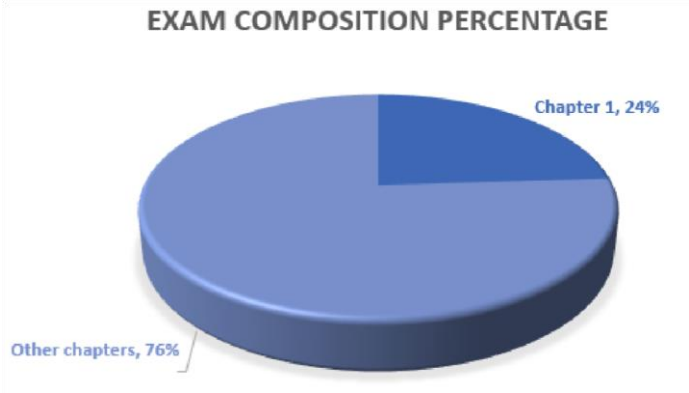
CISM MASTER CHEAT SHEET

CHAPTER 1:

Information Security Governance

Exam Relevance: 24% (approximately 48 questions)



Objective

Ensure that the information security manager has the knowledge to establish and maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives, information risk is managed appropriately and program resources are managed responsibly

Information Security Governance Overview

- **Information** has become an indispensable component of conducting business for virtually all organizations.
- **Information security governance** is the set of responsibilities and practices exercised by the board and executive management

Information vs. Knowledge

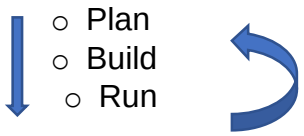
- **Information** can be defined as "**data endowed with meaning and purpose**." It is the substance of knowledge.
- **Knowledge** is, in turn, captured, transported and stored as **organized information**.

Information Security Governance

- Must be addressed at the **highest organizational level**
- Is part of **enterprise governance**
- **Executive management & board of directors** are accountable and must provide the necessary: ○ Leadership ○ Organizational structures ○ Processes

Management Tasks

- Any management process involves four key phase:



- IS governance focuses on high-level planning as a foundation for management activities

Information Security Manager's Responsibility

Executive management looks to the ISM to:

- **Define and manage** the information security program
- **Provide education and guidance** to the executive team
- **Present options** and information to enable decision making
- Acts an **information security advisor**

Importance of Information Security Governance

Benefits of strong information security governance include:

- Improving trust in customer relationships
- Protecting the organization's reputation
- Providing accountability for safeguarding information during critical business activities

Importance of Information Security Governance

Effective information security can add significant value to organizations by:

- **Reducing losses** from security-related events
- **Providing assurance** that security incidents and breaches are not catastrophic

Frameworks Enable Governance

- Establish:

- Basis for consistent/ **repeatable behavior** ○ Eliminates the "**moving target**"
- Formal, documented evidence of stewardship
- Demonstrates due diligence to employee / business partners/customers/other stakeholders
- Should serve as basis for audit criteria and employee evaluations

IT is a Basic Business Requirement

- Rules are required for all types of business processes and activities:
  - Sales processes, hiring firing routines, payables accounting, workplace etiquette, environmental/ disposal practices
- Information security is no different:
  - Relatively complex rules need to be spelled out to all information system stakeholders/users

Most Governance Transcends Technology

- Based on principles that go beyond a particular technology or platform:
  - "**Information is a valuable asset that requires protection from unauthorized access or disclosure**."
- Anchored in sound **business goals** and ideals
- Helps organization deal with rapidly changing technological environment:
  - Passwords… pass phrases… two keys… biometrics

Governance Owner/ Sponsor

- Depends on how information security is integrated into the organization
- Elevation of information security to the level of an officer within an organization is evidence that **senior management understands** the need to integrate information security governance into the overall enterprise governance framework ○ Example: if role exists, Chief Information Security Officer
- The **CISO** position has been gaining popularity.

○

Percentage of respondents saying their companies have a security executive:

- In 2011, > 80%
- In 2006, 22% ○ One-third of CISOs report to CIOs ○ 35% of CISOs report to CEOs

○ 28% of CISOs report to board of directors

Outcomes of Information Security Governance

- **Strategic alignment**: ○ Aligned with **business strategy** to support objectives
- **Risk management**
  - ○ **Mitigate** risk and **reduce** impacts to **acceptable levels**
- **Value delivery** ○ Optimizing security investments **in support of objectives**
- **Resource optimization**
  - ○ Security knowledge/ infrastructure used efficiently/ effectively
- **Performance measurement**
  - ○ Monitoring and reporting to ensure objectives achieved
- **Integration** ○ Integrate relevant assurance factors to ensure that processes operate as intended from end to end

Effective Information Security Governance

- **BMIS-** a clear organizational strategy for preservation is equally important to and must accompany a strategy for progress
- **CMU-** viewing adequate security as a non-negotiable requirement of being in business

Business Goals and Objectives

- **Corporate governance** is the set of responsibilities and practices exercised by the board and executive management:
- Goals include:
  - Providing **strategic direction**
  - ○ Ensuring that objectives are achieved
  - ○ Ascertaining that risk is **managed appropriately** ○ Verifying that the enterprise's resources are used responsibly

○

- What is information security governance?
    - Is a subset of corporate governance
    - Provide strategic direction for security activities and ensures that objectives are achieved
    - Ensures that information security risk is appropriately managed ○ Also helps ensure that information resources are used responsibly
- To achieve effective information security governance, management must establish and maintain a **framework** ○ **Framework** will guide the development and management of a comprehensive information security program that supports business objectives
- The governance framework generally consists of:
    - A comprehensive **security strategy** linked with business objectives ○ **Security policies** that address each aspect of strategy, controls and regulation
    - A complete set of **standards** for each policy
    - An **organizational structure** void of conflicts of interest with sufficient authority and resources
    - **Metrics and monitoring** processes to ensure compliance and provide feedback

Scope and Charter of Information Security Governance

- Information security deals with ***all*** **aspects** of information.
- **IT security** is concerned with security of information within the boundaries of the technology domain

Roles and Responsibilities of Senior Management

- **Board of directors/ senior management** ○ Information security governance
- **Executive management** ○ Implementing effective security governance and defining the strategic security objectives
- **Steering committee**
  Ensuring that all stakeholders impacted by security considerations are involved
- **Chief information security officer (CISO)** ○ Responsibilities currently range from the CISO who reports to the CEO to system administrators who have part-time responsibility for security management

○

Information Security Roles and Responsibilities

- **Information Security Manager** ○ Develops security strategy with input from key business units and approval of strategy by senior leadership ○ Educates management
- Information Security Requires:
    - **Leadership** and ongoing **support from senior management** ○ Integration with and **cooperation from organizational business unit** management
    - Establishing reporting and communication channels

Governance, Risk Management and Compliance

GRC-approach adopted by many organizations to combine assurance processes including:

- Internal Audit
- Compliance programs (SOX)
- Enterprise risk management (ERM)
- Incident management

An IT GRC program generally includes:

- Controls and policy library
- Policy distribution and response
- IT control self-assessment and measurement
- IT asset repository
- Automated general computer control collection
- Remediation and exception management
- Reporting
- Advance IT risk evaluation and compliance dashboards

Business Model for Information Security

•

Model originated at the Institute for Critical Information Infrastructure Protection

- A business-oriented approach to managing information security
- Best viewed as flexible, 3-D, pyramid-shaped structure made up of four elements linked by six dynamic interactions

Assurance Process Integration-Convergence

Information security has traditionally been executed in silos, using different terminology and reporting structures. Drivers for convergence are:

- Rapid expansion of the enterprise ecosystem
- Value migration from physical to information-based and intangibles assets
- New protective technologies blurring functional boundaries
- New compliance and regulatory regimes
- Continuing pressure to reduce cost

Goals of convergence are to:

- Reduce security gaps
- Minimize duplication of efforts
- Increase return on security investment

Information Security Concepts and Technologies

- **Access Control**-who/how someone can access a resource
- **Auditability**-enable reconstruction, review and examination of sequence of events
- **Authentication**-verify identity: something you know, something you have and something you are
- **Authorization**-what you can do once you have access
- **Availability**-accessible and usable when required
- **Confidentiality**-data secrecy
- **Integrity**-assurance of no unauthorized modification in processing, transmission and storage
- **Layered security**-defense in-depth
- **Nonrepudiation**-cannot deny

Governance and Third-party Relationships

Rules in processes for:

- Service providers
- Outsourced operations
- Trading partners
- Merged or acquired organization

