



IM/IT Security Program

Managing IM/IT Security Risks

Mark Scherling



Agenda

- Shifting the security perspective
- Shifting the security approach
- Security Program
 - Structure
 - Processes

Security is here to stay

- Security is:
 - Not a one-shot, silver bullet
 - Not only technology
 - Lives in an organizational and operational context
 - A collaborative effort that draws on organizational capabilities
 - Must be aligned with the organization's strategic drivers and business objectives
 - Risk assessment and risk management must drive decision making

Shifting the security perspective

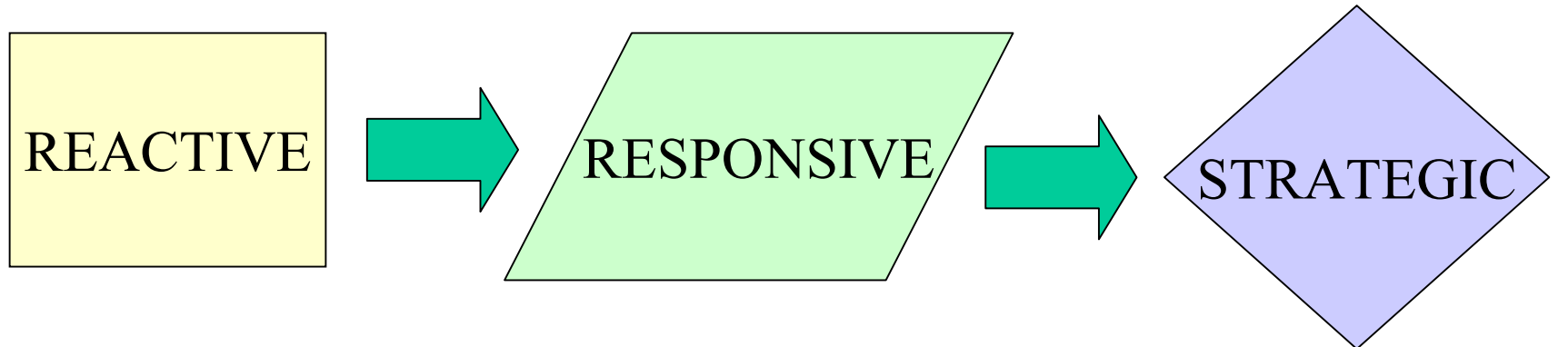
- FROM

- Technical problem
- Owned by IT
- Expense-driven
- Practice centric
- Survivability

- TO

- Business problem
- Owned by organization
- Investment
- Process-centric
- Resiliency

Shifting the security approach (1)



- Immeasurable
- Poor documentation
- Not repeatable
- Vulnerability driven
- Technical problem
- Rewards for individual skills and heroics

- Some measurements
- Some documented processes
- Some repeatability
- Vulnerability managed
- Impact to business is recognized

- Measured
- Documented
- Repeatable
- Business problem
- Organization Ownership
- Rewards for consistency and discipline

Shifting the security approach (2)

- Requires consideration of two important concepts:
 - Defining and reaching the organization's "secure state"
 - Maintaining "adequate" security

