# Institute of Forensic Science
# M.Tech. Cyber Security & Incident Response

**(*Semester* – MCSIR SI P1: Introduction to Cyber Security)**


# Introduction to Risk Analysis, Risk Assessment & Risk Mitigation

**Source:**
**1. Jamie Sharp CISSP, Security Advisor, Microsoft Australia**
**2. *CISSP CIB*, January 2012 (4.17.14 Rev. 13)**
**3. Notes CS498IA – Information Assurance**

# Syllabus

## MCSIR SI P1: Introduction to Cyber Security- Unit 5

- Introduction to Risk Analysis,
- Risk Assessment,
- Risk Mitigation
- Need for BCP,
- Overview of BCP Life Cycle,
- Identifying and Selecting Business Continuity Strategies,
- DR Strategies,
- Plans for Business Resumption,
- BCM Program Management and
- System Audit.

# Organization of Sessions

**Session 1**

- **Introduction to Risk Analysis,**
- **Risk Assessment,**
- **Risk Mitigation**

**Session 2**

- **Need for BCP,**
- **Overview of BCP Life Cycle,**
- **Identifying and Selecting Business Continuity Strategies,**
- **DR Strategies,**
- **Plans for Business Resumption,**

**Session 3**

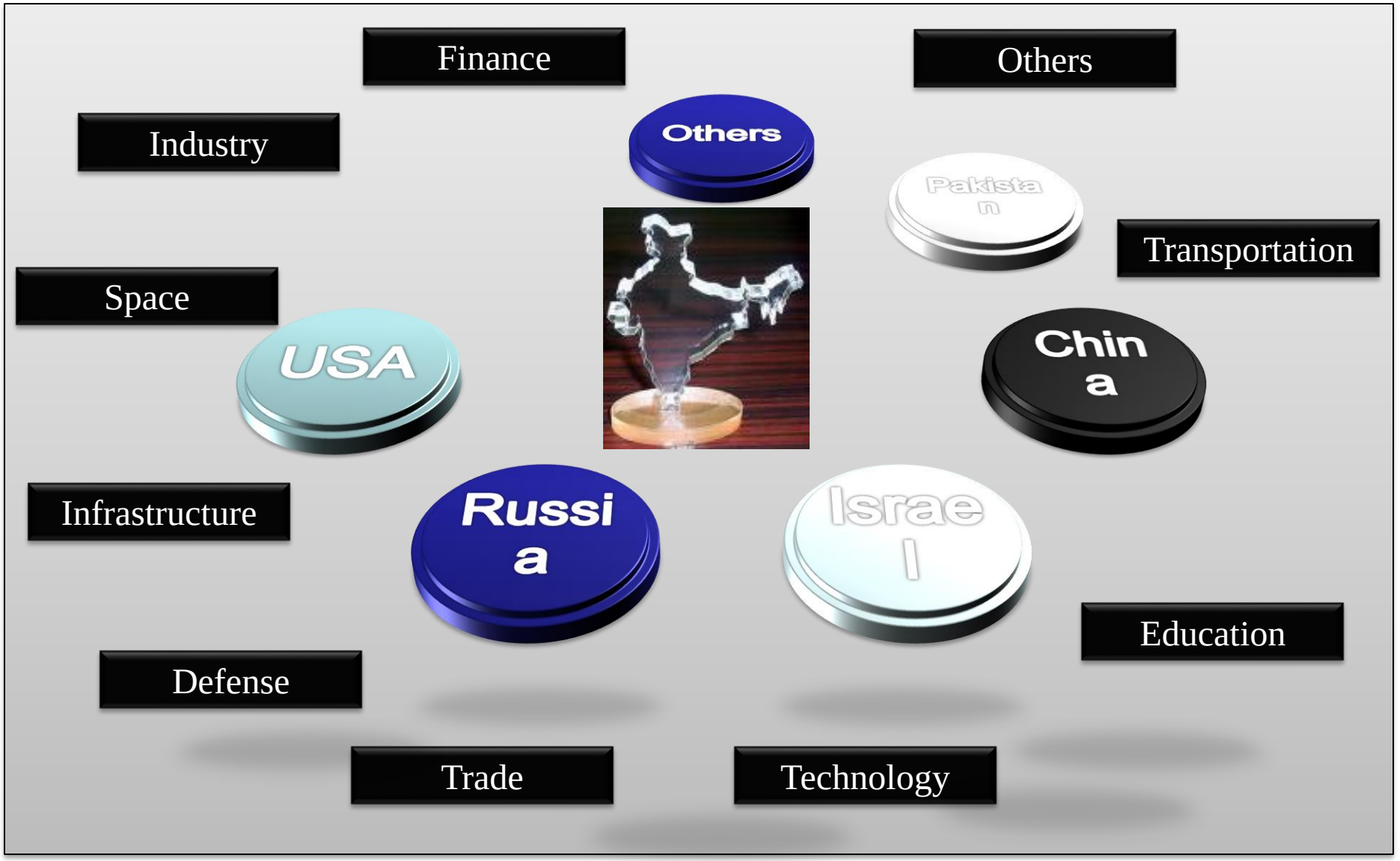
- **BCM Program Management and**
- **System Audit.**

# Scope Session 1

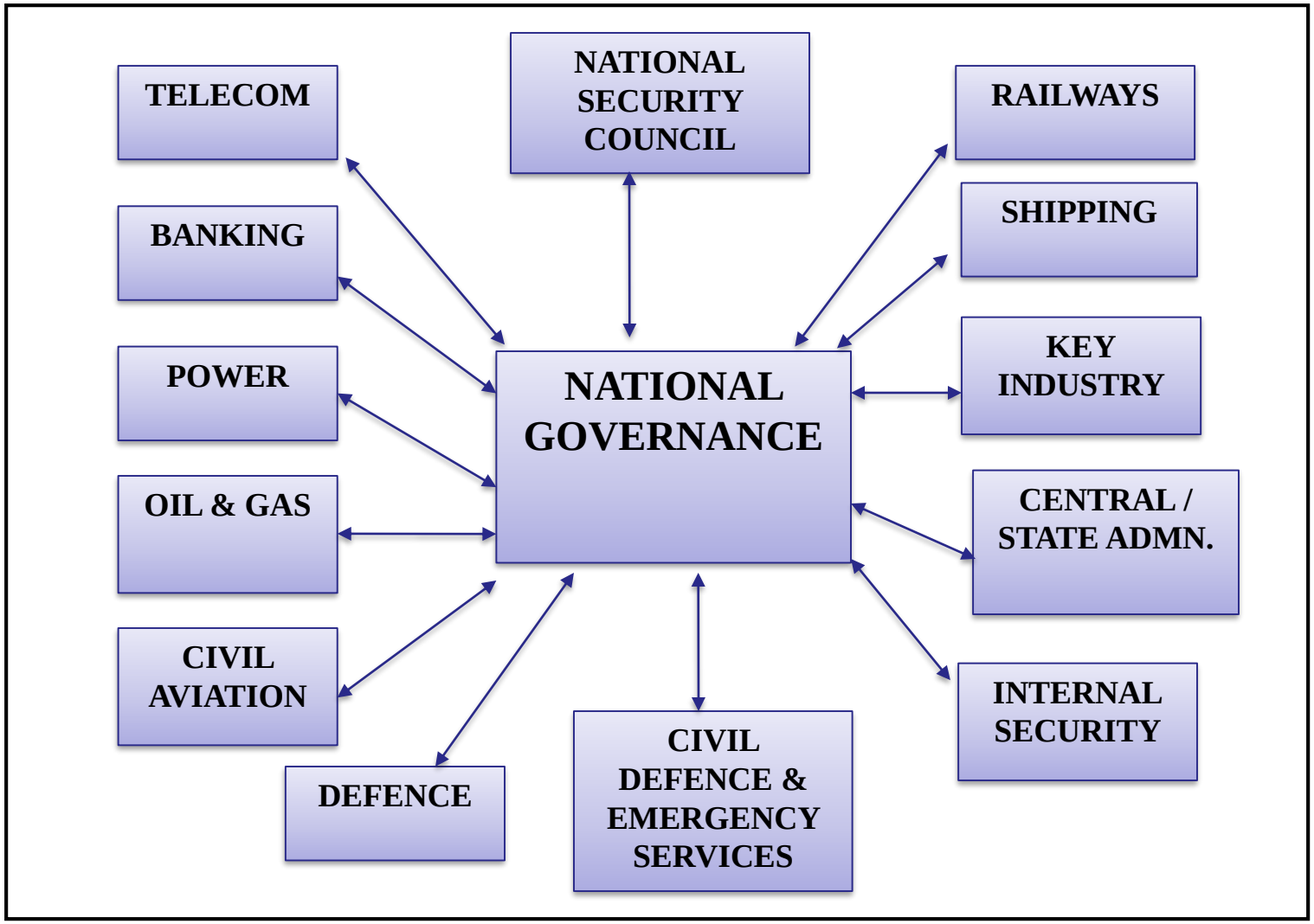
- Information Age Interdependencies and Risks
- Introduction to Risk & Risk Analysis
- Security Risk Management Concepts
- Security Risk Management Prerequisites
- Assessing Risk
- Conducting Decision Support
- Implementing Controls and Measuring Program Effectiveness
- Risk Management Framework Outlines

# Information Age Interdependencies & Risks

# Information Age: Global Dependence & Vulnerability



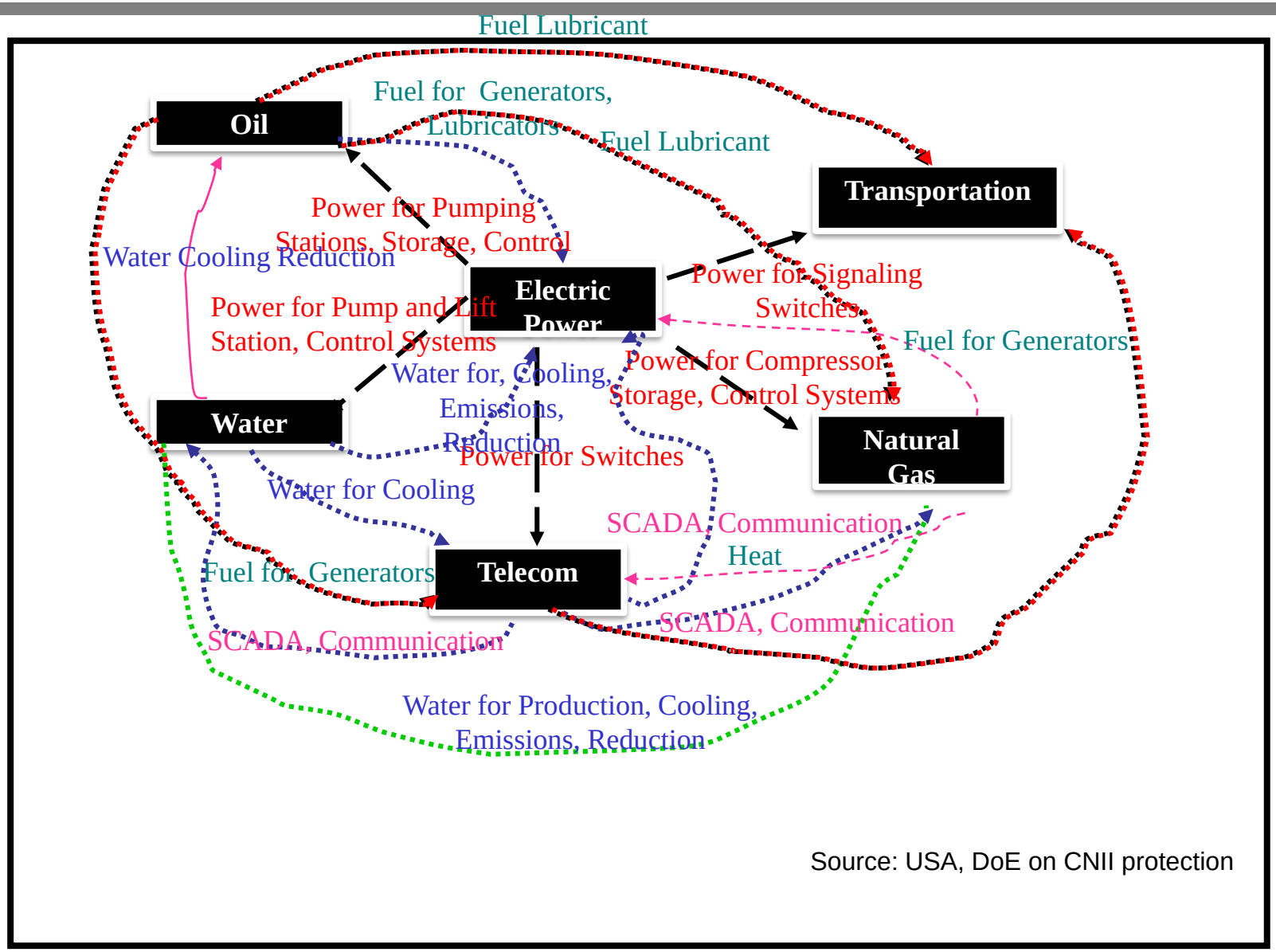
# Critical National Infrastructures



# Sector wise Critical Infrastructure

| | |
|---|---|
| Core Infrastructure | • Info and Telecom |
| Governance and Security | • Transportation (Aviation , rail , mass , transit , water , commerce , pipelines and highways<br>• Postal and Shipping<br>• Emergency services<br>• Continuity of Govt |
| Treasury | • Banking and Finance |
| Health and Human Services | • Public health |
| Energy | • Electric power , oil and gas production and storage |
| Environmental Protection | • Water<br>• Chemical industry & Hazardous materials |
| Agriculture | • Agriculture<br>• Food (meat and poultry) |
| Defence | • Defence  Industrial base |