Information Security Governance Metrics

- **Metrics** is a term used to denote measurements based on one or more references and involves at least two points, the measurement and the reference.
- **Contemporary security metrics** usually *fail* to tell us about the state or degree of safety relative to a reference point.
- It is difficult or impossible to manage any activity that cannot be measured • Standard security metrics may include: ○ Downtime due to viruses ○ Percentage of servers patched ○ Number of penetrations of systems
- No metric in and of itself actually provides information on how *secure* the organization actually is, however-all that can be stated is that:
    - Some organizations are attacked more frequently and/or suffer greater losses than others.
    - There is a strong correlation between good security management and practices and relatively fewer incidents and losses.
- Key goal indicators **(KGIs)** and key performance indicators **(KPIs)** can be useful in providing information about achievement of process or service goals
- KGIs tend to reflect more **strategic goals**
- KPIs tend to reflect more **tactical goals**
- **Strategic alignment** of information security in **support of organizational objectives** is a highly desirable goal
- The best overall indicator that security activities are in alignment with business objectives is a **security strategy that defines security objectives in business terms**
- Indicators of alignment are as follows:
    - The extent to which the security program demonstrably enables specific business activities
    - Business activities delayed or not undertaken because of inadequate risk management capability
    - A security organization that is responsive to **defined business requirements**
    - Organizational and security objectives that are defined and clearly understood by all involved in security and related assurance activities
    - Security programs that are mapped to organizational objectives ○ A security steering committee consisting of key executives with a charter to ensure ongoing alignment of security activities and business strategy
- **Value delivery** occurs when security investments are optimized in support of organizational objectives

•

- **KPIs and KGIs** are used to demonstrate value delivery
  Information security resource management includes: ○ Processes to plan, allocate, and control information security resources ○ People, processes, and technologies for improving the efficiency and effectiveness of business solutions
- Indicators of effective resource management can include:
  - Infrequent problem rediscovery
  - Effective knowledge capture and dissemination
  - The extent to which security-related processes are standardized ○ Clearly defined roles and responsibilities
  - Information security functions incorporated into every project plan ○ The proper organizational location, level of authority and number of personnel for the information security function
- **Measuring, monitoring, and reporting** on information security processes is required to ensure that organizational objectives are achieved
- Metrics that provide an indication of the performance of the security machinery are among the most frequently used types of performance measures
- Indicators of effective performance measurement:
  - The **time** it takes to detect and report security-related incidents ○ The number and frequency of subsequently discovered unreported incidents
  - **Benchmarking** comparable organizations for costs and effectiveness ○ The ability to determine the effectiveness/efficiency of controls ○ Clear indications that security objectives are being met
  - The absence of unexpected security events ○ Knowledge of **impending threats**
  - Effective means of determining **organizational vulnerabilities** ○ Consistency of log review practices
  - Results of business continuity planning/ disaster recovery tests ○ The extent that key controls are **monitored**
  - The percentages of metrics **achieving defined criteria**

Assurance Process Integration

- It is important for the ISM to **integrate assurance functions** in order to: Increase security effectiveness, reduce duplication efforts, and minimize gaps in protection
- KGIs to support assurance integration may include:

- No gaps in information asset protection
- Elimination of unnecessary **security overlaps**
- Seamless integration of assurance activities
- Well-defined roles and responsibilities

Information Security Strategy

- An information security strategy should:
  - State **objectives/ purpose/ goals**
  - Delineate principal policies and plans for achieving objectives/ purpose/goals
  - Define the range of business and desired state for the business
  - Provide the **basis for an action plan** – based on available resources and constraints; must contain provisions for monitoring and metrics to determine the level of success
- Below are some of the common **pitfalls** for an Information Security Strategy that an ISM must be cautious from:
  - Overconfidence
  - Optimism
  - Anchoring
  - The status quo bias
  - Mental accounting
  - False consensus
- Objectives of information security strategy must be **clearly defined** and **accompanied by metrics** developed to determine if the objectives are being achieved
- The six major **goals of governance** are:
  - Strategic alignment
  - Effective risk management
  - Value delivery
  - Resource management
  - Performance management
  - Process assurance integration
- The goal of the information security strategy is to **protect the organization's information assets**
- In order to achieve the goal of the strategy, relevant information assets must be: **located, classified, labelled, and protected** based on its classification
- **Information** is an asset only to the degree it supports the primary purpose of the business
- Long term security strategy objectives should be in terms of a '**desired state'**
- Objectives should reflect well-articulated vision of desired outcomes for a security program
- **Business linkages** can uncover information security issues at the operational level

- The desired state should include a **snapshot of all relevant conditions** at a particular point in the future
- A **'desired state of security'** must be defined qualitatively in terms of attributes, characteristics and outcomes
  According to **COBIT**, the desired state is – 'Protecting the interests of those relying on information, and the processes, systems and communications that handle, store and deliver the information, from harm resulting from failures of availability, confidentiality and integrity
- The five key principles for governance and management of enterprise IT based on COBIT 5: ○ Meeting stakeholder needs ○ Covering the enterprise end-to-end ○ Applying a single, integrated framework ○ Enabling a holistic approach ○ Separating governance from management
- The desired state of security may also be defined as levels in the **Capability Maturity Model (CMM):**
  - **0. Nonexistent**: no recognition of need
  - **1. Ad hoc**: Risks are considered on an ad hoc basis – no formal processes ○ **2. Repeatable but intuitive**: Emerging understanding of risk and need for security
  - **3. Defined process**: Companywide risk management policy / security awareness
  - **4. Managed and measurable**: Risk assessment standard procedure, roles and responsibilities assigned, policies and standards in place
  - **5. Optimized**: Organization-wide processes implemented
- Determining the **current state of security** is also a critical activity where the same methodology can be applied as to finding out the desired state.
- A security strategy needs to include:
  - Resources needed ○ Constraints
  - A road map that includes people, processes, technologies, and other resources and a security architecture defining the business drivers • Achieving the **desired state** is a **long-term goal** of a series of projects • Information security strategy resources include:
  - Policies ○ Standards ○ Procedures ○ Guidelines ○ Architecture(s)
  - Controls – physical, technical, procedural
  - Countermeasures ○ Layered defenses ○ Technologies ○ Personnel security ○ Organizational structure ○ Roles and responsibilities ○ Skills ○ Training ○ Awareness education

•

Information security strategy constraints include: ○ Legal: laws and regulatory requirements ○ Physical: Capacity, space, environmental constraints ○ Ethics: Appropriate, reasonable and customary ○ Culture: Both inside and outside the organization

- ○ Costs: Time, money
- ○ Personnel: resistance to change, resentment against new constraints

Policies and Standards

- **Policies** are the high-level statements of management intent, expectations and direction
- **Standards** are the metrics, allowable boundaries or the process used to determine whether procedures meet policy requirements
- **Procedures** are the responsibility of operations, but are included here for clarity
- **Guidelines** for executing procedures are also the responsibility of operations
- **Information security architecture** is analogous to the architecture associated with buildings:
  ○ Concept ○ Design ○ Model ○ Blueprint ○ Build, development
- **Controls** are defined as the policies, procedures, practices, and organizational structure designed to provide reasonable assurance that business objectives will be achieved
- Controls can be physical, technical, or procedural
- **Countermeasures** are protection measures that reduce the level of vulnerability to threats and can be considered targeted controls
- **Technology** is one of the cornerstones of an effective security strategy accompanied by policies, standards, and procedures
- The first line of defense is trying to ensure the trust worthiness and integrity of new and existing personnel
- Personnel-related measures must be proportional to the sensitivity and criticality of the requirements of the position held
- Security **centralization/standardization** depends on the organizational structure
- A **decentralized security process** allows security administrators to be closer to the users and understand local issues better
- An employee's annual job performance and objectives can include security-related measurements
- The ISM needs to work with HR o define security roles and responsibilities
- A **skills inventory** is important in determining the resources available in developing a security strategy

- **Recurring security awareness program** aimed at end users reinforces the importance of information security
- Evidence indicated that the majority of end users are not aware of existing security policies and standards
- **Security awareness and training** has often produced the most cost-effective improvement in overall security
- **Audits** – both **internal** and **external** are one of the main processes used to determine information security deficiencies
- **Internal audits** in most larger organizations are performed by an **internal audit department**, generally reporting to either a chief risk officer (CRO) or to an audit committee of the board of directors
- **External audits** are most often conducted by the **finance department**
- The ISM must develop procedures for **handling compliance violations**
- **Threat assessment** is a task within risk assessment, but has a strategic component. It helps optimize risk response and facilitates policy development
- **Vulnerability assessments** should include assessing vulnerabilities in: processes, technologies, facilities
- The most common types of insurance that can be considered: first party, third party, fidelity bonds
- Business impact is the **'bottom line'** of risk
- It is generally easier to reduce a potential impact than to mitigate a risk or reduce a vulnerability
- **Outsourcing** is being used increasingly to cut costs but risks due to outsourcing may be difficult to quantify and potentially difficult to mitigate
- Outsourced security services must not become a critical single point of failure