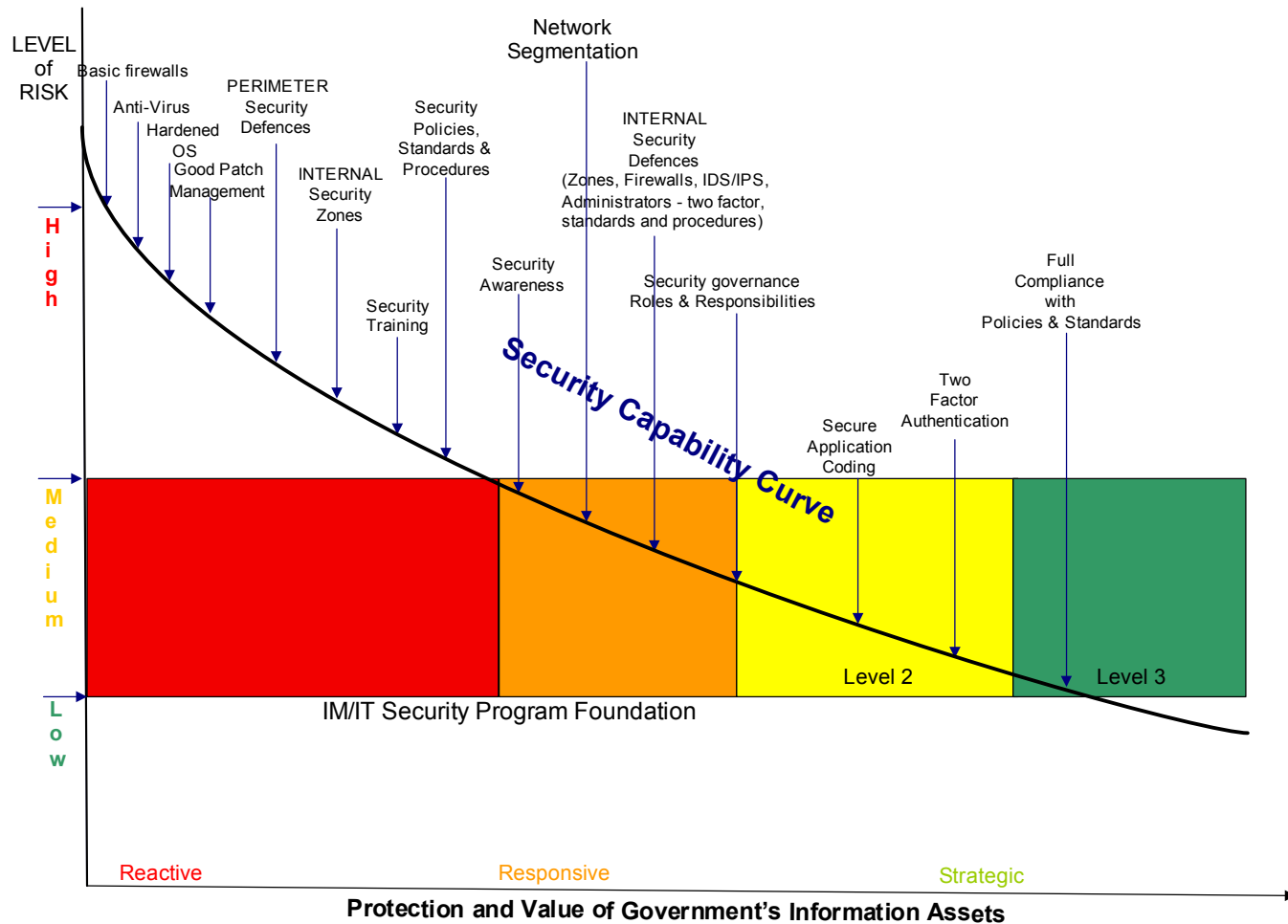
Defining the “secure state”

- All organization’s security requirements are met
- Factor of an organization’s drivers and mission
- Changes as the organization’s risk environment changes
- Balance between security efforts and security requirements: “adequate security”

Adequate security

- Equilibrium between requirements and efforts, asset value and controls
- Efforts in context of organization's drivers, not best practices or compliance
- Decision-making for protection strategies based on risk, drivers
- Avoidance of costs and constraints of over-protection
- Residual risk is in line with organization's risk tolerance

Security Capability Model



Version 1.0
December 17, 2004




**Office of the Chief Information Officer
Ministry of Management Services**

IM/IT Security Program

“Objective is to enhance trust and protect the interests of all parties relying on government managed information and information systems from harm resulting from failures of availability, integrity and confidentiality.”

