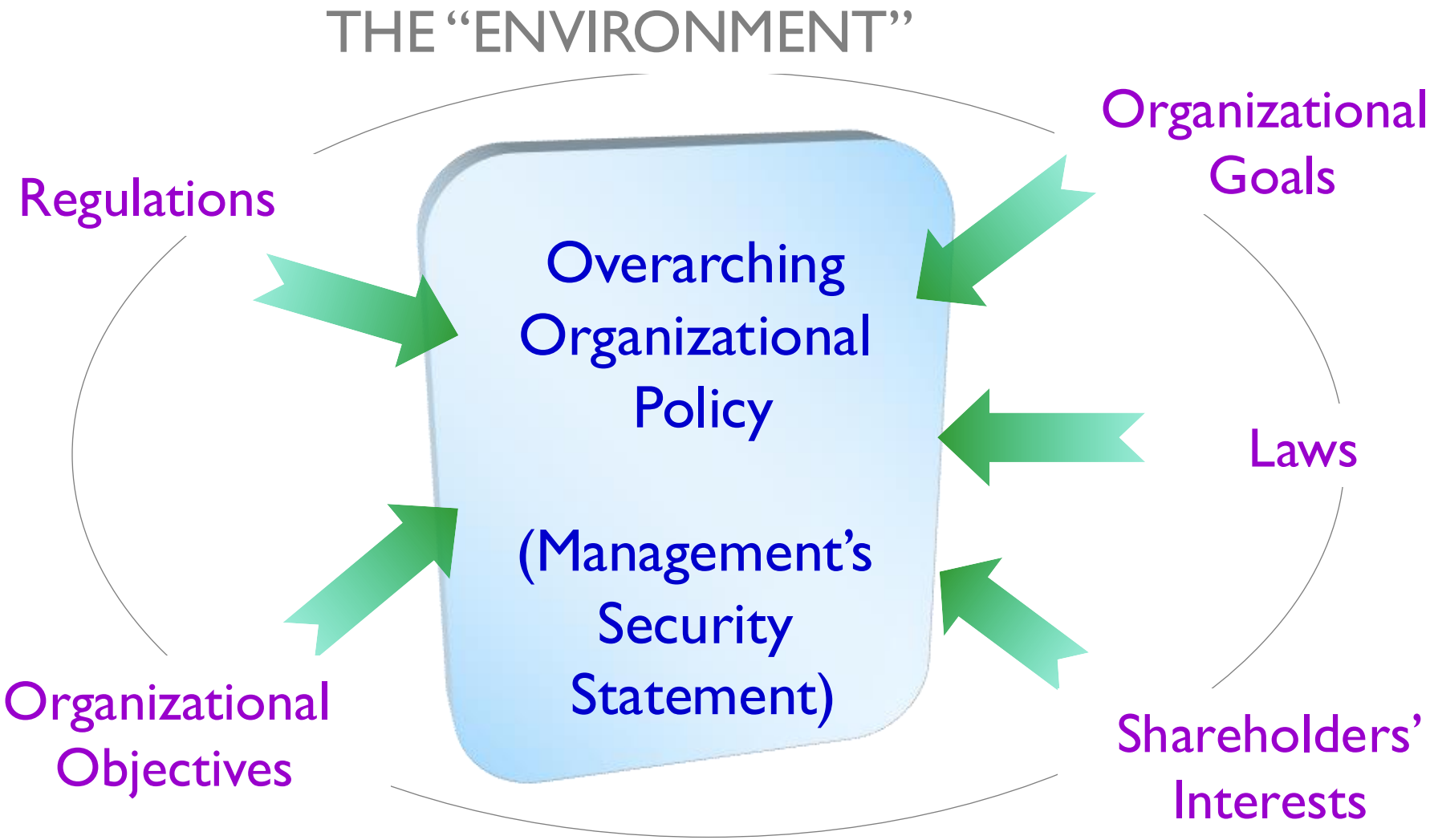
- Fully integrated into overall risk analysis/management.
- Ensure that IT infrastructure:
  - Meets all requirements.
  - Supports the strategies and objectives of the company.
  - Includes service level agreements [if outsourced].