# Debilitating Interdependencies of CNII



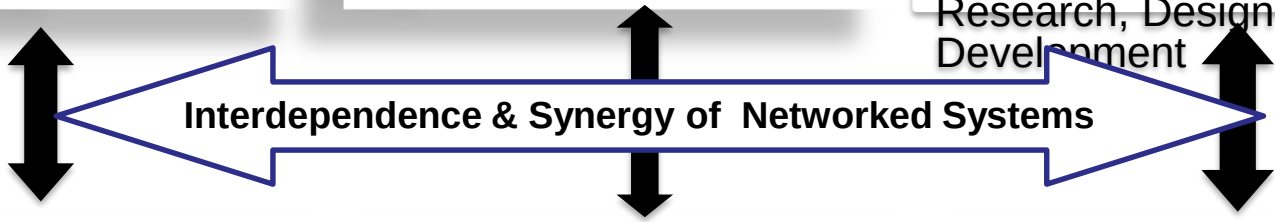

Source: USA, DoE on CNII protection

# Networked National Infrastructure at Risk

**Defence**
Facilities
Command & Control Warfare
Information Warfare
Hundred Information Sites
Force Formations
Infrastructure Supporting Armed Forces

**National Core Infrastructure**
Water
Telecommunication
Transport
Institute of Governance
Electric Power
Space
Ports

**Economic , Social & Political**
Environment
Crime/ Lawenforcement
Healthcare
Safety / Protection
Society / Culture
Economy / Finance / Banking
Political / Diplomatic
Education
Research, Design and Development




**Major Commodities**
Energy( Coal, oil, gas)
Food
Chemicals
Raw Materials
Irreplaceable components
Human Resource
Mines

**Industry**
Steel
Military Hardware
Heavy Engineering
Machinery
Electronics
Computers
Software
Information (content, IPR)
Consumer durables
Insurance.

**Intangible Networks**
Perceptions
Public Confidence
Entertainment
Media
Legal Framework
Privacy
Trust in Institutions

# Critical Infrastructures at Risk

## City Centers
- Loitering detection
- Vehicle overstay
- Graffiti detection
- Slip & fall detection
- Bus lane monitoring
- Crowd detection
- Camera tempering

## Infrastructure
- Perimeter protection
- Loitering detection
- Graffiti detection
- Object removal
- Camera tempering

## Government
- Perimeter/ border protection
- Tailgating through secure access
- Abandoned object detection
- Camera detection



## Airports
- Perimeter protection
- Abandoned object removal
- Debris on runways
- Directional Alarms
- Loitering detection

## Railways
- Platform crowing
- Graffiti detection
- Track monitoring
- Level crossing
- Camera tempering

## Bus Stands
- Camera Tempering
- Slip & fall
- Graffiti detection

# Introduction to Risk & Risk Analysis

# Information Security & Risk Management

- **Information Security - (Confidentiality, Integrity, Availability & safety of information assets (software, hardware, data, networks, documentation..), in transit or at rest/ storage.**

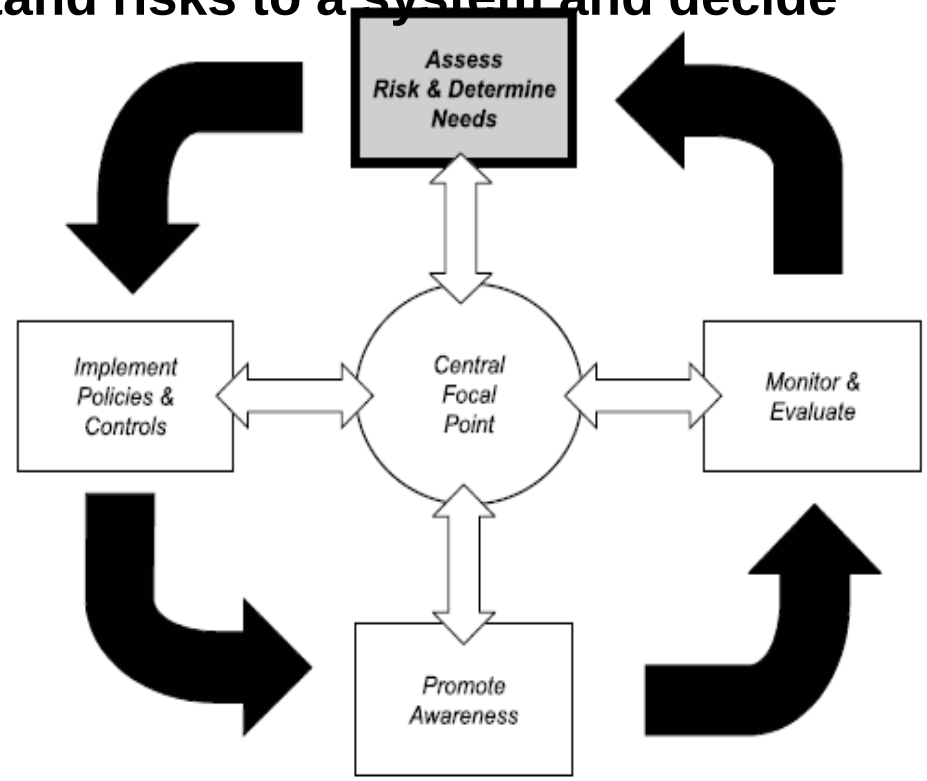
- **Risk Management involves Identification of an organization's information assets and the development, documentation, implementation, and updating of policies, standards, procedures, and guidelines that ensure confidentiality, integrity, and availability.**

- **Management tools such as data classification, risk assessment, and risk analysis are used to identify threats, classify assets, and to rate their vulnerabilities so that effective security measures and controls can be implemented.**

# Risk & Risk Management

- **The probability that a particular threat will exploit a particular vulnerability**
- **Need to systematically understand risks to a system and decide how to control them.**


- **The probability that a particular threat will exploit a particular vulnerability**
- **Need to systematically understand risks to a system and decide how to control them.**


**Risk Management Cycle**

From GAO/AIMD-99-139

# What Does Risk Management Involve?

- **Understanding the planning, organization, roles, and responsibilities of individuals in identifying and securing organization's information assets;**

- **The development and use of policies stating management's views and position on particular topics and the use of guidelines, standards, and procedures to support the policies;**

- **Security training to make employees aware of the importance of information security, its significance, and the specific security-related requirements relative to their position;**

# What Does Risk Management Involve?...

- **The importance of confidentiality, proprietary, and private information;**

- **Third party management and service level agreements related to information security;**

- **Employment agreements, employee hiring and termination practices, and risk management practices, and tools to identify, rate, and reduce the risk to specific resources.**

# Risk assessment vs. risk analysis vs. risk management

- A **risk analysis** involves identifying the most probable threats to an organization and analyzing the related vulnerabilities of the organization to these threats.

- A **risk assessment** involves evaluating existing security and controls and assessing their adequacy relative to the potential threats of the organization.

- **Risk management** is the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analyzing, evaluating, treating, monitoring and communicating risk.

# Risk Analysis, Assessment & Communication

- **The process of identifying, assessing, and reducing risks to an acceptable level**
  - Defines and controls threats and vulnerabilities
  - Implements risk reduction measures

- **An analytic discipline with three parts:**
  - Risk assessment: determine what the risks are
  - Risk management: evaluating alternatives for mitigating the risk
  - Risk communication: presenting this material in an understandable way to decision makers and/or the public

# Basic Risk Analysis Structure

- **Evaluate**
  - Value of computing and information assets
  - Vulnerabilities of the system
  - Threats from inside and outside
  - Risk priorities
- **Examine**
  - Availability of security countermeasures
  - Effectiveness of countermeasures
  - Costs (installation, operation, etc.) of countermeasures
- **Implement and Monitor**

# Benefits of Risk Analysis

- **Assurance that greatest risks have been identified and addressed**
- **Increased understanding of risks**
- **Mechanism for reaching consensus**
- **Support for needed controls**
- **Means for communicating results**

# Security & Risk Management Concepts

# Critical Assets in an Enterprise

**Asset is anything of value: Physical Assets & Logical Assets**

- **People and skills**
- **Goodwill**
- **Hardware/ Software**
- **Data**
- **Documentation**
- **Supplies**
- **Physical plant**
- **Money**

# Threats

- **An expression of intention to inflict evil injury or damage**
- **Attacks against key security services**
  - **Confidentiality, integrity, availability**

# Example Threat List

- T01 Access (Unauthorized to System - logical)
- T02 Access (Unauthorized to Area - physical)
- T03 Airborne Particles (Dust)
- T04 Air Conditioning Failure
- T05 Application Program Change (Unauthorized)
- T06 Bomb Threat
- T07 Chemical Spill
- T08 Civil Disturbance
- T09 Communications Failure
- T10 Data Alteration (Error)
- T11 Data Alteration (Deliberate)
- T12 Data Destruction (Error)
- T13 Data Destruction (Deliberate)
- T14 Data Disclosure (Unauthorized)
- T15 Disgruntled Employee
- T16 Earthquakes
- T17 Errors (All Types)
- T18 Electro-Magnetic Interference
- T19 Emanations Detection
- T20 Explosion (Internal)
- T21 Fire, Catastrophic
- T22 Fire, Major
- T23 Fire, Minor
- T24 Floods/Water Damage
- T25 Fraud/Embezzlement
- T26 Hardware Failure/Malfunction
- T27 Hurricanes
- T28 Injury/Illness (Personal)
- T29 Lightning Storm
- T30 Liquid Leaking (Any)
- T31 Loss of Data/Software
- T32 Marking of Data/Media Improperly
- T33 Misuse of Computer/Resource
- T34 Nuclear Mishap
- T35 Operating System Penetration/Alteration
- T36 Operator Error
- T37 Power Fluctuation (Brown/Transients)
- T38 Power Loss
- T39 Programming Error/Bug
- T40 Sabotage
- T41 Static Electricity
- T42 Storms (Snow/Ice/Wind)
- T43 System Software Alteration
- T44 Terrorist Actions
- T45 Theft (Data/Hardware/Software)
- T46 Tornado
- T47 Tsunami (Pacific area only)
- T48 Vandalism
- T49 Virus/Worm (Computer)
- T50 Volcanic Eruption