Defining Govt's secure state

- Protection of government's information and information systems
- Automated security systems that handle 98% of all security events including the identification of threats,
- Managed response processes to handle security incidents when automated security systems fail
- Appropriate metrics to help manage risks



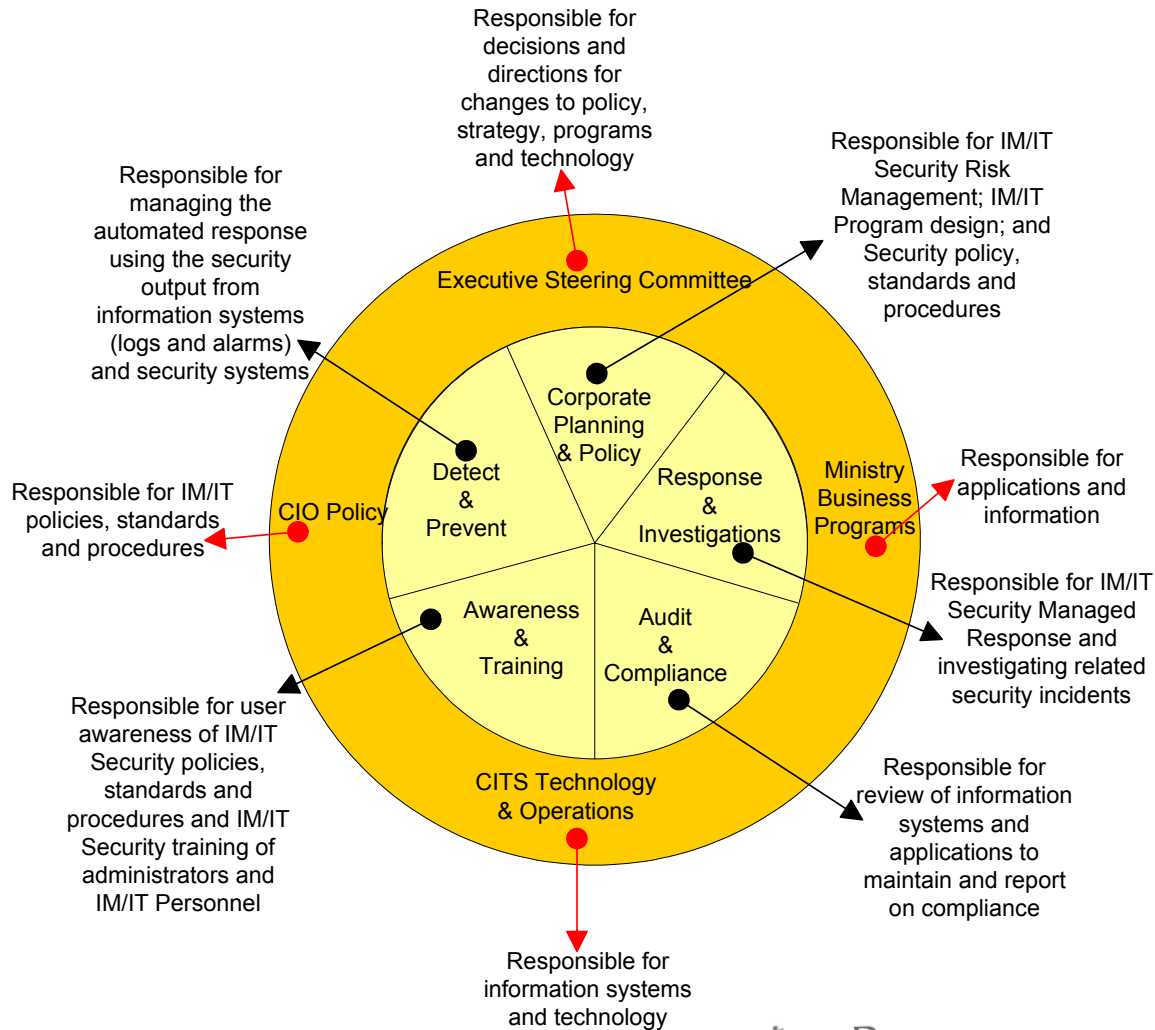
Defining “adequate” security for Government

- Critical assets and infrastructure identified and protected in accordance to the value of the information and information systems
- Risk management approach to security
- Integrated with business requirements
- Metrics reported to senior management