Action plan to Implement Strategy

- Analysis of the **gap** between the **current state** and the **desired state** for each defined metric identifies the requirements and priorities for the overall plan or road map to achieve the objectives and close the gaps
- Policies must capture the intent, expectations and **direction of management**
- Security policies generally must be related to **the security strategy**
- Each security policy should state only **one general security mandate**
- Policies should rarely be more than few sentences long
- **Standards are the 'law'** developed from policy. It governs the creation of procedures and guidelines
- **Action plan metrics** are methods to monitor and measure progress and the achievement of milestones. Senior management is typically not interested in detailed technical metrics

•

Implementing Security Governance

Capability Maturity Models (CMM) are available for use on the implementation of security governance

- Risk assessment is a standard procedure and exceptions to following the procedure would be noticed by IT management
- Depending on the structure of the organization, each significant area needs to be evaluated separately
- Policies need to be reviewed to determine whether they address each of the CMM elements
- Objective is to achieve consistent maturity levels across specific security domains

Action Plan Intermediate Goals

- **Intermediate goals** are defined once the overall strategy has been completed

Information Security Program

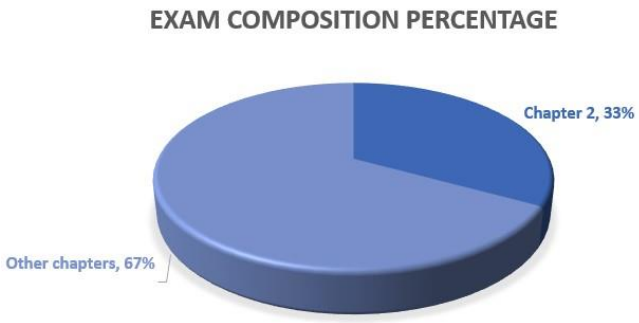
- Foundations of an information security program are: the **security strategy** and the **action plan**
- The objective of the information security program is to protect the interests of those relying in the information and the processes, systems, and communications that handle, store and deliver the information from harm, resulting from failures of:
  - **Confidentiality**
  - **Integrity**
  - **Availability**
- Information is **available** and usable when required, and the systems that provide it can appropriately resist attacks
- Information is observed or disclosed to only those who have a right to know
- Information is protected against unauthorized modification
- Business transactions and information exchanges between enterprise locations or with partners can be trusted

.

CHAPTER 2:

Information Risk Management and Compliance

Exam Relevance: 33% (approximately 66 questions)



Objective

Ensure that the information security manager understands how to manage information risk to an **acceptable level** to meet business and compliance requirements of an organization.

Risk Management Overview

- Risk management is a process aimed at achieving an **optimal balance** between realizing opportunities (+) and minimizing (-) vulnerabilities and loss.
- Risks are being **managed** so that they do not have an **adverse material impact** on business processes.
- Risk is **inherent** to all business activities.
- Risk management provides rationale and justification for virtually all information security activities.
- **Risk assessment** is a key requirement for effective information security strategy.
- Risk management **balances risk exposure** against **mitigation strategies**.
- **Controls and countermeasures** are designed as part of Risk Management Framework.
- Risk has its corresponding **likelihood**/probability of occurrence and consequence/business **impact**
- **Informed decision making:**
    - based on the organization's threat, vulnerability and risk profile
    - based on **risk exposure** and **potential consequences** of compromise
- Risk management results to organizational **acceptance** / **deference** based on an understanding of potential consequences of **residual risk.**

Risk Management Strategy

- A risk management **strategy** is an integrated business process and **has defined objectives**.
- Incorporates all processes, activities, methodologies and policies of risk management carried out in an organization.

Effective Information Security Risk Management

- Activities must be **continuously supported** by all members of the organization.
- **Senior management commitment** is required to achieve the objectives of the risk management program.
- All personnel must understand their **responsibilities** in terms of information security
- Personnel must also be **trained in applicable control procedures** • Compliance must be **tested** and **enforced** consistently.
- Develop a Risk Management Program based on the following requirements:
    - Establish context and purpose ○ Define scope and charter
    - Define authority, structure, and reporting
    - Ensure asset identification, classification and ownership ○ Determine objectives ○ Determine methodologies ○ Designate program development team
- Risk management is part of the **responsibility of the board of directors** or the equivalent to ensure that these efforts are effective.
- Management must be involved in and signs off on **acceptable risk** levels and risk management objectives.
- **Steering committee** sets the risk management **priorities**.
- Steering committee defines risk management **objectives** in terms **of supporting business** strategy.
- Information Security Manager is responsible for developing, collaborating, and managing the risk management program to meet the defined objectives.

Information Security Risk Management Concepts

- **Information security-related risk management** falls to the information security manager.
- Key information **security risk management concepts**:
    - Threats

- Vulnerabilities ○ Exposures ○ Risk ○ Impacts
- Controls ○ Countermeasures ○ Resource valuation ○ Information asset classification ○ Criticality ○ Sensitivity ○ Recovery Time Objectives **(RTOs)** ○ Recovery Point Objectives **(RPOs)** ○ Service Delivery Objectives **(SDOs)** ○ Acceptable Interruption Window **(AIW)** ○ Redundancy

- **Risk management functions** related to information security:
  ○ Service Level Agreement (SLAs) ○ System robustness and resilience ○ Business continuity/disaster recovery ○ Business process re-engineering ○ Project management timelines and complexity ○ Enterprise and security governance ○ Systems life cycle management ○ Policies -> standards -> procedures
- Information security manager (ISM) must have conceptual understanding of the following technologies: ○ Application security ○ Physical security ○ Environmental controls ○ Logical access controls ○ Network access controls
  - Routers, firewalls, and other network components ○ Intrusion detection/prevention ○ Wireless security ○ Platform security ○ Encryption and PKI ○ Anti-virus software and malware ○ Spyware and adware ○ Anti-spam
  - Telecommunications and VoIP

Risk Management Implementation

- Risk management contains a series of process of **weighing policy alternatives** in consultation with interested parties
- Risk management should be a **continuous and dynamic process** to ensure that changing threats and vulnerabilities are addressed in a timely manner.
- Risk management consists of the following processes:
  - Establish scope and boundaries
  - Risk assessment ○ Risk treatment ○ Acceptance of **residual risk** ○ Risk communication and monitoring
- Risk acceptance can be optional and be covered by both **risk treatment** and **risk communication**

- Determining the **appropriate level** of security depends on the potential risks that an organization faces.
- **Framework** for risk management should have the following requirements:
  - Policy ○ Planning and resourcing ○ Implementation program ○ Management review ○ Risk management process ○ Risk management documentation
- An efficient framework corresponds to **understanding the background** of the organization and its risk
- **Risk management framework** should also develop a structure and process for the development of risk management initiatives and controls
- **Framework approach** is critical in developing a set of criteria against which the risks will be measured
- Following key areas are essential in providing a comprehensive view of the organization's **internal environment** ○ Key business drivers
  - The organization's strengths, weaknesses, opportunities, and threats ○ Internal stakeholders ○ Organization structure and culture ○ Assets in terms of resources
  - Goals and objectives, and the strategies already in place to achieve them
- **Risk profile** is essential for effective risk management and can be easily achieved through a **risk register**
- Risk management context can be determined through defining the following:
  - Organization range and the process or activities to be assessed ○ Duration
  - Full scope of the risk management activities
  - Roles and responsibilities of various parts of the organization participating in the risk management process
- Evaluation of risk must be decided upon three important criteria: **Impact, likelihood**, and the **rules** that will determine whether the risk level is such that further treatment activities are required

Risk Assessment

- **Aggregate risk** can exist when a particular threat affects a large number of minor vulnerabilities that, in the aggregate, can have a significant impact.
- **Cascading risks** can also manifest unacceptable impacts as a result of one failure leading to a chain reaction of failures.
- The first step in a risk management program should be generating a comprehensive list of sources of **threats, risks, and events** that might impact achieving each objective
- Risk can be characterized by the following: ○ Origin