# Threat-Sources

| Threat-source | Motivation | Threat Actions |
|---|---|---|
| Hacker | Challenge, ego, rebellion | Hacking<br>Social engineering<br>System intrusion<br>Unauthorized access |
| Terrorist | Blackmail, Destruction, Revenge | Information warfare<br>System attack<br>System tampering |
| Insider | Ego, Revenge, Monetary gain | Blackmail<br>Malicious code<br>Input of falsified data<br>System bugs |

# Vulnerabilities

- **Flaw or weakness in system that can be exploited to violate system integrity.**
  - Security Procedures
  - Design Weaknesses
  - Implementation Inadequacies
- **Threats trigger vulnerabilities**
  - Accidental
  - Malicious

# Example Vulnerabilities

- **Physical**
- V01 Susceptible to unauthorized building access
- V02 Computer Room susceptible to unauthorized access
- V03 Media Library susceptible to unauthorized access
- V04 Inadequate visitor control procedures
- (and 36 more)
- **Administrative**
- V41 Lack of management support for security
- V42 No separation of duties policy
- V43 Inadequate/no computer security plan policy
- V47 Inadequate/no emergency action plan
- (and 7 more)
- **Personnel**
- V56 Inadequate personnel screening
- V57 Personnel not adequately trained in job
- ...
- **Software**
- V62 Inadequate/missing audit trail capability
- V63 Audit trail log not reviewed weekly
- V64 Inadequate control over application/program changes

***Communications***

- *V87 Inadequate communications system*
- *V88 Lack of encryption*
- *V89 Potential for disruptions*
- *...*

- **Hardware**
- *V92 Lack of hardware inventory*
- *V93 Inadequate monitoring of maintenance*

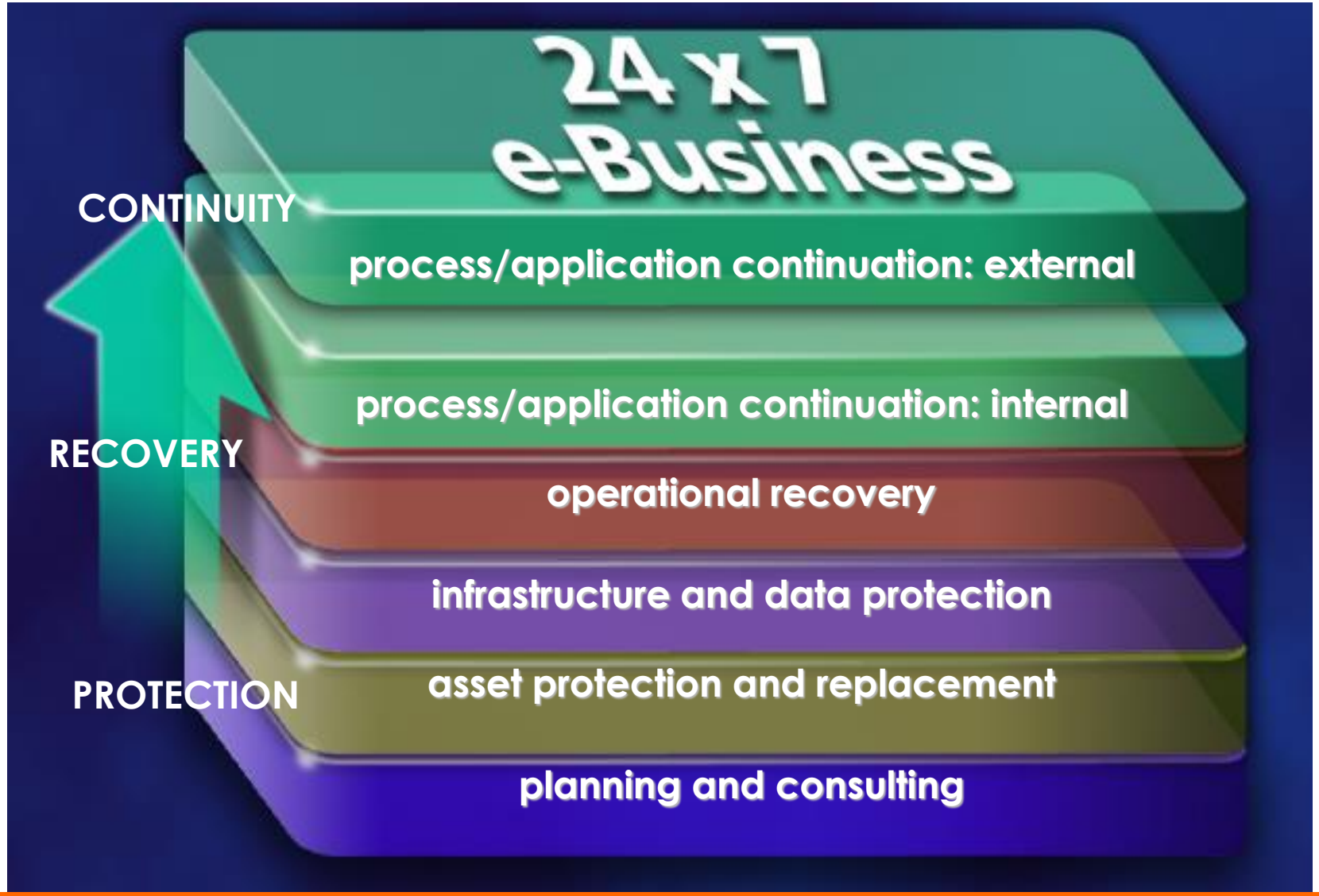
**personnel**

- *V94 No preventive maintenance program*
- *…*
- *V100 Susceptible to electronic emanations*

# Controls/Countermeasures

- **Mechanisms or procedures for mitigating vulnerabilities**
  - Prevent
  - Detect
  - Recover
- **Understand cost and coverage of control**
- **Controls follow vulnerability and threat analysis**

# Controls/Countermeasures



# Example Controls

- C01 Access control devices - physical
- C02 Access control lists - physical
- C03 Access control - software
- C04 Assign ADP security and assistant in writing
- C05 Install-/review audit trails
- C06 Conduct risk analysis
- C07Develop backup plan
- C08 Develop emergency action plan
- C09 Develop disaster recovery plan
- ...
- C21 Install walls from true floor to true ceiling
- C22 Develop visitor sip-in/escort procedures
- C23 Investigate backgrounds of new employees
- C24 Restrict numbers of privileged users
- C25 Develop separation of duties policy
- C26 Require use of unique passwords for logon
- C27 Make password changes mandatory
- C28 Encrypt password file
- C29 Encrypt data/files
- C30 Hardware/software training for personnel
- C31Prohibit outside software on system
- ...
- C47 Develop software life cycle development program
- C48 Conduct hardware/software inventory
- C49 Designate critical programs/files
- C50 Lock PCs/terminals to desks
- C51 Update communications system/hardware
- C52 Monitor maintenance personnel
- C53 Shield equipment from electromagnetic interference/emanations
- C54Identify terminals

# Risk/Control Trade Offs

- **Only Safe Asset is a Dead Asset**
  - Asset that is completely locked away is safe, but useless
  - Trade-off between safety and availability
- **Do not waste effort on assets with low loss value**
  - Don’t spend resources to protect garbage
- **Control only has to be good enough, not absolute**
  - Make it tough enough to discourage enemy

# Need for Risk Management Process

- **Security risk management**
  - A process for identifying, prioritizing and managing risk to an acceptable level within the organization
- **A formal security risk management process can address the following:**
  - Threat response time
  - Regulatory compliance
  - Infrastructure management costs
  - Risk prioritization and management

# Critical Success Factors

- Executive leadership sponsorship
- Well defined list of stakeholders
- Organizational maturity
- Open communication and teamwork
- Holistic view of the organization
- Security risk management team authority

# Strategies for Risk Management

- **Reactive**
  - A process that responds to security events as they occur
- **Proactive**
  - A process that reduces the risk of new vulnerabilities in your organization

# Security & Risk Management Pre-requisites

# Types of Risk Analysis

**Quantitative**

1. Identify and value assets
2. Determine vulnerabilities and impact
3. Estimate likelihood of exploitation
4. Compute Annual Loss Exposure (ALE)
5. Survey applicable controls and their costs
6. Project annual savings from control
7. Assigns real numbers to costs of safeguards and damage
8. Probability of event occurring
9. Can be unreliable/inaccurate

# Types of Risk Analysis...

- **Risk = Risk-impact x Risk-Probability**
  - **Loss of car: risk-impact is cost to replace car, e.g. $10,000**
  - **Probability of car loss: 0.10**
  - **Risk = 10,000 x 0.10 = 1,000**
- **Generally measured per year**
  - **Annual Loss Exposure (ALE)**

# Types of Risk Analysis

## Qualitative Risk Analysis (QRA)

- Judges an organization's risk to threats
- Based on judgment, intuition, and experience
- Ranks the seriousness of the threats for the sensitivity of the asserts
- Subjective, lacks hard numbers to justify return on investment

- **Generally used in Information Security**
  - Hard to make meaningful valuations and meaningful probabilities
  - Relative ordering is faster and more important
- Many approaches to performing qualitative risk analysis
- **Same basic steps as quantitative analysis**
  - Still identifying asserts, threats, vulnerabilities, and controls
  - Just evaluating importance differently

# Example: 10 Step QRA

- **Step 1: Identify Scope**
  - **Bound the problem**
- **Step 2: Assemble team**
  - **Include subject matter experts, management in charge of implementing, users**
- **Step 3: Identify Threats**
  - **Pick from lists of known threats**
  - **Brainstorm new threats**
  - **Mixing threats and vulnerabilities here...**

# Example: 10 Step QRA...

**Step 4: Threat prioritization**

- Prioritize threats for each asset
  - Likelihood of occurrence
- Define a fixed threat rating
  - E.g., Low(1) … High(5)
- Associate a rating with each threat
- Approximation to the risk probability in quantitative approach

**Step 5: Loss Impact**

- With each threat determine loss impact
- Define a fixed ranking
  - E.g., Low(1) … High(5)
- Used to prioritize damage to asset from threat

# Example: 10 Step QRA...

## Step 6: Total impact

- Sum of threat priority and impact priority

| Threat | Threat Priority | Impact Priority | Risk Factor |
|---|---|---|---|
| Fire | 3 | 5 | 8 |
| Water | 2 | 5 | 7 |
| Theft | 2 | 3 | 5 |

# Example: 10 Step QRA...

**Step 7: Identify Controls/Safeguards**

- Potentially come into the analysis with an initial set of possible controls
- Associate controls with each threat
- Starting with high priority risks

**Step 8:**

- Do cost-benefits and coverage analysis

**Step 9**

- Rank controls

# Example: 10 Step QRA...

## Safeguard Evaluation

- | Threat | Risk Factor | Possible Safeguard | Safeguard cost |
|---|---|---|---|
| Fire | 8 | Fire supression system | $15,000.00 |
| Tornado | 8 | Business Continuity Plan | $75,000.00 |
| Water Damage | 7 | Business Continuity Plan | $75,000.00 |
| Theft | 5 | | |
| | | | |
| | | | |
| | | | |

# Example: 10 Step QRA...

**Step 10: Communicate Results**

- Most risk analysis projects result in a written report
  - Generally not read
  - Make a good executive summary
  - Beneficial to track decisions.
- Real communication done in meetings and presentations

# Key Considerations in Risk Analysis

- **Key Elements of Risk Analysis**
  - **Assets, Threats, Vulnerabilities, and Controls**
- **Most security risk analysis uses qualitative analysis**
- **Not a scientific process**
  - **Companies will develop their own procedure**
  - **Still a good framework for better understanding of system security**

# Enterprise Risk Management Model

**Source: Dept of Energy USA**

# Enterprize Risk Management Review Process

- **Risk Identification.** What can go wrong? List all possible events that could occur in a subsystem if there are no controls. Once risks are identified, combine like risks according to the following key areas impacted by the risks: people, mission, physical assets, financial assets, and customer/stakeholder trust.
- **Risk Analysis.** What is the likelihood and impact? Rate risks according to probability and impact.
- **Requirements Identification.** What is in place to prevent it? List all controls that would exist without subsystem-specific controls.
- **Controls Identification.** What else is needed to control the risk? Where there is a significant or extreme risk rating, list gaps between existing risks and existing controls.
- **Risk Registry.** What documentation is needed so that the logic and conclusions are clear? Create a register that documents the results of the risk evaluation, including the events, probabilities, impacts, and risk management strategy.