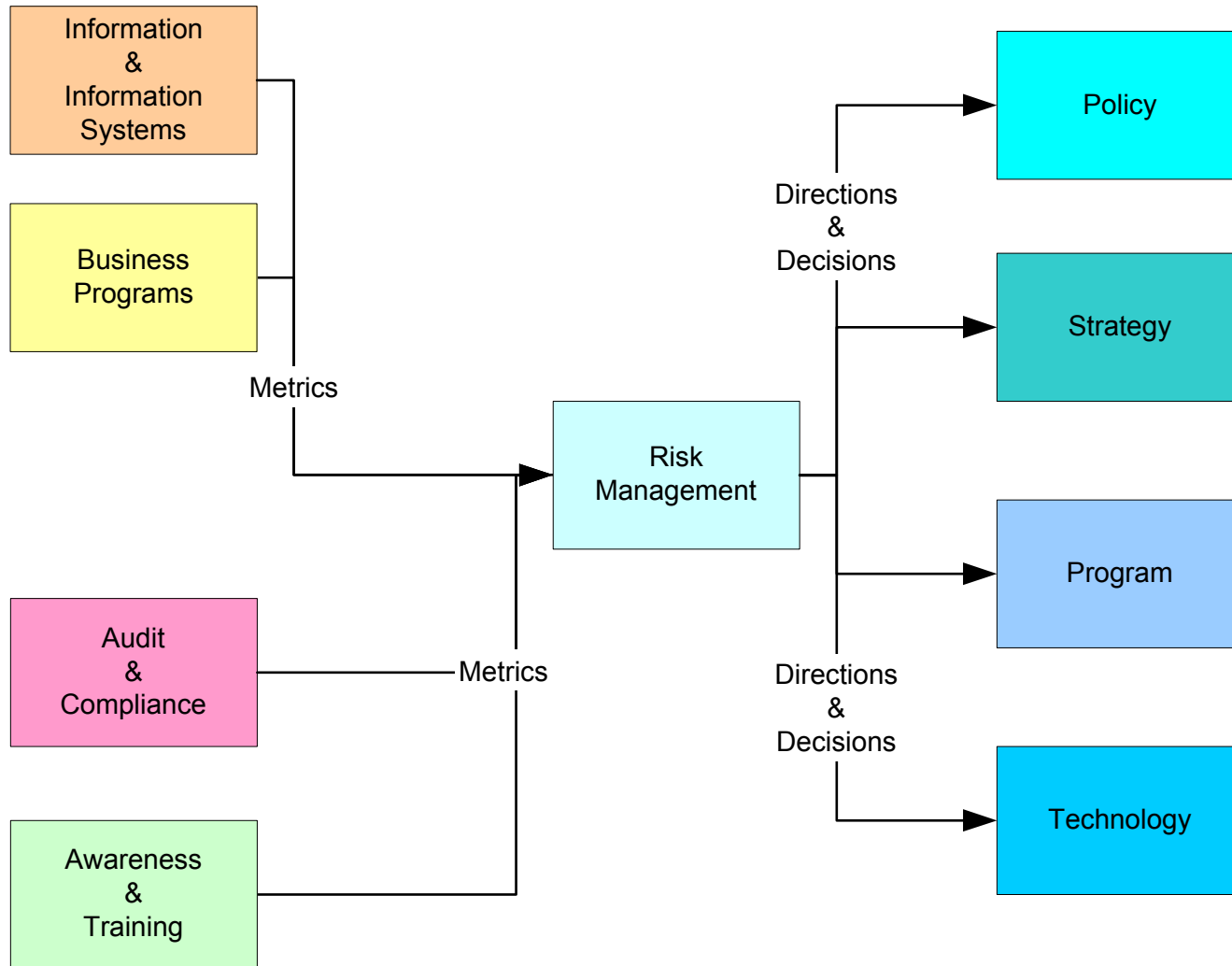
Principles

- Security principles based on GASSP:
 - Address the following properties of information and Information Systems
 - Confidentiality – disclosure of information only to authorized persons, entities and processes
 - Integrity – preservation of accuracy and completeness of information
 - Availability – information and information systems being accessible and usable
 - Pervasive Principles
 - Accountability; Awareness; Ethics; Multidisciplinary; Separation of Duties; Least Privilege