    - A certain activity, event or incident ○ Its consequences, results or impact ○ Specific reason for its occurrence ○ Protective mechanisms and controls ○ Time and place of occurrence
- Risk identification methodology can be any one of the following:
    - **Team-based brainstorming**: effective in building commitment and making use of different experiences
    - **Structured techniques**: flow charting, system design review, system analysis, hazard and operability studies, and operational modeling
    - **What-if and scenario analysis**: for less clearly defined scenarios such as identification of strategic risks and processes with a more general structure
- Threat categories are as follows ○ **Natural**: Flood, fire, cyclones, rain/hail, plagues, and earthquakes ○ **Unintentional**: fire, water, building damage/ collapse, loss of utility services and equipment failure
    - **Intentional physical**: Bombs, fire, water and theft
    - **Intentional nonphysical**: fraud, espionage, hacking, identity theft, malicious code, social engineering, phishing attacks and denial-of-service attacks
- The ISM must understand the **business risk profile** of the organization
- Risk is an **inherent** part of the business
- Risk **cannot entirely be eliminated**; every organization has a **level of risk it will accept**
- The ISM must determine the point where cost of losses **intersects** with cost of risk mitigation
- **Risk analysis**: the level of risk and its nature are assessed and understood ○ Involves thorough examination of the **risk resources** ○ Analysis of both positive and negative **consequences**
    - Assessment of existing **controls** that tend to minimize negative risks or enhance positive outcomes
- Risk level can be analyzed using **statistical analysis** of impact and likelihood
- Data that can be used to **estimate** impact and likelihood comes from: past experiences, international standards, market research, experiments, economic or engineering models, and specialist or expert advise
- **Quantitative risk analysis**: numerical values are assigned to both impact and likelihood; consequences may be expressed in monetary, technical, or operational terms
- **Semi-quantitative analysis** involves detailed analysis of magnitude and likelihood of potential consequences
- **Risk evaluation** involves the decision to which risk to treat and the treatment priorities
- **Risk treatment** involves four strategic options: Terminate, Transfer, Mitigate, Tolerate
- To **terminate** a risk is to stop the activity giving rise to that risk
- **Transferring** a risk involves tapping a third party to manage that specific risk

- **Mitigation** is to reduce the risk through appropriate control measures • **Tolerating** a risk means it falls to a certain acceptable level
- The **cost of mitigating risk must not exceed the value** of the asset
- Accepted risks should be evaluated and reviewed **regularly**
- **Residual risk** is the amount of risk that remains after countermeasures have been implemented
- Acceptance of residual risk depends on: **regulatory compliance, organizational policy, sensitivity and criticality of assets, acceptable levels of potential impacts, uncertainty inherent in the risk assessment approach, cost and effectiveness of implementation**
- **Impact** is the bottom line for risk management
- All risk management activities are designed to reduce impacts to **acceptable levels**
- **Impact** is a result of any **vulnerability exploited** by a **threat** that causes a **loss**
- **Business Impact Assessment (BIA)** helps prioritize risk management and provides the levels and types of protection required
- **Controls** that address the same risk are excessive and wasteful
- Risk assessment is important to be conducted from the **beginning of process through to the end**
- If the cost of specific controls or countermeasures exceed the benefits of mitigating a given risk, the organization may choose to **accept the risk** rather than incur the cost of mitigation
- **Total Cost of Ownership (TCO)** must be considered for the full life cycle of the control or countermeasure
- **Monitoring processes** is essential to have warning for events that could impact the security program

Information Resource Valuation

- **Resource valuation** is an essential undertaking required for an effective information risk management program
- It is essential for an ISM to **locate and identify all information resources**, determine **ownership and custodianship** of information, **assign classes** or levels of sensitivity and criticality to information resources, and make **classifications simple**
- **Asset classifications** are being used by end-user managers and security administrators to determine access levels
- **Data classification** reduces the risk and cost of over or under protecting information resources by correlating security to business objectives
- **Business Impact Analysis (BIA)** helps to identify the impact of adverse events on critical business processes or activities

- Common approach to performing impact assessment is to identify an asset's value proposition to the organization in terms of the impact associated with the loss of **integrity, availability, and confidentiality**
- Some impacts can be measured quantitatively, where others cannot

Recovery Time Objectives

- **Recovery Time Objectives (RTO)** depend upon numerous factors such as: cyclical need of the information and organization, interdependencies upon the information, organizational requirements, senior management requirement, legal or regulatory requirement, and customer service levels
- RTOs are needed to identify and develop **contingency strategies**
- **Shorter** RTOs require **costlier** contingency procedures
- There is a **break-even point** where the impact of the disruption will begin to be greater than the cost of recovery
- **Recovery Point Objective (RPO)** is determined based on the acceptable data loss in case of disruption of operations
- **Service Delivery Objective (SDO)** is the minimum level of service that must be restored after an event to meet business requirements
- **Third-party service providers** are sometimes tapped for risk transfer.
- It is important for the ISM to assess the **risk of any outsourcing process** where there should be appropriate information **risk management clauses** in the contract
- For outsourcing arrangements, the organization must have **appropriate controls** in place to facilitate the activity
- Considerations for outsourcing include: **criticality** of the business function, **complexity** of the process, **separation** setting control requirements, **regulatory** requirements, **changes** in internal and external business environment
- Some key clauses that should be part of **Service Level Agreements (SLA)** are: **right to audit** the vendor's books of accounts, **right to review** their processes, insistence on **standard operating procedures (SOP), right to assess skill sets** of vendor resources and advance information if the resources are to be changed

Integration with Life Cycle Processes

- **Change management** is an effective method to maintain adequate security protection
- **Proactive approach** enables the ISM to better plan and implement security policies and procedures in alignment with business goals and objectives
- It is more cost effective to **update risk regularly**
- **Life cycle approach** is the best way to employ to identify, analyze, assess and track risk

- **Top-down systematic approach** can benefit from supporting tools, training and assistance
- **Software tools** are also available to track the risk management life cycle

Security Control Baselines

- **Baselines** specify minimum security control requirement
- It is important to assess the level of security that is appropriate for an organization
- **Reporting significant changes** in risk to appropriate levels is a primary role of the ISM
- Risk assessment should be **updated as the organization changes**
- Risk assessment process should include an entry whereby a significant security breach or event will trigger a report to upper management

Training and Awareness

- **People** are generally the **greatest risk** to an organization, appropriate training can significantly mitigate risk
- End users should receive **training** on the importance of adhering to the security policies and procedures of the enterprise, responding to emergency situations, significance of logical access in an IT environment, privacy and confidentiality requirements

Documentation

- Appropriate **risk management documentation** that is **readily available** is required to effectively manage risk
- Inclusions to a **risk management documentation** should include: objective, audience, information resources, assumptions, and decisions
- **Risk management policy** document may include information such as:
    - Objectives of the policy
    - Scope and charter of risk management
    - Links between the risk management policy and the organization's strategic and corporate business plans
    - Extent and range of issues to which the policy applies ○ Guidance on what is considered acceptable risk ○ Risk management responsibilities
    - Support expertise available to assist those responsible for managing risks ○ Level of documentation required for various related activities

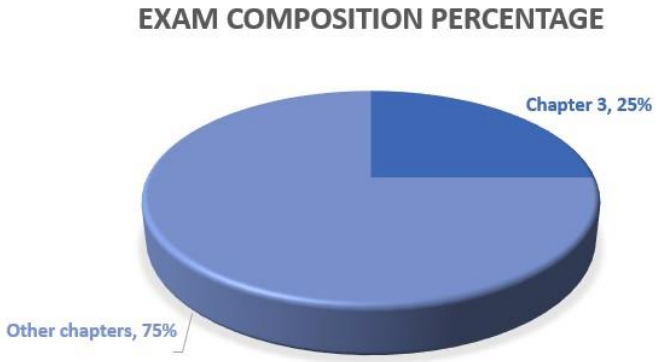
- A plan for reviewing compliance ○ Incident and event severity levels
- Risk reporting and escalation procedures, format, and frequency

- **General risk management documentation** should include:
  - A **risk register**
  - Consequences and likelihood of compromise
  - Initial risk rating
  - Vulnerability to external/internal factors ○ An inventory of information assets ○ A risk mitigation action plan

CHAPTER 3:

Information Security Program Development and Management

Exam Relevance: 25% (approximately 50 questions)



Objective

Ensure that the information security manager understands the broad requirements and activities needed to establish and manage the **information security program** in alignment with the **information security strategy**.

Information Security Program Management Overview

The three elements essential to ensure successful security program design, implementation and ongoing management:

- The **execution** of a well-developed information security strategy
- Must be well-designed with cooperation and **support from management** and stakeholders
- **Effective metrics** must be developed

The ISM must realize that the objectives and expected benefits will work best if defined in **business terms**.

- **Importance of Information Security Program**
  A well-executed security program will serve to effectively:
  - ✦ Design, implement, manage and monitor the security program, transforming strategy into actuality.
  - ✦ Provide the capabilities to meet security objectives.
  - ✦ Accommodate changes in security requirements.

- **Outcomes of Information Security Program Management** Objectives for information security governance include:
  - ✦ Strategic alignment
  - ✦ Risk management
  - ✦ Value delivery
  - ✦ Resource management
  - ✦ Assurance process integration
  - ✦ Performance measurement

Information Security Program Objectives

- Execute the information security strategy in the most **cost-effective** manner
- Maximize **support of business functions**
- Minimize **business disruptions**

Information security program management uses a structured grouping of projects to produce clearly identified **business value.**

Information Security Program Concepts

A **security program implementation** effort should include a series of specific control objectives:

- Technical
- Procedural
- Physical

Concepts

Implementing and managing a security program will require the information security manager to understand and have a working knowledge of a number of management and process concepts including:

- System development life cycles (SDLCs)
- Requirements development
- Specification development
- Control objectives
- Control design and development
- Control implementation and testing
- Control monitoring and metrics
- Architectures
- Documentation
- Quality Assurance
- Project management
- Business case development
- Business process reengineering
- Budgeting, costing and financial issues
- Deployment and integration strategies
- Training needs assessments and approaches
- Communications
- Problem resolution
- Variance and noncompliance resolution
- Risk management
- Compliance monitoring and enforcement
- Personnel issues

Technology Resources

Technology itself is not a control - technology is used to *implement* controls:

- It is essential that the Information Security Manager understands where a given technology fits into the basic prevention, detection containment, reaction and recovery framework.