# Risk Identification and Analysis

For each subsystem a group of senior level staff and subject matter experts complete the following-

1. **Risk Identification.** What can go wrong? What events can have an impact on people, mission, physical assets, financial assets, and customer/stakeholder trust? A risk can also be a missed opportunity for improving effectiveness and efficiency.
2. **Risk Analysis.** Look at the subsystem in the context of existing external controls. If there were no specific controls what is the probability and impact of specific risks?

| | | Impact | | | |
|---|---|---|---|---|---|
| Probability | | Negligible | Low | Medium | High |
| | Certain | Minor | Moderate | Extreme | Extreme |
| | Likely | Minor | Moderate | Significant | Extreme |
| | Possible | Minor | Moderate | Significant | Extreme |
| | Unlikely | Minor | Minor | Moderate | Significant |
| | Rare | Minor | Minor | Minor | Moderate |

# Requirements Identification

3. **Requirements Identification.** What is in place to prevent it? List all controls that would exist without subsystem-specific controls.
4. **Controls Identification.**

   What else is needed to control the risk? Where there is a significant or extreme risk rating, list gaps between existing risks and existing external controls. Defer to existing external controls and standards whenever possible.

**Cost Effective Risk Management**

•What is the most effective method for bringing risk down to an acceptable level?

•Are the controls most expensive than the risk?

**Minor – risk acceptance may be preferred**

**Moderate – existing controls may be adequate**

**Significant – may need to add more controls**

**Extreme – more controls likely needed**

# Risk Register

## 5. Risk Registry

- Clearly document the analysis of identified risks, existing controls, and proposed controls to address any serious gap between existing controls and risk.
- Risk Mitigation Options – Acceptance, Monitoring, Mitigation, and Avoidance
- Evaluate the costs of various mitigation techniques compare the cost/benefit of the risk

| Risk/ Opportunity | Risk Level | Potential Cost/Benefit | External Control(s) | Proposed Mitigation Technique | Internal Control (if needed) |
|---|---|---|---|---|---|
| Identify specific risks and their risk level | Minor, Moderate, Significant and Extreme – based on the probability and impact chart. | Give a rough estimate of the magnitude of the cost/benefit of the risk/opportunity without specific controls. | List all external controls that help address the risks and opportunity identified. | Based on any gap between the risk/opportunity and existing controls, what strategy should adopt? | List all internal controls needed to effectively and efficiently address gaps between risks and external controls. |

# Sample Risk Analysis

| Risk Assessment for DOE O 333.1, *Workforce Discipline* | | | | | |
|---|---|---|---|---|---|
| **Risk/ Opportunity** | **Risk Level** | **Potential Cost/Benefit** | **External Control(s)** | **Proposed Mitigation Technique** | **Internal Control** |
| **1.** Loss of employee trust and low morale from perception of favoritism. (Failure to take the appropriate disciplinary action; arbitrary and inconsistent discipline; failure to address misconduct at the earliest possible stage.) | Extreme | Significant time commitment for managers and costs to the department in excess of $1M | 5 U.S.C., 5 CFR, Part 752, MSPB, EEOC, DOE Inspector General (IG) | Mitigation | **A.** Disciplinary action must be taken for: (1) the purpose of correcting unacceptable conduct at work; (2) behavior that adversely affects job performance; (3) violations of laws, rules, or regulations; or (4) off-duty misconduct when there is a nexus between the misconduct and employment with DOE. |
| **2.** Disruption in the workplace | Significant | Moderate time commitment for all staff | 5 U.S.C., 5 CFR, Part 752, MSPB, EEOC, DOE Inspector General (IG) | Monitoring | **B.** Contact Servicing HR offices before initiating disciplinary/adverse actions. |
| **3.** Embarrassment to the agency; potential political concerns. | Minor | Moderate time commitment for PR staff | | Acceptance | |

Please note: The sample above has been tweaked for instructional purposes.

# Why is ERM important?

- **Integrated Strategy** - ERM is important because it supports the Department's strategy and Management Principles including, "we will manage risk in fulfilling ou mission".

- **Consistency-** Systematic approach for management and operations – how we make decisions, govern how we establish and implement requirements, and how we hold ourselves accountable .

- **Better Communication** - ERM will provide that framework for clearly articulate the processes we use for program execution, and governance.

- **Clear and Concrete Measures of Performance** - It will improve efficiency and allow organization to consistently speak with one voice to our contractors, customers, and stakeholders.

# Assessing the Risk in an Enterprise

# Risk Assessment Methodologies

| | Benefits | Drawbacks |
|---|---|---|
| **Quantitative** | • Risks prioritized by financial impact; assets prioritized by their financial values<br>• Results facilitate management of risk by return on security investment<br>• Results can be expressed in management-specific terminology | • Impact values assigned to risks are based upon subjective opinions of the participants<br>• Very time-consuming<br>• Can be extremely costly |
| **Qualitative** | • Enables visibility and understanding of risk ranking<br>• Easier to reach consensus<br>• Not necessary to quantify threat frequency<br>• Not necessary to determine financial values of assets | • Insufficient granularity between important risks<br>• Difficult to justify investing in control as there is no basis for a cost-benefit analysis<br>• Results dependent upon the quality of the risk management team that is created |

# Security Risk Management Process

# Risk Management vs. Risk Assessment

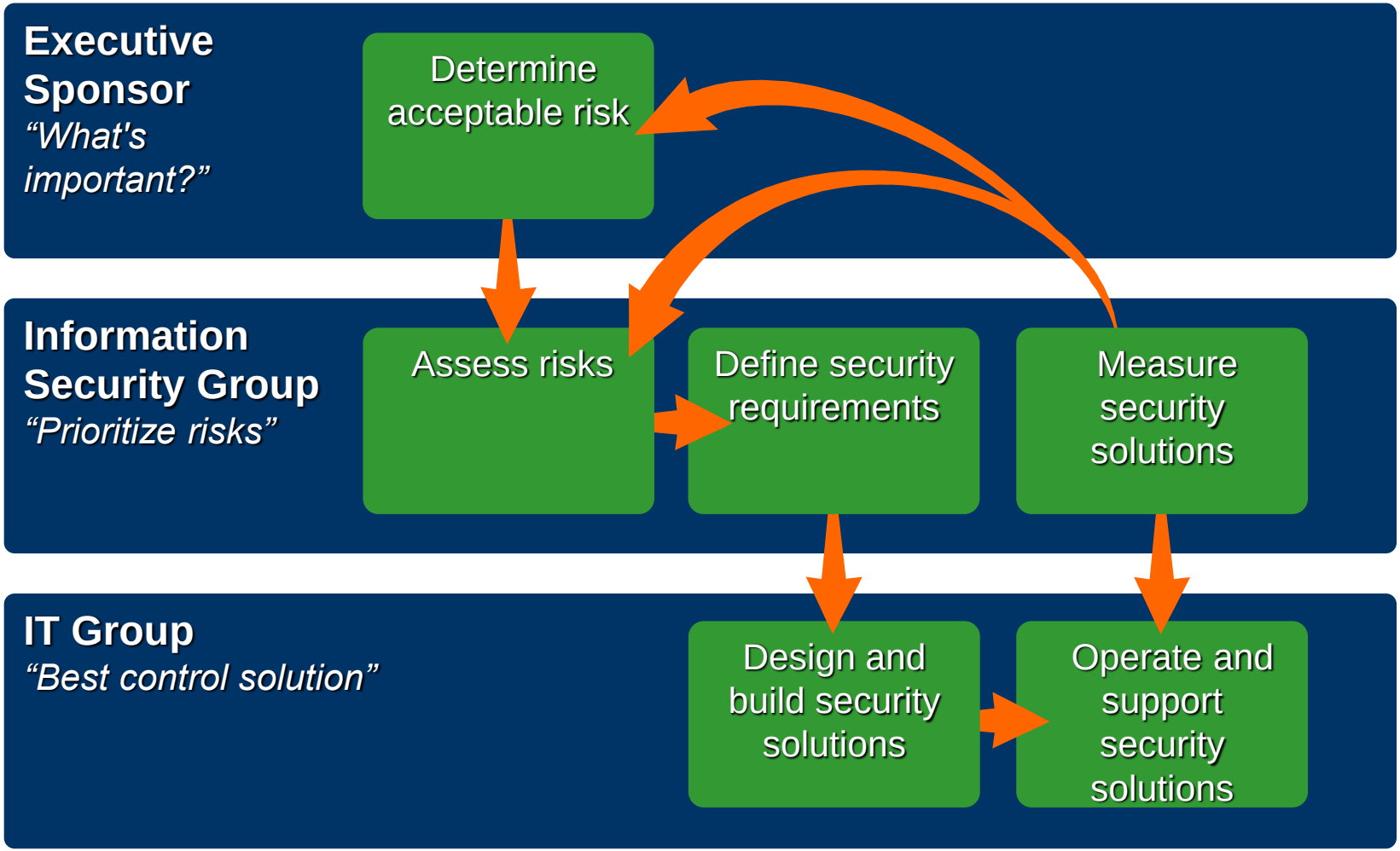
| | Risk Management | Risk Assessment |
|---|---|---|
| **Goal** | • Manage risks across business to acceptable level | • Identify and prioritize risks |
| **Cycle** | • Overall program across all four phases | • Single phase of risk management program |
| **Schedule** | • Scheduled activity | • Continuous activity |
| **Alignment** | • Aligned with budgeting cycles | • Not applicable |

# Communicating Risk

# Risk Management Maturity Self-Assessment

| Level | State |
|---|---|
| 0 | **Non-existent** |
| 1 | **Ad hoc** |
| 2 | **Repeatable** |
| 3 | **Defined process** |
| 4 | **Managed** |
| 5 | **Optimized** |

# Roles and Responsibilities



# Overview of the Assessing Risk Phase

# Understanding the Planning Step

- **The primary tasks in the planning step include the following:**
  - Alignment
  - Scoping
  - Stakeholder acceptance
  - Setting expectations

# Facilitated Data Gathering

- **Elements collected during facilitated data gathering include:**
  - Organizational assets
  - Asset description
  - Security threats
  - Vulnerabilities
  - Current control environment
  - Proposed controls
- **Keys to successful data gathering include:**
  - Meet collaboratively with stakeholders
  - Build support
  - Understand the difference between discussing and interrogating
  - Build goodwill
  - Be prepared

# Identifying and Classifying Assets

- **An asset is anything of value to the organization and can be classified as one of the following:**
  - High business impact
  - Moderate business impact
  - Low business impact

# Organizing Risk Information

- **Use the following questions as an agenda during the facilitated discussions:**
  - What asset are you protecting?
  - How valuable is the asset to the organization?
  - What are you trying to avoid happening to the asset?
  - How might loss or exposures occur?
  - What is the extent of potential exposure to the asset?
  - What are you doing today to reduce the probability of the extent of damage to the asset?
  - What are some actions that you can take to reduce the probability in the future?