IM/IT Security Program Structure



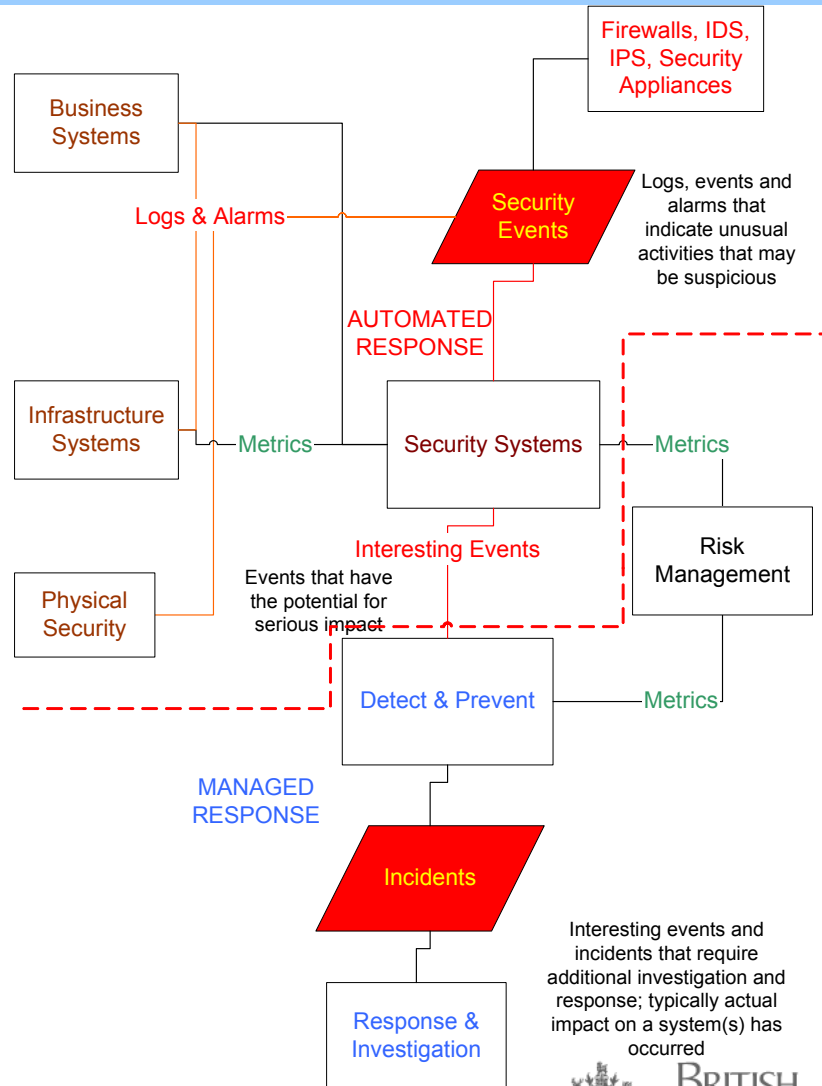
Security Program Processes



Processes Overview

- Automated Response – aggregates event information and determines response based on pre-determined rules
- Managed Response – events analysis and incident management
- Audit and compliance – review of information systems and users to ensure conformance to policy
- Awareness and training – providing security information to users and technical persons
- Risk Management – aggregates security information and business risks reporting to Executive Steering Committee on security metrics and recommendations for strategic and policy changes
- Directions and Decisions (Executive Steering Committee) – information and metrics reported to senior decision makers for decisions and directions