Security Blueprints

- Provide a structure for organizing requirements and solutions.
  - Ensure that security is considered holistically.
- To identify and design security requirements



Policy Overview



Policy overview

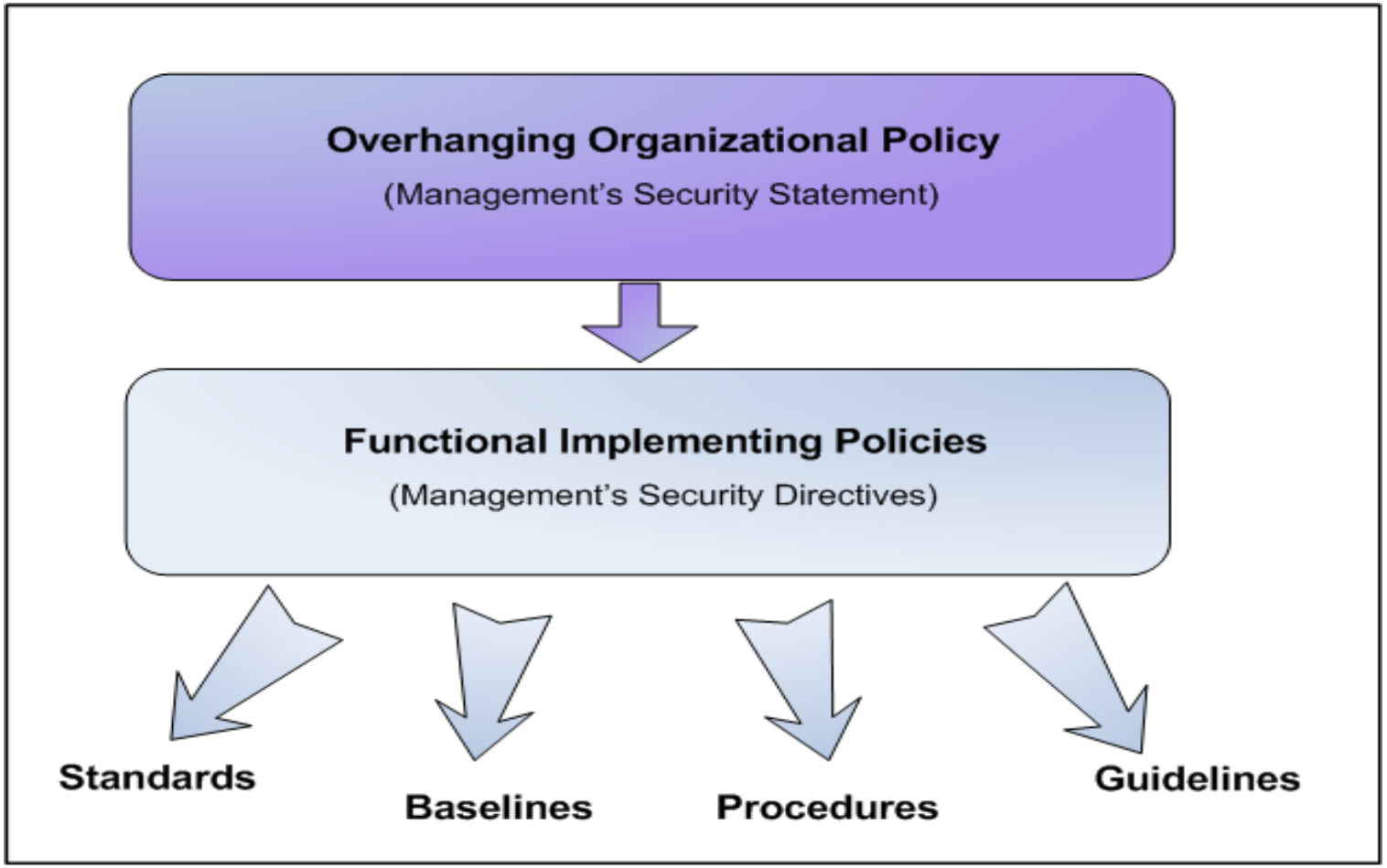


Figure 2

Security Statement Example

SECURITY POLICY STATEMENT

Kerry Logistics is committed to protecting the company's employees, properties, information, reputation and customer's assets from potential threats in the supply chain. This policy is guided by the company's basic core values, code of conduct, business ethics and supply chain security standards, and it fashions the way we operate throughout the supply chain. All security activities must adhere to the general principles laid down below:

- All employees and contractors must always be aware of and take responsibility for the security aspects of the company's business activities;
- Threats analysis and risk evaluations should be conducted on a regular basis;
- Security procedures and guidelines should be seamlessly integrated with business activities;
- "Incident prevention" must be the first priority;
- Preparedness response plans must be developed and tested to deal with assessed risks rapidly and effectively;
- Security measures and procedures must be subject to regular inspections, validations and verifications by security auditor so as to maintain high security standards for Kerry Logistics' operations world-wide;
- The level of professionalism, knowledge and integrity of staff involved in security matters must be tightly controlled;
- Appropriate training plans, customer screening, recruitment, contracting and termination procedures must be established and implemented;
- All incidents, including security breaches and irregularities must be reported and recorded. Corrective action should be taken and followed up through regular verifications to improve the overall security standard.