# Estimating Asset Exposure

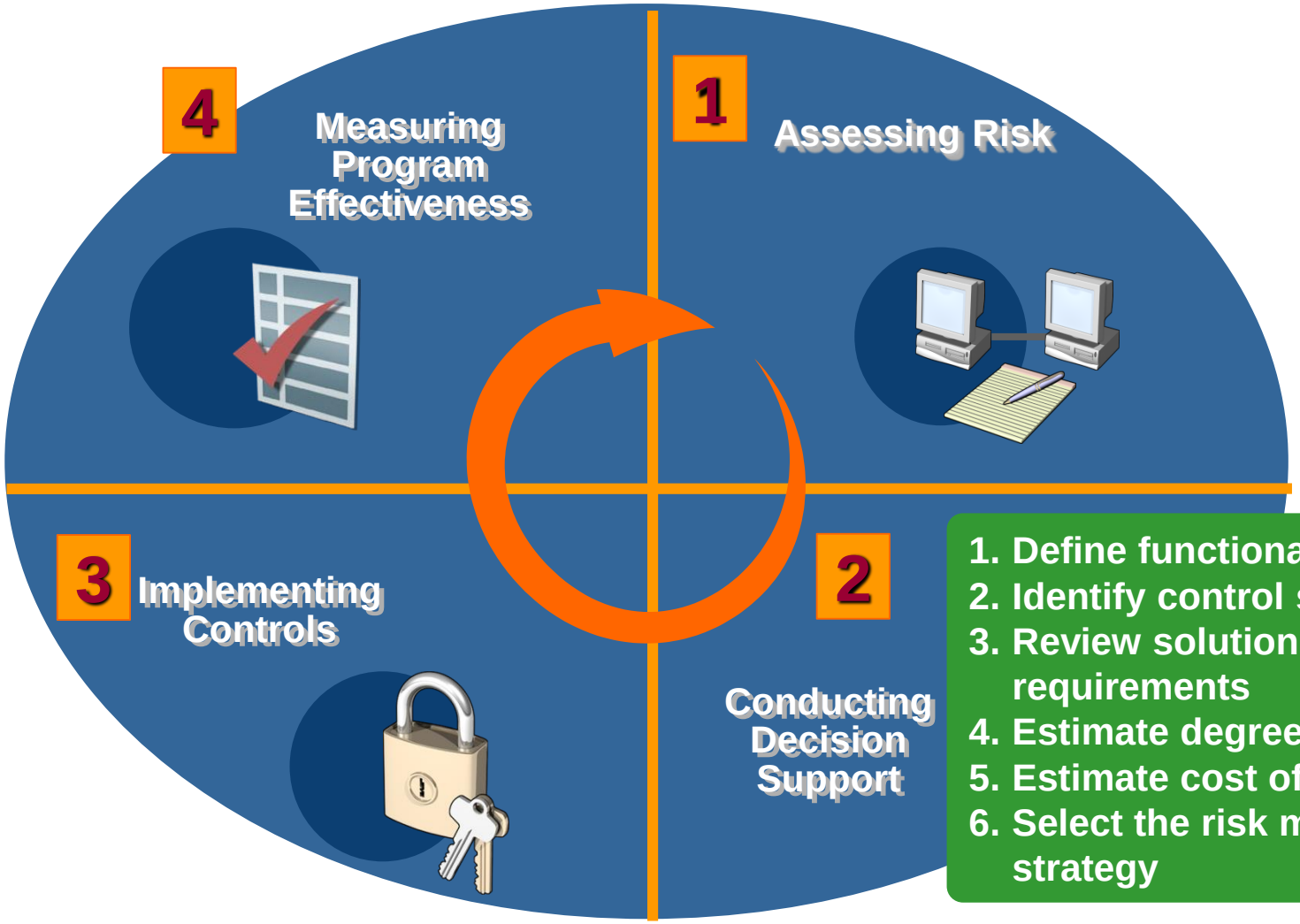
- **Exposure: The extent of potential damage to an asset**
- **Use the following guidelines to estimate asset exposure:**
  - High exposure: severe or complete loss of the asset
  - Medium exposure: limited or moderate loss
  - Low exposure: minor or no loss

# Estimating Threat Probability

- **Guidelines to estimate probability for each threat and vulnerability identified:**
  - High threat: Likely—one or more impacts expected within one year
  - Medium threat: Probable—impact expected within two to three years
  - Low threat: Not probable—impact not expected to occur within three years

# Conducting Decision Support

# Overview of the Decision Support Phase




1. Define functional requirements
2. Identify control solutions
3. Review solution against requirements
4. Estimate degree of risk reduction
5. Estimate cost of each solution
6. Select the risk mitigation strategy

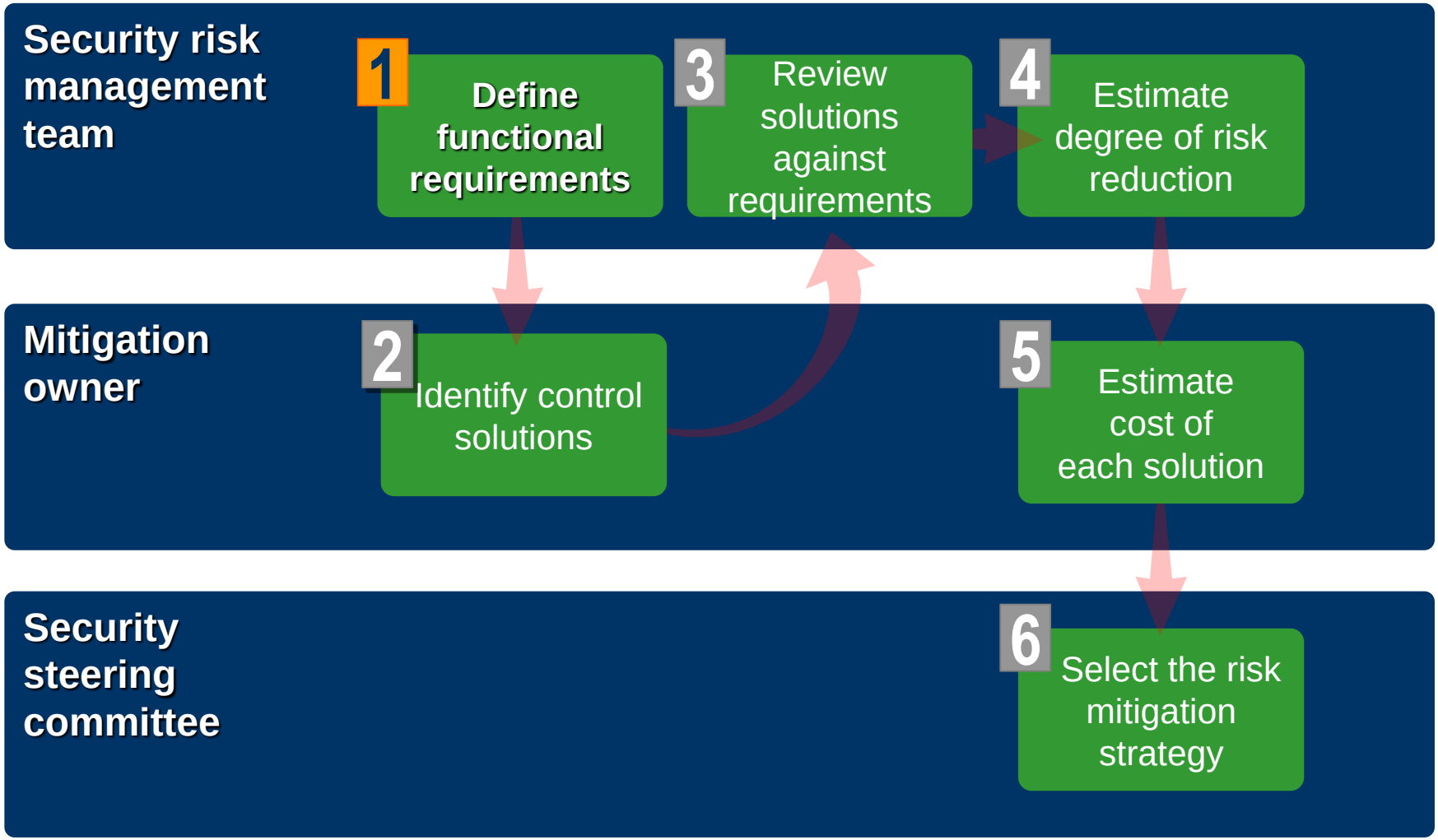
# Identifying Output for the Decision Support Phase

- **Key elements to gather include:**
  - **Decision on how to handle each risk**
  - **Functional requirements**
  - **Potential control solutions**
  - **Risk reduction of each control solution**
  - **Estimated cost of each control solution**
  - **List of control solutions to be implemented**

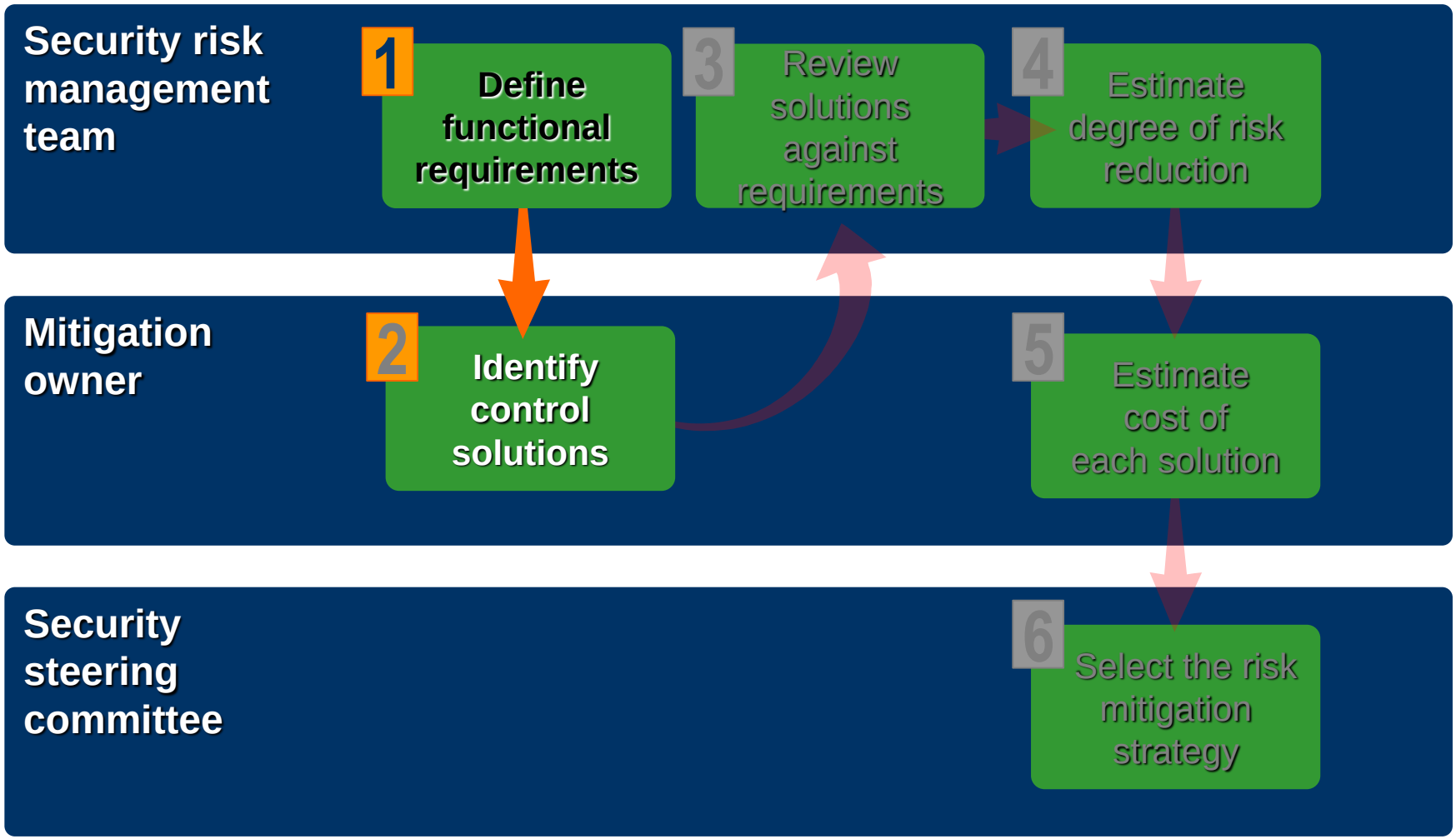
# Considering the Decision Support Options

- **Options for handling risk: ATAM**
  - **Accept**
  - **Transfer**
  - **Avoid**
  - **Mitigate**