Automated Response Process



Automated Response

- Integrated Security Systems includes:
 - Firewalls, IDS/IPS, anti-virus, vulnerability management, Security Information Management, Analysis engines, appliances, etc.
 - Logs from Infrastructure and Business systems
- **Detect and Prevent**
 - Automated response based on DARI (Detect, Analysis , Response Infrastructure)
 - Exceptions (incidents) provides input into **Managed Response** process
- Proper Configuration and Vulnerability Management
- Metrics include system vulnerability reports, Anti-virus reports, security events

Managed Response

- Review and respond to incidents reported by automated response systems
- Manage incidents and investigations resulting from compromises in confidentiality, integrity or availability of information and information systems
- Recover from compromises
- Metrics include reports on incidents responded to and investigated

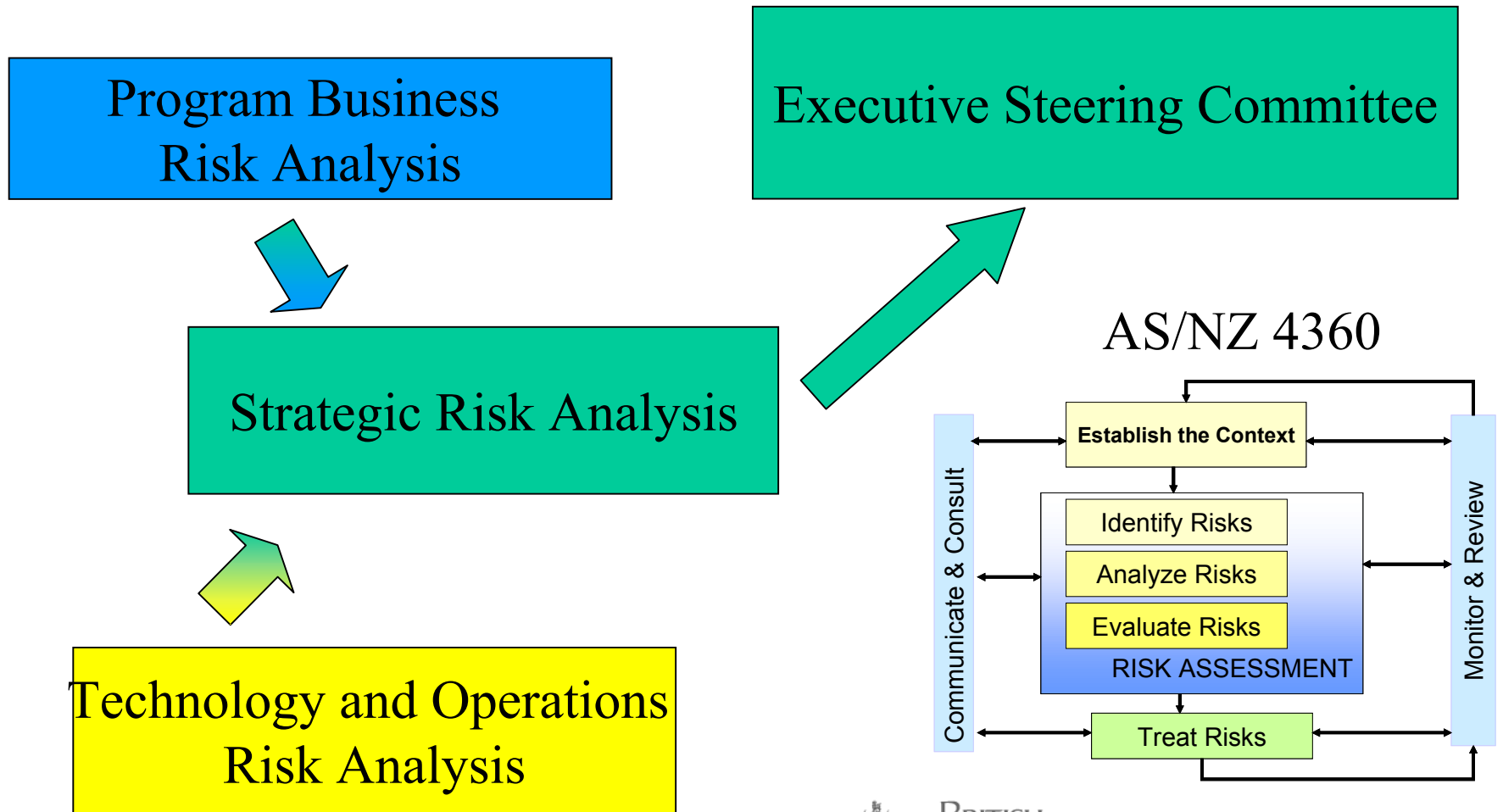
Audit and Compliance

- Audit and/or review of processes and systems
- Determine compliance
- Provide input into awareness and training requirements based on audits
- Inputs from business, infrastructure, physical security, personnel security
- Metrics include compliance with policies

Awareness and Training

- User and management security awareness
 - Ongoing user and management awareness sessions
 - Metrics will be based on the percentage of users and management aware of security policies
- Training
 - Security training for administrators, programmers, designers
 - Metrics will be based on the percentage of employees with security responsibilities who have received security training

Risk Management Process