There are numerous technologies related directly to information security with which the ISM should be familiar including:

- ✦ Firewalls
- ✦ Routers and switches
- ✦ IDS, NIDS, HIDS
- ✦ Cryptographic techniques (PKI, AES)
- ✦ Digital signatures
- ✦ Smart cards

Scope and Charter of an Information Security Program

- Since the scope and charter are generally not explicitly stated, the ISM must gain a thorough understanding of the organization's:
- Goals
- Risk appetite and tolerance
- Principles, Policies, Frameworks
- Processes
- Organizational Structures
- Culture, Ethics and Behaviors
- Information
- Services, Infrastructure and Applications
- People, Skills and Competencies

- The ISM must try to integrate information security policy into existing sets of people following established processes and policies using existing systems.

- The ISM must also identify the technologies in use that process the information covered by the information security policy

The Information Security Management Framework

- Should fundamentally describe the information security management components and their interactions.
- Information security management components include:

○ Roles ○ Policies ○ Standard operating procedures ○ Management procedures ○ Security architectures, etc.

- **Cobit 5**

The ISM should understand the benefits of the following principles as they apply to an information security management framework:

- Meeting Stakeholder Needs
- Covering the Enterprise End-to-End
- Applying a Single, Integrated Framework
- Enabling a Holistic Approach
- Separating Governance from Management

- **ISO/IEC 27001:2013**

The ISM should be aware of the breadth of the following information security management control areas:

- Information security policies
- Organization of information security
- Human resource security (controls that are applied before during or after employment)
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operation security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance (with internal requirements, such as policies, and with external requirements, such as laws)

Operational Components

- Operational components are ongoing activities that must be performed because of information security requirements
- Operational components that are part of an information security program include:
  - Standard operating procedures **(SOPs)** ○ Business operations **security practices**
  - **Maintenance and administration** of security technologies (e.g., identity management, access control administration, and SIEM monitoring and analysis)

- The ISM should determine the operational components needed to implement policies and standards: ○ Should then plan for deployment, monitoring and management of operational components
- Because many operational components fall outside of the information security domain (e.g., patching procedures), the ISM should leverage IT, business units and other resources to ensure that operational needs are thoroughly covered.
- For each operational component, the ISM should:
    - **Identify** the component owner
    - **Collaborate** to document key information needed for component effectiveness

Management Components

- **Sets the stage** for the information security program
- Takes place **less frequently** than operational components
- Are often responsibility of **middle and senior management** • Issues can be escalated to the **board level** (e.g., oversight)
- Include:
    - **Standards development** or modification ○ **Policy reviews**
    - **Oversight** of initiatives or program executions
- **Management objectives, requirements and policies** are key in shaping the rest of the information security program
- The information security manager must ensure that this process is executed with **appropriate consideration to legal, regulatory, risk and resource issues** as well as a suite of metrics needed for decision support
- Ongoing or **periodic analysis** of assets, threats, risks and organizational impacts must continue to be the basis for modifying security policies and developing or modifying standards
- The information security manager is well advised to exercise flexibility in making adjustments to standards and policy interpretation during the initial stages of a security program
- It is important that there is **management oversight** ensuring fulfillment of requirements and consistency with strategic direction

Administrative Components

- The ISM must **ensure effective administration** of the information security program including matters related to:

- Finance ○ HR
- Support functions

- Strong working **rapport with Finance and HR departments** will help facilitate an effective information security program execution
- The ISM must balance project efforts and ongoing operational overhead with:

○ Staff headcount ○ Utilization levels ○ External resources

- Resource utilization must be prioritized based on guidance from:
  - **Steering committee** ○ **Executive management**
- **Workload balancing** and **external resources** help addresses planned/unplanned spikes in activity
- Roles and responsibilities:

○ The ISM must:

- ✦ Ensure that **executive management** understands the risk implications of starting an initiative without full security diligence ○

Executive management must:

- ✦ **Decide** if the initiative is important enough to warrant the risk

Educational and Informational Components

- Training and Education: ○ Can be considered **preventive measures** ○ Educate employees on:
  - ✦ Threats and risks
  - ✦ Appropriate practices
  - ✦ Repercussions of non-compliance ○ Include:
  - ✦ Organizational policies and procedures
  - ✦ Appropriate Use Policy
  - ✦ Protection of Proprietary Information (POPI) Policy
  - ✦ Employee monitoring ○ Generally communicated and administered by HR function

Defining an Information Security Program Road Map

- Key goals are universal and include:
  - Strategic alignment ○ Risk optimization ○

Resource optimization
  - Benefits realization
- Value delivery

- An ISM road map helps define what each process means to a given organization.

- Because the ISM rarely begins with a blank slate, the ISM must be able to review and evaluate the security level of existing: ○ Data
  - Applications
  - Systems ○ Facilities
  - Processes

*Security reviews need to have an objective, scope, constraints, approach and result

Gap Analysis – Basis for an Action Plan

- The ISM must:
  - Identify where **control objectives** are not adequately supported by control activities
  - Establish procedures for **continuously monitoring** achievement of control objectives
  - Design an information security with the flexibility to **evolve** and **mature**

Information Infrastructure and Architecture

- **Infrastructure**: the underlying base or foundation upon which information systems are deployed
- **Security infrastructure**: the foundation that enables security resources to be deployed
- When infrastructure is designed and implemented to support policies and standards, the infrastructure is said to be secure

Enterprise Information Security Architecture

- Information security architecture includes multiple layers ranging from **contextual to physical**
- The design is tightly aligned with the purpose. **Good architecture** is an articulation of policy

Objectives of Information Security Architectures

Architecture:

- Helps manage complexity by acting as an integrated road map for projects and services
- Provides simplicity and clarity through layering and modularization • Take into account organizational:
    - Goals ○ Environment
    - Technical (and business) capabilities
- Is broader than “technology”
- Has a ***business*** focus

- The underlying principle for architecture is that the objectives of **complex systems** must:
- Be comprehensively **defined**
- Have **precise specifications** developed
- Have their structures engineered and **tested** for form, fit and function
- Have their performance **monitored and measured** in terms of the original design objectives and specification

Architecture Implementation

- Development of comprehensive enterprise security architecture
- Approach
- Framework considerations
- Numerous architectural frameworks have been developed to address the need for overall comprehensive model for information systems: ○ COBIT ○ ITIL
    - ISO/IEC 27001:2013 ○ SABSA

Personnel, Roles and Responsibilities and Skills

- **Personnel**:
  - Architects, designers, builders, developers, testers and others involved in the construction of the information security program
  - Likely to be different from the personnel that will administer systems once they are functioning
- **Roles**:

○ Responsibilities and/or **access rights** assigned according to function

- Personnel and skills differ for:

○ Development of the ISM Program

- ✦ Architects
- ✦ Designers
- ✦ Builders
- ✦ Developers
- ✦ Testers ○ Operations of the ISM Program
- ✦ Security analysts
- ✦ Database administrators
- ✦ Network administrators

- **Role:** A designation assigned to an individual by virtue of a job function responsibilities
- **Responsibility**: A description of some procedure or function related to the role that someone is accountable to perform
- Skills: Training, expertise and experience held by the personnel for a given job function
- Culture:

○ Represents the organizational behavior:

- ✦ Methods for navigating and influencing the organization's formal and informal structures
- ✦ Attitudes
- ✦ Norms
- ✦ Level of teamwork
- ✦ Existence or lack of turf issues
- ✦ Geographic dispersion

Security Awareness, Training and Education

- **Background and training** is necessary for execution of tasks
- Training classes should be tailored for those with security job responsibilities
- An information security **awareness program** must also include end-user training

- Topics for awareness training can include topics such as:
- **Choosing passwords** wisely and protecting them from exposure
- Avoiding e-mail and web-based **malware**
- Recognizing **social engineering** attacks
- Recognizing and **reporting** security incidents
- Securing **electronic and paper media** against theft and exposure
- Spotting malware that could lead to identity theft and desktop spying
- **Backing up** work-related files

Documentation

- Primary documentation used to implement the information security program include:
- Policies
- Standards
- Procedures
- Guidelines