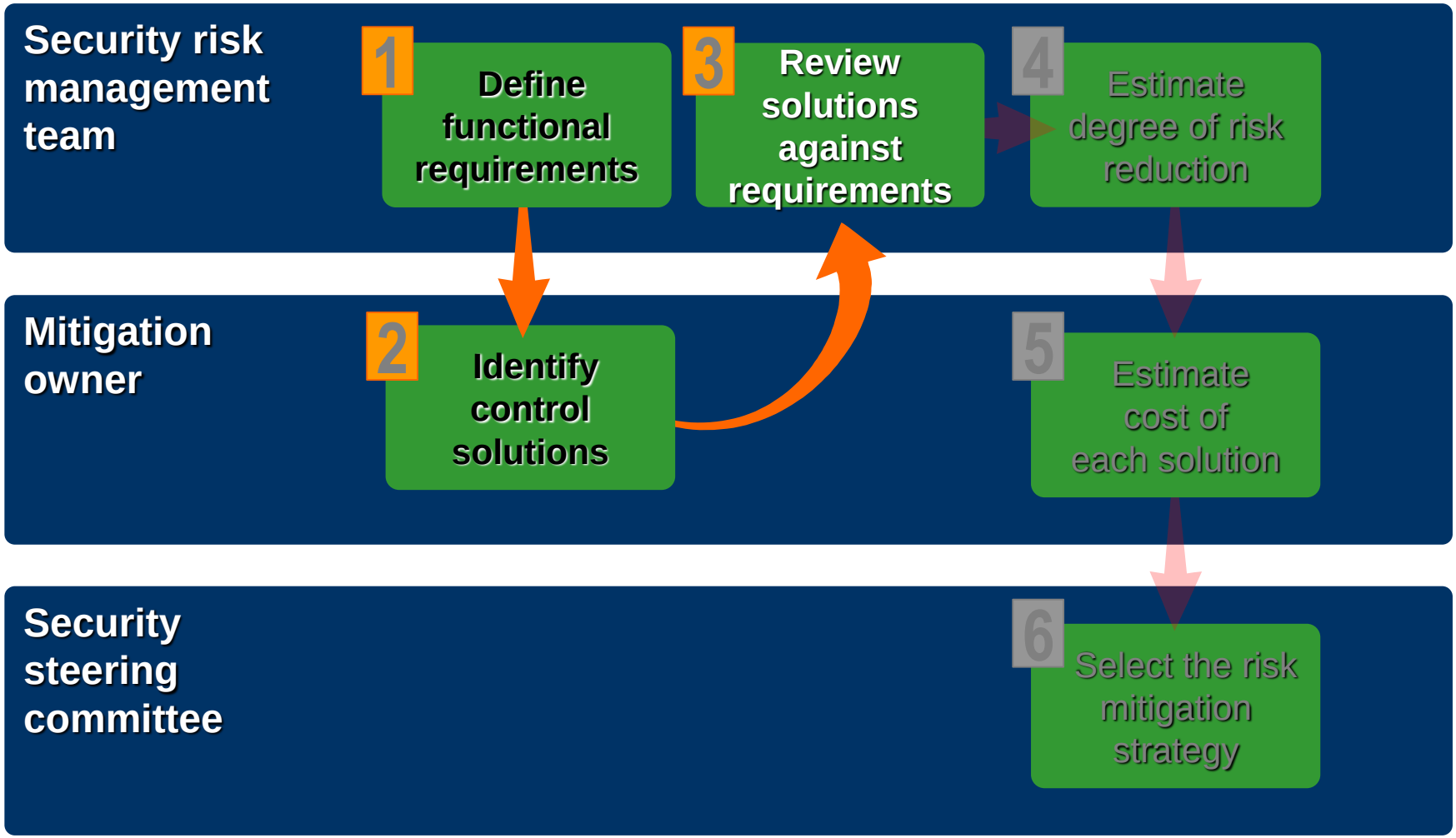
# Step 1: Define Functional Requirements



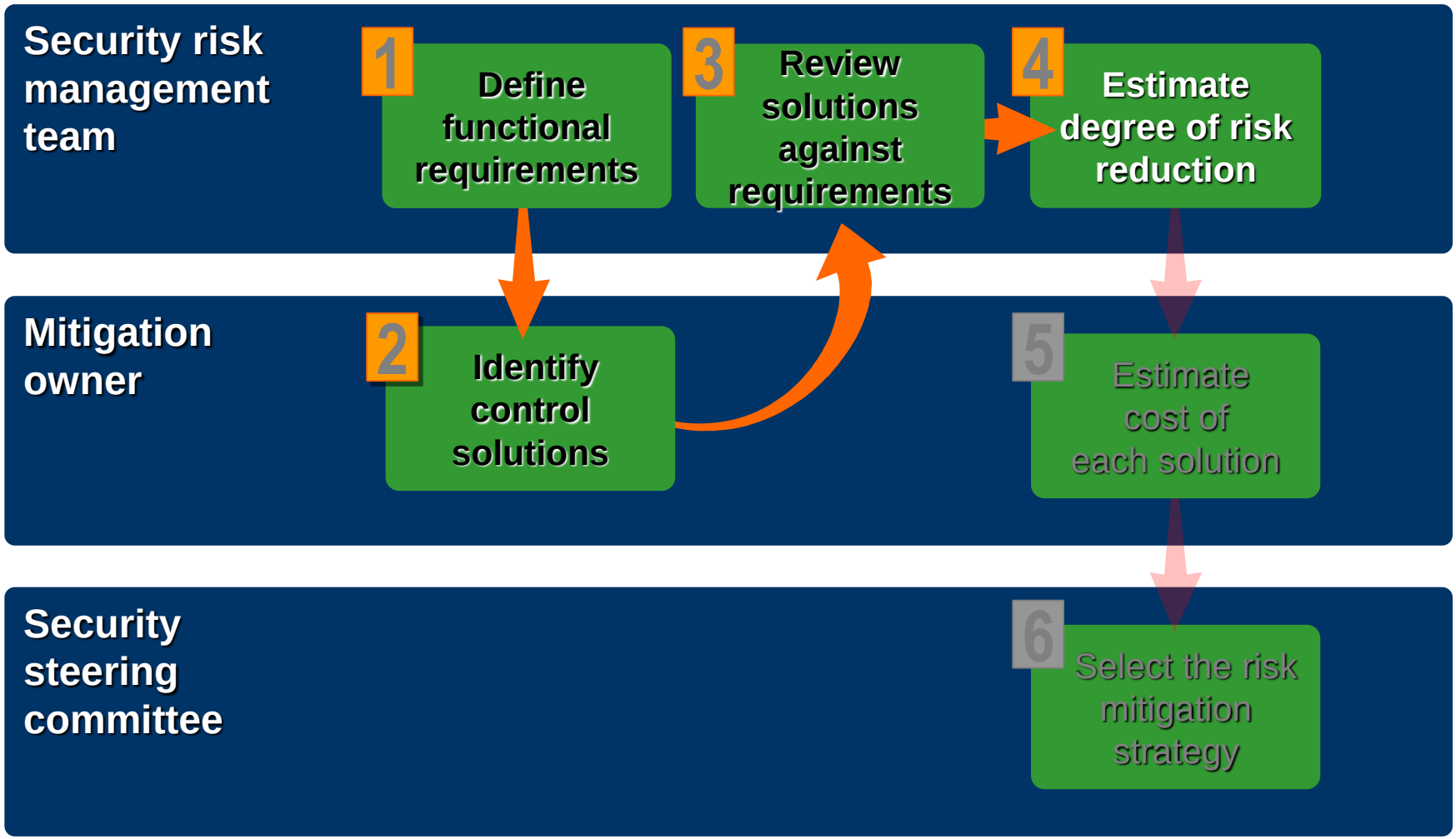
# Step 2: Identify Control Solutions



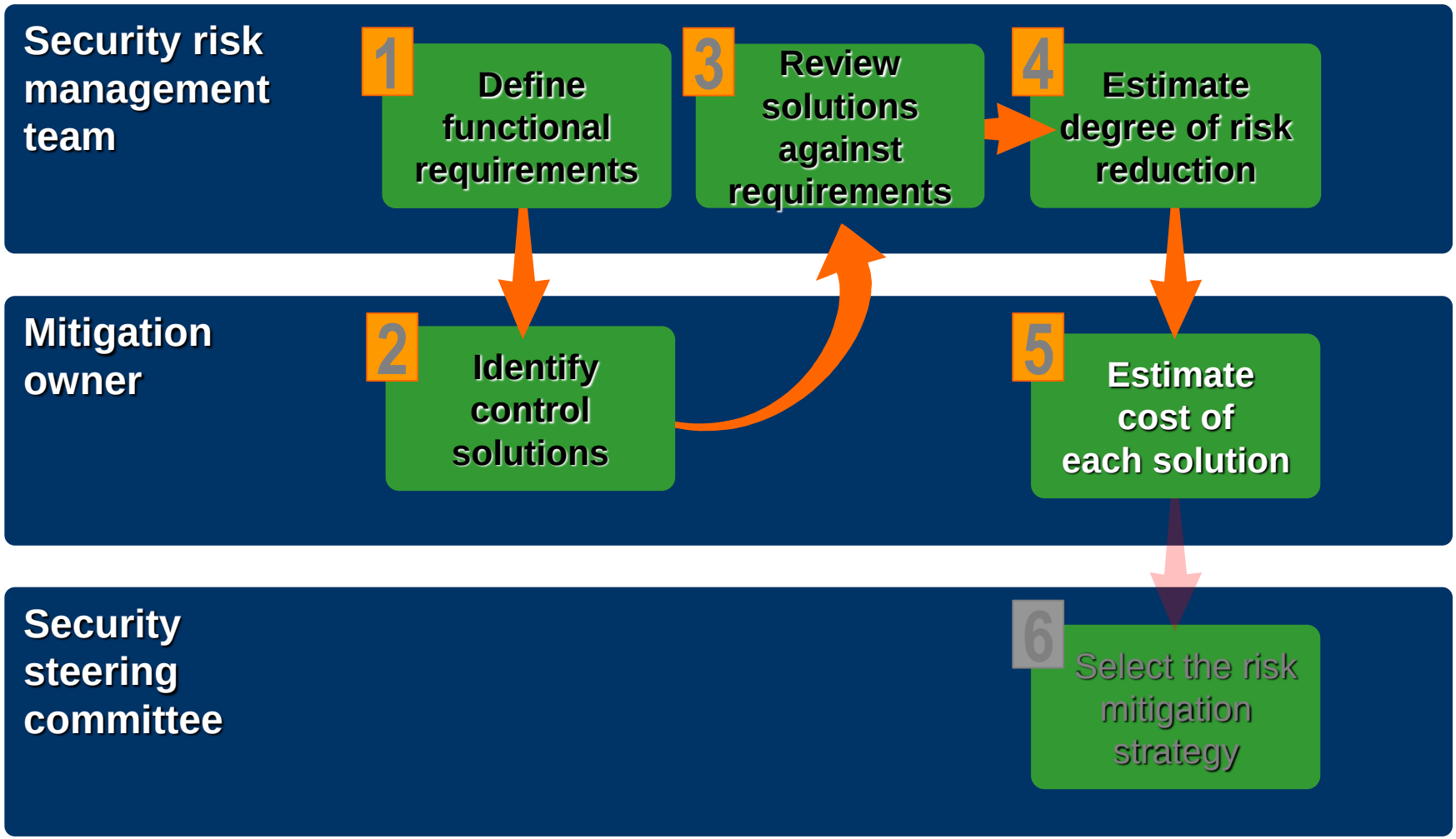
# Step 3: Review Solutions Against Requirements