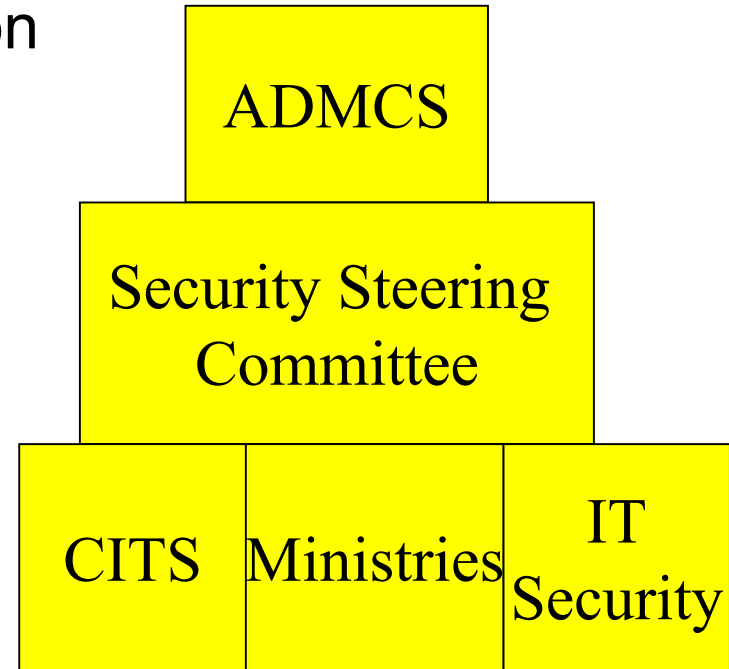
Risk Management Process (2)

- Cross government representation
 - Management and technical representation
 - Business input
 - Technology and operations input
 - Aggregated metrics and recommendations output to executive steering committee
- Managed by **Corporate Planning and Policy**

Executive Steering Committee

Provides direction and decisions regarding IM/IT security based on risk analysis and security metrics.

Comprised of CIO, EFOs



Strategy

- Provides direction and coordination for the program
- Align security with business requirements to provide adequate security of information and information systems
- Develop, maintain and measure a baseline security standard across government that reflects the secure state
- Determines changes to the program and processes
- Use referenced standards where possible and practical (i.e. ISO 17799, COBIT, GASSP, ITIL)

Policies, standards & procedures

- Policies based on ISO 17799-2005
 - Sets the tone of what must be done
- Standards
 - Supporting the policies with detailed direction
- Procedures
 - Supporting the standards, how to do it
- Changes based on direction from Executive Steering Committee

Security Program Summary

- Organizational ownership not an IT problem
- Risk managed at organization level
- Segmented network with critical assets protected at a level commensurate with the value of the asset
- Integrated security response solution including automated response and managed response
- Metrics that reflect security program and the value the program is bringing to government

Questions?

Mark Scherling
Security Program Manager
(250) 356-2860

Email: mark.scherling@gems6.gov.bc.ca