- Some of the documentation required will typically include:
- Program objectives
- Road maps
- Business cases
- Resources required
- Controls
- Budgets
- Systems designs/ architectures
- Policies, standards, procedures, guidelines
- Project plan milestones, time lines
- KGIs, KPIs, critical success factors (CSFs), other metrics
- Training and awareness requirements
- Business impact and risk analysis
- Service level agreements (SLAs)
- Severity criteria
- Declaration criteria

Program Development and Project Management

- A **gap analysis** will identify a series of projects that will improve the information security program ○ Each project must:

- ✦ Have a **defined time, budget and measurable objectives**
- ✦ Make the environment more secure without otherwise causing control weaknesses in other areas

- The ISM prioritizes the portfolio of projects so that:
  - **Interdependent projects** do not delay each other ○ Resources are optimally allocated
  - Results are smoothly integrated into existing operations
- The ISM should employ generally accepted project management techniques, such as: ○ Goal setting ○ Progress monitoring ○ Tracking deadlines

○ Assigning responsibilities

Risk Management

- Virtually all aspects of the information security management (ISM) program aim to reduce risk to an **acceptable level**
- One risk management aspect of the ISM program is **incident management** • The ISM must understand and develop the requisite skills to:

○ Identify ○ Evaluate/analyze ○ Manage (respond to) risk

- Knowledge and skills to manage risk as part of the ISM program may include:
  - Program development life cycle risk ○ Program management risk ○ Project risk
  - Vulnerability assessment methods
  - Threats specific to the information security manager's organization ○ Risk analysis approaches ○ Risk response options
  - Ability to understand and assess potential impacts if risk are exploited ○ Risk monitoring and reporting ○ Threat analysis

Business Case Development

- Purpose of a **Business case**
- Obtain support of **influencers and decision makers**
- Require those proposing projects to provide a clear value proposition
- Enable:
  - Comparison between competing projects/proposals ○ Objective decision-making
  - Measurability of project success against projection

- Business case content:

- Reference
- Context
- Value proposition
- Focus
- Deliverables
- Dependencies
- Project metrics
- Workload
- Required resources
- Commitments

- Objectives of the **business case process** is to be:
- Adaptable
- Consistent
- Business oriented
- Comprehensive
- Understandable
- Measurable
- Transparent
- Accountable

Program Budgeting

- Program budget has a significant impact on program success. Project budget elements to be considered include:
- Employee time
- Contractor and consultant fees
- Equipment
- Space requirements
- Testing resources
- Support documentation
- Ongoing maintenance
- Contingencies for unexpected costs

General Rules of Use/Acceptable Use Policy

- Rules for all personnel include policies and standards for:
- Access control
- Classification
- Marking and handling of documents and information
- Reporting requirements

- Disclosure constraints

Information Security Problem Management Practices

- Requires a systematic approach to:
- Understanding the aspects of the issue
- Defining the problem
- Designing an action program
- Assigning responsibilities and due dates for resolution

Vendor Management

- ISM is responsible for the **oversight and monitoring** of external providers.

Program Management Evaluation

- Evaluation of program management components will reveal the extent of **management support** and the overall depth of the program:
- Very technical, tactically-driven programs are **weak** in management components

- Considerations of program management components include:
- Is there thorough documentation of the program itself? Have key policies, standards and procedures been reduced to accessible operating guidelines and distributed to responsible parties?
- Do responsible individuals understand their roles and responsibilities? Are roles and responsibilities defined for members of senior management, boards, etc.? Do these entities understand and engage their responsibilities?
- Are responsibilities for information security represented in business manager's individual objectives and part of their individual performance rating?
- Are policies and standards defined, formally approved and distributed?
- Are business unit managers involved in guiding and supporting information security program activities?
- Is there a formal steering committee?
- How is the program positioned within the organization?
- To whom is the program accountable?

- Does this positioning impart an appropriate level of authority and visibility for the objectives that the program must fulfill?
- Does the program implement effective administration functions?
- Are meaningful metrics used to evaluate program performance? Are these metrics regularly collected and reported?
- Are there forums and mechanisms for regular management oversight of program activities? Does management regularly reassess program effectiveness?

Information Security Liaison Responsibilities

- Physical/Corporate Security
- IT Audit
- Information Technology Unit
- Business Unit Management
- Human Resources
- Legal Department
- Employees
- Procurement
- Compliance
- Privacy
- Training
- Quality Assurance
- Insurance
- Third Party Management
- Project Management Office

Other Security Program Services and Operational Activities

- Cross-organizational responsibilities
- Incident Response
- Security Reviews and Audits
- Management of Security Technology
- Due Diligence
- Compliance Monitoring and Enforcement
- Assessment of Risk and Impact
- Outsourcing and Service Providers
- Cloud Computing
- Integration with IT Processes

Controls and Countermeasures

- A vital element of an information security program is a **roles and responsibilities matrix**.
- An ISM must understand the **general risk appetite** of an organization to determine whether gaps in an information security program exist have reached acceptable levels.
- Key criteria in selecting technical elements of an information security road map are thus: ○ Adoption of a security architecture
  - The ability of formally delegate responsibility for operating within it

Control Categories

- Control categories include:
- Preventive
- Detective
- Corrective
- Compensatory
- Deterrent

Other Control and Countermeasures

- Control Design Considerations
- Control Strength
- Control Methods
- Control Recommendations
- Countermeasures
- Physical and Environmental Controls
- Control Technology Categories
- Technical Control Components and Architecture
- Control Testing and Modification
- Baseline Controls

Control Technology Categories

- **Native control technologies** comprise an essential part of the technology environment:
- **Out-of-the-box security features** can be integrated with business information systems
- Generally configured and operated by IT

- Supplemental control technologies can also be used:
- Components can be added on to an information systems environment
- Usually provide some function that is not available on the native components (network intrusion detection), or that is more appropriate to implement outside of primary business application systems
- Tend to be more specialized than native control technologies

- Management support technologies are frequently used:
- Can automate security-related procedures, provide management information processing, and/or increase management efficiency
- Examples include security information management (SIM) tools, compliance monitoring scanners and security event analysis systems
- Are often used by information security group independently of information technology

Technical Control Components and Architecture

- Analysis of technical components and architecture must be performed:
- When analyzing **technical security architecture**, the ISM must use a clearly defined set of measurable criteria to enable tracking of performance metrics
- A few possible criteria for analyzing technical security architecture and components might include ○ Control placement ○ Control effectiveness ○ Control efficiency ○ Control policy ○ Control implementation

Security Program Metrics and Monitoring

- Used to track and guide a program with the following:
- Metrics Development
- Monitoring Approaches
- Measuring Information Security Management Performance

- Measuring Information Security Risk and Loss
- Measuring Support of Organizational Objectives
- Measuring Compliance
- Measuring Operational Productivity
- Measuring Security Cost Effectiveness
- Measuring Organizational Awareness
- Measuring the Effectiveness of Technical Security Architecture
- Measuring the Effectiveness of Management Framework and Resources
- Measuring Operational Performance
- Monitoring and Communication

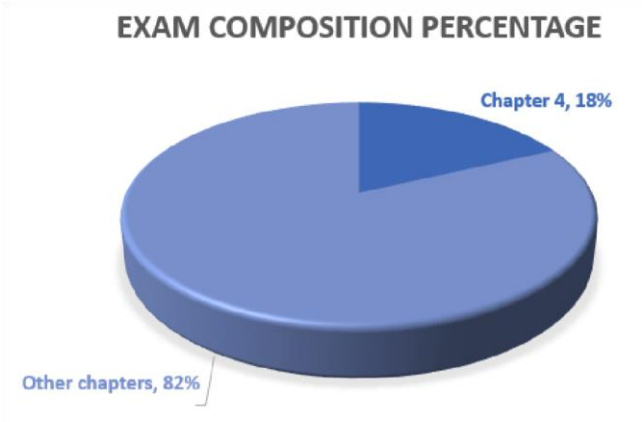
Common Information Security Program Challenges

- Management Support
- Funding
- Staffing

CHAPTER 4:

Information Security Incident Management

Exam Relevance: 18% (approximately 36 questions)



Objective

Ensure that the information security manager has the knowledge and understanding necessary to **plan, establish and manage** the capability to **detect, investigate, respond** to and **recover** from information security incidents to **minimize business impact**.