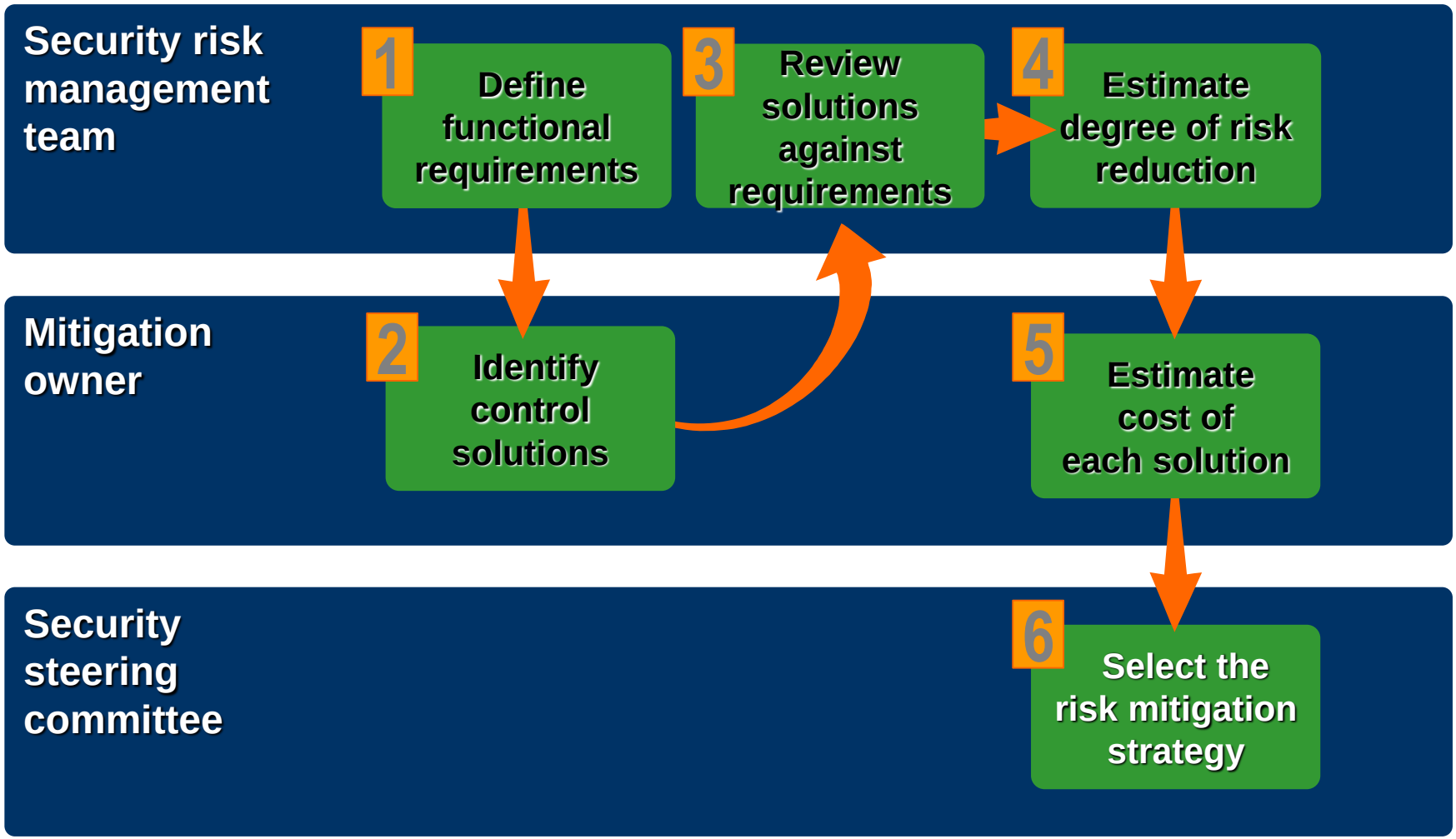
# Step 4: Estimate Degree of Risk Reduction



# Step 5: Estimate Cost of Each Solution



# Step 6: Select the Risk Mitigation Strategy



# Conducting Decision Support: Best Practices

- **Assign a security technologist to each risk**
- **Set reasonable expectations**
- **Build team consensus**
- **Focus on the amount of risk after the mitigation solution**

# Implementing Controls and Measuring Program Effectiveness

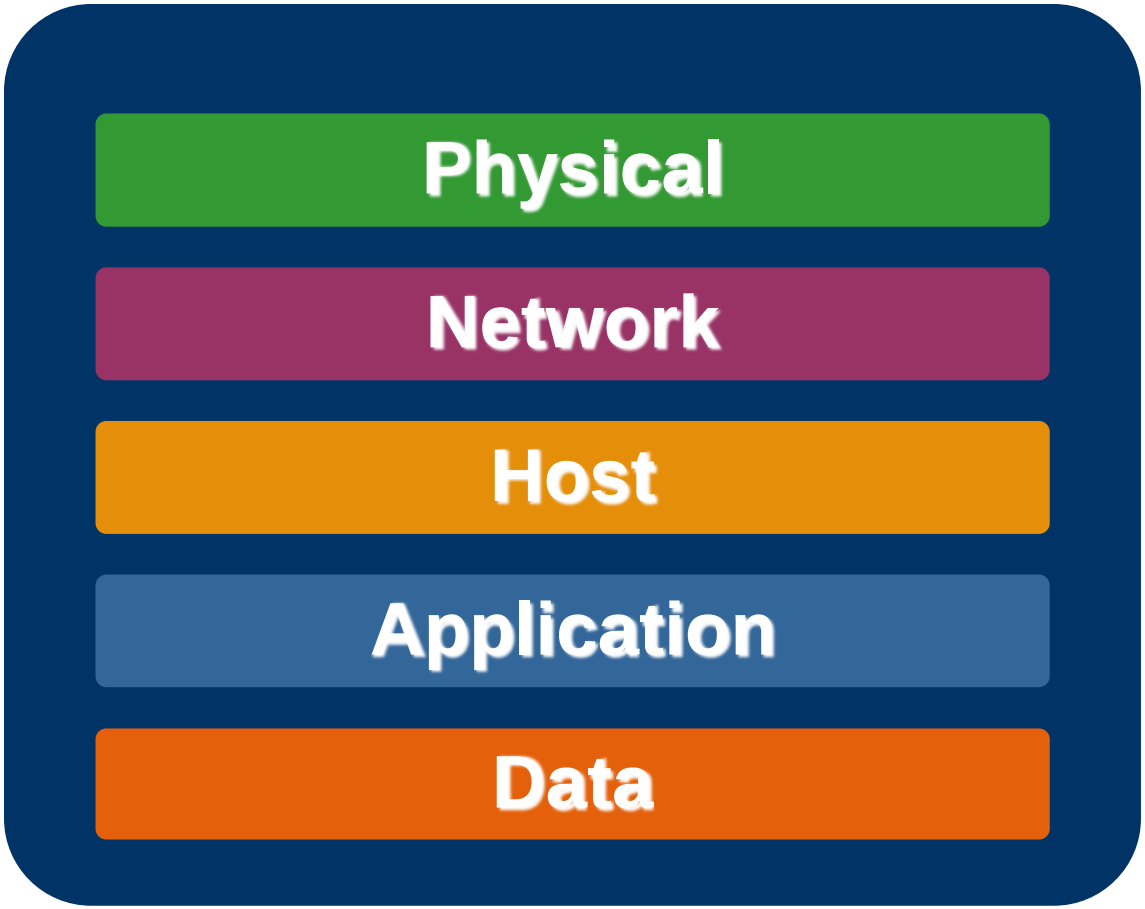
# Implementing Controls


- Seek a holistic approach
- Organize by Defense-in-Depth

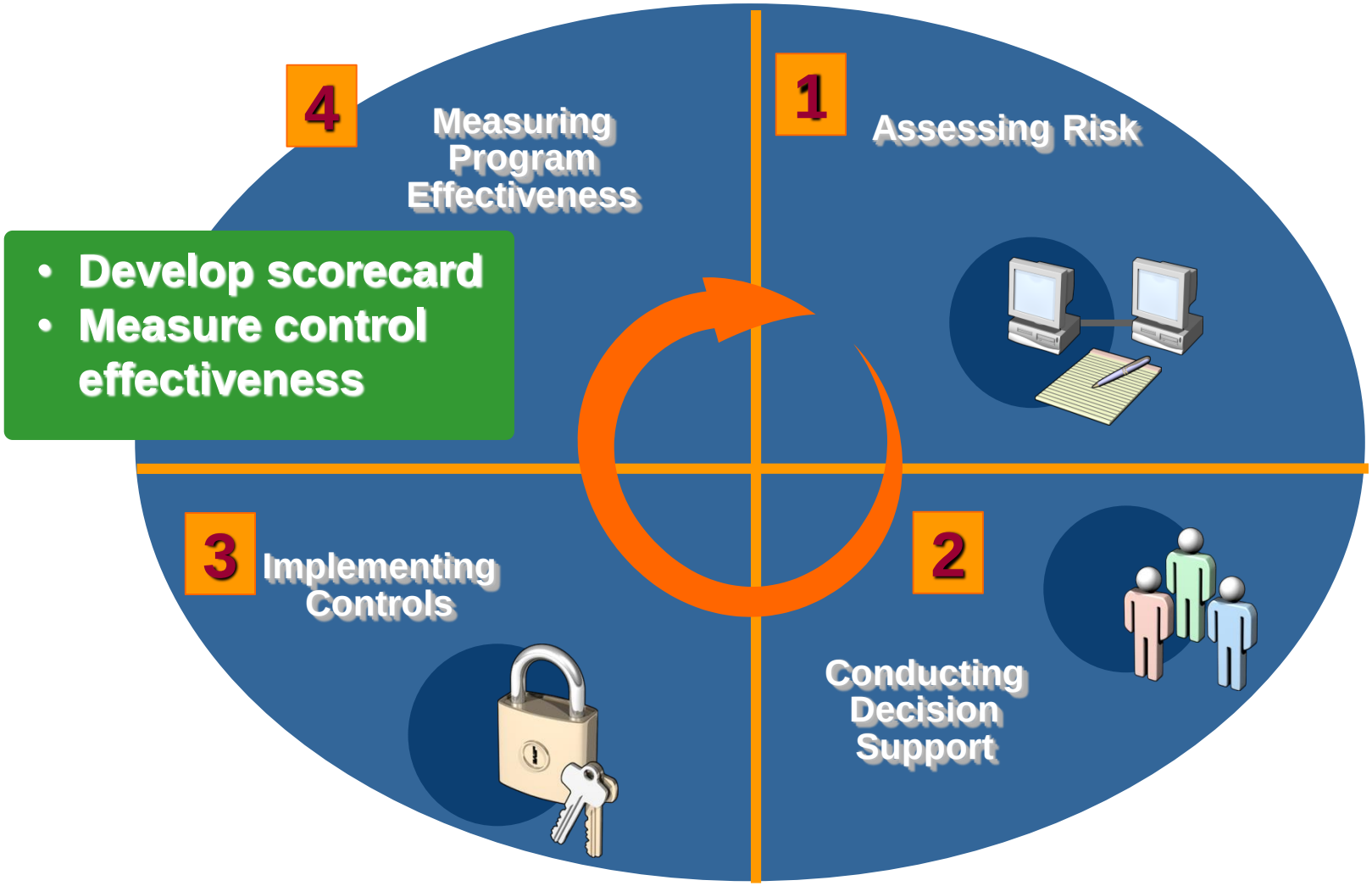
# Organizing the Control Solutions

- **Critical success determinants to organizing control solutions include:**
  - Communication
  - Team scheduling
  - Resource requirements

# Organizing by Defense-in-Depth



# Measuring Program Effectiveness



# Developing a Security Risk Scorecard for Your Organization

- **A simple security risk scorecard organized by the Defense-in-Depth layers:**

| | FY05 Q1 | FY05 Q2 | FY05 Q3 | FY05 Q4 |
|---|---|---|---|---|
| Physical | **H** | **M** | | |
| Network | **M** | **M** | | |
| Host | **M** | **M** | | |
| Application | **M** | **H** | | |
| Data | **L** | **L** | | |
| Risk Levels (H, M, L) | | | | |

# Measuring Control Effectiveness

- **Methods for measuring the effectiveness of implemented controls include:**
  - Direct testing
  - Submitting periodic compliance reports
  - Evaluating widespread security incidents

# Summary

- **Decide on risk management methodology**
- **Determine your maturity level**
- **Conduct risk assessment**
- **Conduct decision support**
- **Implement controls & measure effectiveness**

# Risk Management Framework

*Enterprise Risk Management Framework 2012-2016 aligns with the Australian/New Zealand Standard ISO 31000:2009 Risk management – Principles and guidelines (AS/NZS ISO 31000).*

**Source: Risk Management Framework, Dept of Edu Australia**

# Goals of Risk Management Framework

- **Integrate enterprise risk management within the organization's performance management cycle**
- **Communicate the benefits of risk management**
- **Convey the Organization's policy, approach and attitude to risk management**
- **Set the scope and application of risk management within the organization**
- **Establish the roles and responsibilities for managing risk**
- **Set out a consistent approach for managing risks across the organization, aligned with relevant standards and industry best practice**
- **Detail the process for escalating and reporting risks**
- **Convey the Organization's commitment to the periodic review and verification of the Framework and its continual improvement**
- **Describe the resources available to assist those with accountability or responsibility for managing risks**
- **Ensure the department meets its risk reporting obligations.**

**Source: Risk Management Framework, Dept of Edu Australia**

# Benefits of Risk Management

- **Effective management of adverse events or opportunities that impact on our purpose and objectives**
- **Ability to make informed decisions regarding management of potential negative effects of risk and take advantage of potential opportunities**
- **Improved planning and performance management processes — enabling us to focus on core business service delivery and implement business improvements**
- **Ability to direct resources to risks of greatest significance or impact**
- **Greater organizational efficiencies through avoiding 'surprises'**
- **Creation of a positive organizational culture in which people understand their role in contributing to the achievement of objectives**.