This policy has been approved by the Global Executive Committee. It will be reviewed, and if necessary revised, annually to keep up to date and will be released on our company website. We welcome interested parties' comments on the enforcement of the policy and the policy itself.

Policy Infrastructure

1. High level policies interpreted into functional policies.
2. Functional polices derived from overarching policy and create the foundation for procedures, standards, and baselines to accomplish the objectives
3. Polices gain credibility by top management buy-in.

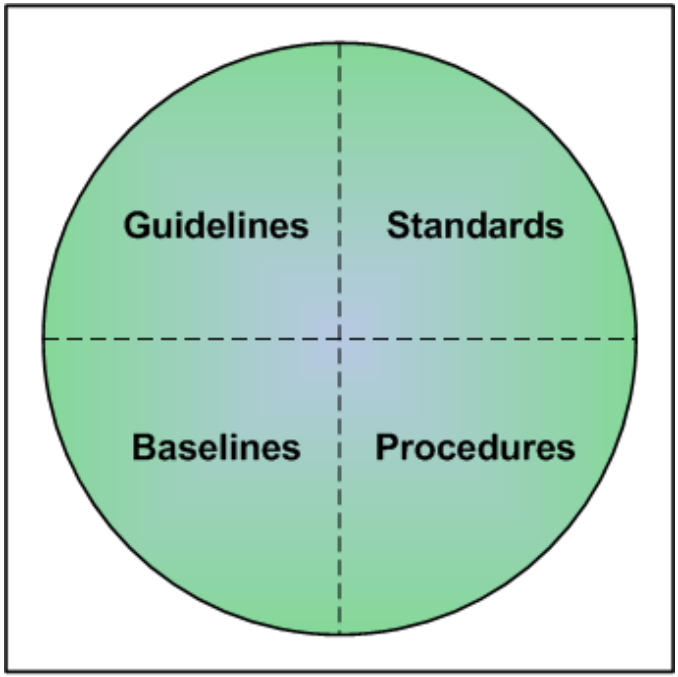


Figure 3

Examples of Functional Policies

1. Data classification
2. Certification and accreditation
3. Access control
4. Outsourcing
5. Remote access
6. Acceptable mail and Internet usage
7. Privacy
8. Dissemination control
9. Sharing control

Internet usage policy sample

What shouldn't I do?

You must not

- Access, display or download material from any web sites containing material which may be considered offensive
- Use the internet for illegal or unlawful purposes
- Access or use on-line gaming sites
- Download, distribute or store music, video, film or other copyright material
- Access commercial web-based e-mail sites and portals such as Hotmail and Yahoo Mail

Policy Implementation

- Standards, procedures, baselines, and guidelines turn management objectives and goals [functional policies] into enforceable actions for employees.

Standards and procedure

1. **Standards (local):** Adoption of common hardware and software mechanism and products throughout the enterprise.
   Examples: Desktop, Anti-Virus, Firewall
2. **Procedures:** step by step actions that *must* be followed to accomplish a task.
3. **Guidelines:** recommendations for product implementations, procurement and planning, etc.
   Examples: ISO17799, Common Criteria, ITIL

Security Baselines

Benchmarks: to ensure that a minimum level of security configuration is provided across implementations and systems.

- establish consistent implementation of security mechanisms.
- Platform unique

  Examples:

  - VPN Setup,
  - IDS Configuration,
  - Password rules

Three Levels of security planning

1. Strategic: long term
   - Focus on high-level, long-range organizational requirements
     - Example: overall security policy
2. Tactical: medium-term
   - Focus on events that affect all the organization
     - Example: functional plans
3. Operational: short-term
   - Very specific action to react with a certain incident (Fight fires at the keyboard level), directly affecting how the organization accomplishes its objectives.

Risk Management

جامعة الامير سلطان
PRINCE SULTAN
UNIVERSITY
1998

“Security Transcends Technology”