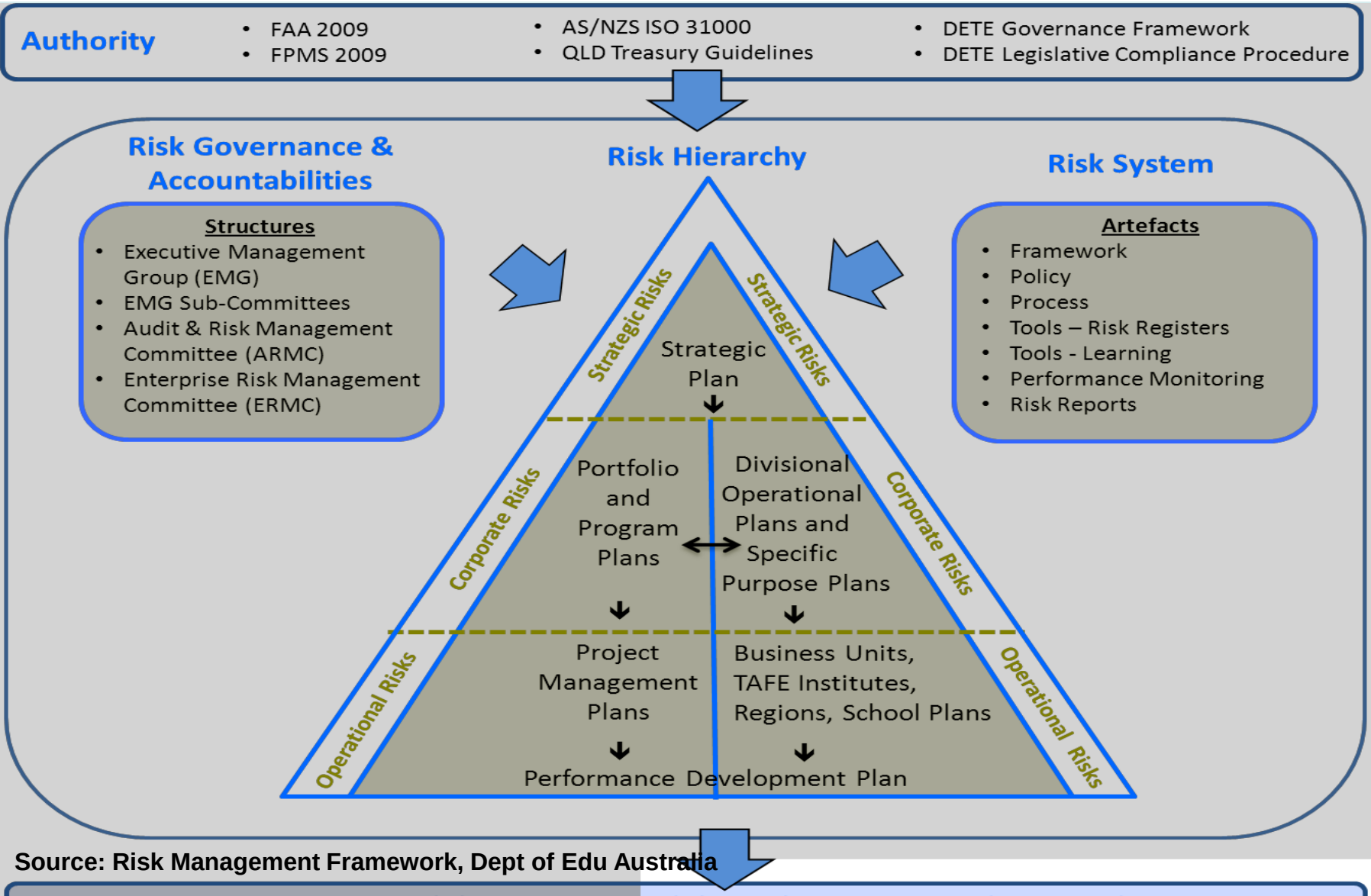
**Source: Risk Management Framework, Dept of Edu Australia**

# Principles underpinning the Risk Framework

- **Creating and protecting value** – risk management contributes to the achievement of our objectives and improves performance in areas such as corporate governance, program and project management, and health and safety of staff and students.
- **An integral part of all organisational processes** – risk management is not a stand-alone activity performed in isolation. Rather, it is an integral part of our governance and accountability arrangements, performance management, planning and reporting processes.
- **Part of decision-making** – risk management aids decision-makers to make informed choices, prioritise activities and identify the most effective and efficient course of action.
- **Explicitly addressing uncertainty** – risk management identifies the nature of uncertainty and how it can be addressed through a range of mechanisms, such as sourcing risk assessment information and implementing risk controls.
- **Systematic, structured and timely** – risk management contributes to efficiency and to consistent, comparable and reliable results.

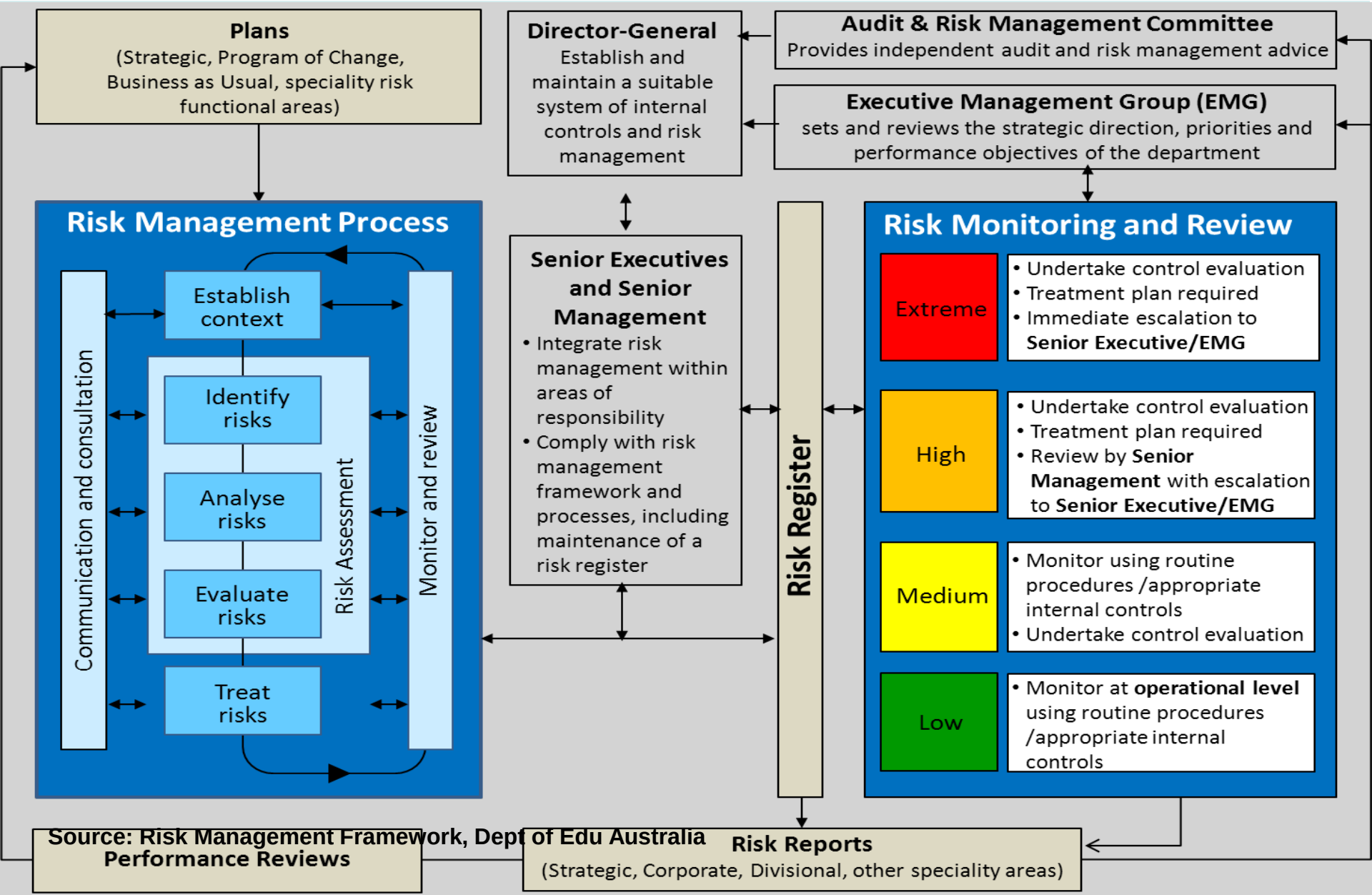
**Source: Risk Management Framework, Dept of Edu Australia**

# Enterprise Risk Management Framework




Source: Risk Management Framework, Dept of Edu Australia

# Department of Education, Training and Employment Risk Management Process



# Reading Material

- Part of Chapter 1 from Secrets of Computer Espionage, by Joel McNamara
- Information Security Risk Analysis, by Thomas R. Peltier
  - Soon to be on reserve at the library
  - Identifies basic elements of risk analysis and reviews several variants of qualitative approaches
- "Information Security Risk Assessment: Practices of Leading organizations", By GAO
  - http://www.gao.gov/special.pubs/ai99139.pdf
  - Case studies of risk analysis procedures for four companies
- "Risk Management Guide for Information Technology Systems", NIST
  - http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
  - Outlines steps for risk assessment

# References

- **Australia Security Portal**

  http://www.microsoft.com/australia/security

- **Microsoft Security Risk Management Guide**

  http://www.microsoft.com/technet/security/guidance/secrisk

- **MOF - Security Management**

  http://www.microsoft.com/technet/itsolutions/cits/mo/smf/mofsmsmf.mspx

- **Additional security tools and content**

  http://www.microsoft.com/security/guidance

# References

- NIST http://www.nist.gov
  - *Security Self-Assessment Guide for Information Technology Systems* (SP-800-26)
- IT Governance Institute http://www.isaca.org
  - *Control Objectives for Information and Related Technology* (CobiT)
- ISO http://www.iso.org
  - ISO 17799 - *ISO Code of Practice for Information Security Management*
- SAI Global http://www.standards.com.au
  - *AS/NZS 4360:2004 - Risk Management*
  - *AS/NZS 7799.2:2003 - Information Security Management*
- Microsoft Security Risk Management Guide
  - *http://www.microsoft.com/technet/security/guidance/secrisk*

# Thank You

**Dr Prem Chand**

**premchand64@gmail.com**

**Ph: +91-981129807**