Incident Management Overview

- Purpose is to **manage** the impact of unexpected disruptive events to **acceptable levels**
- Possible disruptions may be:
  - Technical ○ Physical ○ Environmental
- Any type of incident that can significantly affect an organization's **ability to operate** or that **may cause damage** must be considered by the ISM
- Goals for incident management:
  - **Detect** incidents quickly ○ **Diagnose** incidents accurately ○ **Manage** incidents properly ○ **Contain** and minimize damage ○ **Restore** affected services ○ Determine **root causes**
  - Implement improvements to **prevent recurrence** ○ **Document** and report

Incident Response Procedures

- **Incident response** procedure (IRP) enable a business to:
- Respond effectively when an incident occurs
- To continue operations in the event of disruption

- Survive interruptions or security breaches in information systems
- Plans must be:
- Clearly documented
- Readily accessible
- Based on the long-range IT plan
- Consistent with the overall business continuity and security strategies
- As a part of the planning process, a number of decisions must be **made by the stakeholders** and **ratified by senior management**. These will include:
- Incident detection capabilities
- Clearly defined severity criteria
- Assessment and triage capabilities
- Declaration criteria
- Scope of incident management
- Response capabilities
- The process of developing and maintaining an appropriate plan for the defined scope of incident management and response should include:
- Incident Response Planning
- Disaster Recovery Planning
- Business Continuity Planning

Importance of Incident Management

- The following factors have contributed to the criticality of incident management and response:
- The **trend** of both increased occurrences and escalating losses resulting from information security incidents
- The **increase of vulnerabilities** in software or systems can affect large parts of an organization's infrastructure and impact operations
- **Failure of security controls** to prevent incidents
- **Legal and regulatory** groups requiring the development of an incident management capability
- The **growing sophistication** and capabilities of profit-oriented attackers
- Advanced persistent threats **(APTs)**

Outcomes of Incident Management

- Outcomes of good incident management and response include an organization that:
- Can deal effectively with **unanticipated** events

- Has sufficient **detection and monitoring** capabilities
- Has well defined **severity and declaration criteria** as well as defined **escalation and notification processes**
- Has response capabilities that demonstrably **support the business strategy**
- **Proactively** manage risks of incidents appropriately
- **Periodically tests** its capabilities
- Provide **monitoring and metrics** to gauge performance of incident management and response capabilities

Concepts

- **Incident handling** is one service that involves all the processes or tasks associated with handling events and incidents. It involves multiple functions:
- Detection and reporting
- Triage
- Analysis
- Incident response

- Effective incident management will ensure that incidents are
- Detected
- Recorded
- Managed to limit impacts
- **Incident response** is the last step in an incident handling process

It encompasses:
- Planning, coordination, and execution of any appropriate mitigation
- Recovery strategies and actions

Incident Management Systems

- **Incident management systems** automate many manual processes:
- Can deliver only **filtered information** indicating an incident to be handled by the incident management team (IMT)
- Can be **distributed or centralized**

- An effective incident management system should:
- Consolidate inputs from multiple systems

- Identify incidents or potential incidents
- Prioritize incidents based on business impact
- Track incidents until they are closed
- Provide status tracking and notifications
- Integrate with major IT management systems
- Implement good practices guidelines

Incident Management Organization

- **Incident management** is a component of risk management
- Activities in incident management include meeting with emergency management personnel
- Emergency management activities focus around activities that happen **after the event**

Responsibilities

- The ISM's incident response-related responsibilities include:
- Developing the information security incident management and response plans
- Handling and coordinating information security incident response activities effectively and efficiently
- Validating, verifying and reporting of protective or countermeasure solutions, both technical and administrative
- Planning, budgeting and program development for all matters related to information security incident management and response

- Incident response goals include:
- **Containing** and minimizing the effects of the incident so that damage and losses do not escalate out of control
- **Notifying** the appropriate people for the purpose of recovery or to provide needed information
- **Recovering** quickly and efficiently from security incidents
- **Responding** systematically and decreasing the likelihood of recurrence
- Balancing operational and security processes
- Dealing with legal and law enforcement-related issues

- The ISM must define what constitutes a security-related incident:
- Malicious code attacks
- Unauthorized access to IT or information resources

- Unauthorized utilization of services
- Unauthorized changes to systems, network devices or information
- Denial of service
- Misuse
- Surveillance and espionage
- Hoaxes/social engineering

Senior Management Commitment

- Senior management commitment is **critical to the success** of incident management and response.
- Incident management and response:
  - Is a component of risk management
  - Needs the same level of support from the top

Incident Management Resources

- Develop a clear scope and objective
- Develop an implementation strategy

Policies and Standards

- The incident response plan must be backed up with well-defined policies, standards and procedures. This helps:

- Ensure activities are aligned with IMT mission
- Set correct expectations
- Provide guidance on operational needs
- Maintain consistency and reliability of services
- Clearly understand roles and responsibilities
- Set requirements for identified alternates for all important functions

Incident Response Technology Concepts

- IRT members should be familiar with:
- Basic Security Principles

- IRT members must understand the impact to organizational systems, including:

- Security vulnerabilities/weaknesses
- Internet
- Operating system(s)
- Malicious code
- Programming skills

Personnel

- Composition of IMT
- Information Security Manager
- Steering Committee/Advisory Board
- Perm/Dedicated Team Members
- Virtual/Temp Team Members

- Team organizational types:
- Centralized IRT
- Distributed IRT
- Coordinating IRT
- Outsourced IRT

- Factors for team composition:

- Mission and goals of program
- Nature and range of services offered
- Available staff expertise
- Consistency size and technology base
- Anticipated incident load
- Severity or complexity of incident reports
- Funding

Roles

- **Security steering group**- highest structure of an organization's functions related to information security
- **Information security manager**-IMT leader and main interface to SSG
- **Incident response manager**-IRT leader
- Inc**ident handler**-IMT/IRT team member
- **Investigator**-IMT/IRT team member
- **It security specialist**-IMT/IRT team member

- **Business managers**-business functions owners; information assets/system owners
- **IT specialists/representatives**-subject matter experts in IT services
- **Legal representative**-subject matter expert in legal
- **HR**-subject matter expert in HR area
- **Public relations (PR) representative**-subject matter expert in PR area
- **Risk management specialist**-subject matter expert in risk management
- **Physical security/facilities manager**-knowledgeable about physical plant and emergency capabilities

Skills

Team member skills include:

- Personal skills: ○ Communication ○ Leadership ○ Presentation
  - Ability to follow policies and procedures
  - Team
  - Integrity ○ Self-understanding ○ Coping with stress ○ Problem solving ○ Time management
- Technical skills:
  - Technical Foundation
  - Incident Handling

Awareness and Education

Incident response training must include the following target groups:

- End users
- Management
- IMT team
- General IT team

Audits

- Are performed to verify the incident response process conformance to ○ Policies ○ Standards ○ Guidelines ○ Procedures
- Provide an **objective view** of the overall completeness and functionality of the incident response plans

- Provide assurance that major gaps in the processes do not exist • Audits can be **internal or external**:
  - **Internal audits** are conducted by control specialists within the organization
  - **External audits** are performed by a third party and provide additional independence

Defining Objectives

The objectives of incident management are:

- **Handle incidents when they occur** so that the exposure can be contained or eradicated to enable recovery within an AIW
- Prevent previous incidents from recurring by **documenting** and **learning** from past incidents
- Deploy **proactive countermeasures** to prevent/minimize the probability of incidents from taking place

The Desired State

Incident management and response requires:

- Well-developed **monitoring capabilities** for key controls
- **Personnel trained** in assessing the situation, capable of providing triage, and managing effective responses
- Managers who:
  - Know when a disaster is imminent
  - Have well-defined criteria
  - Have the experience, knowledge and the authority to invoke the disaster recovery processes necessary to maintain or recover operational status

Strategic Alignment

Incident management must be aligned with an **organization's strategic plan**:

- Constituency-to whom does the IMT provide service?
- **Mission**-defines the purpose of the team
- **Services**-services should be clearly defined
- **Organizational structure**-the structure of the IMT should support the organizational structure
- **Resources**-sufficient staffing is necessary for effectiveness

- **Funding**-sufficient funding is required to ensure continuity of services
- **Management buy-in**-senior management buy-in is essential

Risk Management

- Successful outcomes of risk management include effective incident management and response capabilities
- Any **risk that materializes** that is not prevented by controls will constitute an **incident** that must be managed and responded to with the intent that it does not escalate into a disaster

Value Delivery

To deliver value, incident management should:

- **Integrate with business processes** and structures as seamlessly as possible
- Improve the capability of businesses to **manage risk and provide assurance** to stakeholders
- Integrate with **BCP**
- Become part of an **organization's overall strategy** and effort to protect and secure critical business function and assets
- Provide the backstop and optimize risk management efforts

Resource Management

- Optimizes **resource utilization** to meet objective within resource constraints
- Spans ○ Time ○ People ○ Budget ○ Technology
  ○ And other factors

Performance Measurement

- Performance measurements for incident management and response will focus on achieving the defined objective and optimizing effectiveness
- **KPIs and KGIs** should be defined and agreed upon by stakeholders and ratified by senior management

Defining Incident Management Procedures

The two most commonly used approaches are by

- **CMU/SEI** ○ Computer Emergency Response Team (CERT)
- **SANS Institute** ○ Computer Incident Advisory Center (CIAC)

Detailed Plan of Action for Incident Management

- The incident management action plan is also known as the **incident response plan (IRP)**
- In the CMU/SEI technical report titled *Defining Incident Management Processes,* the approach is as follows:

○ **Prepare**/improve/sustain sub process includes:

✦ Coordinating planning and design:

- Identify incident management requirements
- Establish vision and mission
- Obtain funding and sponsorship
- Develop implementation plan ✦ Coordinate implementation:
- Develop policies, processes and plans
- Establish incident handling criteria
- Implement define resources
- Evaluate incident management capability
- Conduct postmortem review
- Determine incident management process changes
- Implement incident management process changes

○ **Protect** infrastructure sub process includes:

✦ Implement changes to computing infrastructure protection improvements from postmortem reviews or other process improvement mechanisms

✦ Evaluate computing infrastructure by performing proactive security assessment and evaluation

✦ Provide input to detect process on incidents/potential incidents

○ **Detect** events sub process includes:

✦ Proactive detection-the detect process is conducted regularly prior to incident

✦ Reactive detection-the detect process is conducted when there are reports from system users or other organizations

○ **Triage** events

✦ Can be done on two levels:

- Tactical, based on a set of criteria

        - Strategic, based on the impact of business
    - Sub process includes
        - Categorization:
- Denial of service ○ Malicious code ○ Unauthorized access ○ Inappropriate usage
- Multiple components (Correlation, Prioritization, Assignment)

- **Respond** sub process includes:
    - Technical response:
        - Collecting data for further analysis
        - Analyzing incident supporting information such as log files
        - Technical mitigation strategies and recovery options
        - Phone or e-mail technical assistance
        - On-site assistance
        - Analysis of logs
        - Development and deployment of patches and workarounds
    - Management response
    - Legal response

Current State of Incident Response Capability

Ways to identify the current state of incident response capability include:

- Survey of senior management, business managers and IT representatives
- Self-assessment
- External assessment or audit

History of Incidents

Past incidents:

- Provide valuable information on trends, types and business impacts
- Are an input into the assessment of the types of incidents that must be considered and planned for

Threats

Threats are any event that may cause harm to an organization's assets, operations or personnel. There are a number of threats that must be considered including:

- Environmental
- Technical
- Man-made

Vulnerabilities

- **Vulnerabilities** are weaknesses in a system, technology, process, people or control that can be exploited and result in exposure
- **Vulnerability management** is the proactive identification, monitoring and fixing of relevant weaknesses

Developing an Incident Response Plan

CIAC (and later the SANS Institute) propose the following incident response phase:

- **Preparation** ○ This phase prepares an organization to develop an incident response plan prior to an incident. Sufficient preparation facilities smooth execution

○ Activities in this phase include:

  - ✦ Establishing an approach to handle incidents
  - ✦ Establishing policy and warning banners in information systems to deter intruders and allow information collection
  - ✦ Establishing communication plan to stake holders
  - ✦ Developing criteria on when to report incident to authorities
  - ✦ Developing a process to activate the incident management team
  - ✦ Establishing a secure location to execute the incident response plan
  - ✦ Ensuring equipment needed is available

- **Identification** ○ This phase aims **to verify** if an incident has happened and find out more details about the incident. Reports on possible incidents may come from information systems, end users or other organizations. Not all reports are valid incident's, as they may be false alarms or may not qualify as an incident.

○ Activities in this phase include:

  - ✦ Assigning ownership of an incident or potential incident to an incident handler
  - ✦ Verifying that reports or events qualify as an incident
  - ✦ Establishing chain of custody during identification when handling potential evidence
  - ✦ Determining the severity of an incident and escalating it as necessary

- **Containment**
  - ○ After an incident has been identified and confirmed, the IMT is activated and information from the incident handler is shared

- The team will conduct a detailed assessment and contact the system owner or business manager of the affected information systems/assets to coordinate further action
- The action taken in this phase is **to limit the exposure**. Activities in this phase include:
  - Activating the incident management/response team to contain the incident
  - Notifying appropriate stakeholders affected by the incident
  - Obtaining agreement on actions taken that may affect availability of a service or risks of the containment process
  - Getting the IT representative and relevant virtual team members involved to implement containment procedures
  - Obtaining and preserving evidence
  - Documenting and taking backups of actions from this phase onward
  - Controlling and managing communication to the public by the public relations team

- **Eradication** ○ When containment measures have been deployed, it is time to determine the **root cause** of the incident and eradicate it
  - Eradication can be done in a number of ways:
    - Restoring backups to achieve a clean state of the system
    - Removing the root cause
    - Improving defenses
    - Performing vulnerability analysis to find further potential damage from the same root cause
  - Activities in this phase include:
    - Determining the signs and cause of incidents
    - Locating the most recent version of backups or alternative solutions
    - Removing the root cause. In the event of worm virus infection, it can be removed by deploying appropriate patches and updated antivirus software
    - Improving defenses by implementing protection techniques
    - Performing vulnerability analysis to find new vulnerabilities introduced by the root cause

- **Recovery**
  - This phase ensures that affected systems or services are restored to a condition specified in the service delivery objectives (SDO) or business continuity plan (BCP). The time constraint up to this phase is documented in the RTO.
  - Activities in this phase include:
    - Restoring operations to normal

- ✦ Validating that actions taken on restored systems were successful ✦ Getting involvement of system owners to declare normal operation

- **Lessons learned** ○ At the end of the incident response process, a report should be developed to share what has happened, what measures were taken and the results after the plan was executed
  - ○ The report should contain lessons learned that provide the IMT and other stakeholders valuable learning points of what could have been done better
  - ○ These lessons should be developed onto a plan to enhance the incident management capability and the documentation of the incident response plan.
    - ✦ Writing the incident report
    - ✦ Analyzing issues encountered during incident response efforts
    - ✦ Proposing improvement based on issues encountered ✦ Presenting the report to relevant stakeholders

Gap Analysis-Basis for an Incident Response Plan

- **Gap analysis**-compares current incident response capabilities with the desired level
- By comparing the two levels, the following may be identified:

○ Processes that need to be improved to be more efficient and effective ○ Resources needed to achieve the objectives for the incident response capability

Business Impact Assessment

- A BIA should:
- **Determine the loss** to the organization resulting from a function being unavailable
- Establish the **escalation** of that loss over time
- Identify the minimum resources needed for recovery
- Prioritize the recovery of processes and supporting systems
- Create report to aide stakeholders in understanding what impact an incident would have on the business
- A successful BIA requires participation from:
- Senior management
- IT
- End-user personnel
- BIA goals

- Critically prioritization
- Downtime estimation
- Resource requirement
- A BIA includes the following activities:
- Gathering assessment material
- Analyzing the information compiled
- Documenting the result and presenting recommendations

Elements include:

- Business/ department mission
- Functions that characterize each business function
- Dependencies-inputs and outputs
- Identify critical processing cycles
- Estimated impact of various incidents
- Identify resources and activities required for restoration
- Determine work-around possibilities
- Estimate recovery time

Benefits include

- Increased understanding of potential loss
- Common facilitation of all response activities
- Raising awareness of response management in organizations

Escalation Process for Effective Incident Management

- Implement escalation process to establish the events to be managed
- For each event, a list of actions should be described in the sequence to be performed
- Each event should be assigned a criticality/sensitivity level
- The ISM should consult others in the development of escalation procedures

Incident Management and Response Teams

Number of teams depends upon **size of organization** and **magnitude** of operations-examples include:

- The emergency action team
- Damage assessment team
- Emergency management team
- Relocation team
- Security team

Organizing, Training and Equipping the Response Staff

Every IMT member should get the following types of training:

- Induction to IMT-basic information about the team and its operations
- Mentoring regarding team's roles, responsibilities and procedures
- On-the-job training
- Formal training

Challenges in Developing an Incident Management Plan

Unanticipated challenges may be the result of:

- **Lack of management buy-in** and organizational consensus
- **Mismatch** to organizational goals and structure
- IMT member **turnover**
- **Lack of communication** process
- **Complex** and wide plan

Business Continuity and Disaster Recovery Procedures

Considerations when developing response and recovery plans include:

- Available resources
- Expected services
- Types, kinds, and severity of threats faced by the organization

Recovery Planning and Business Recovery Process

- **Disaster recovery** has traditionally been defined as the recovery of IT systems after disruptive events
- **Business recovery** is defined as the recovery of the critical business processes necessary to continue or resume operations

Each of these planning processes typically includes several main phases, including:

- Risk and business impact **assessment**
- **Response and recovery** strategy definition
- **Documenting** response and recovery plans
- **Testing** response and recovery plans
- **Auditing** response and recovery plans

Recovery Strategies

- The most appropriate strategy is likely to be one that demonstrably addresses probable events with acceptable recovery times at a reasonable cost
- The development of an incident management and response plan is likely to be a difficult and expensive process that may take considerable time: ○ Requires the development of several alternative strategies ○ It may be prudent to consider outsourcing some or all of the needed capabilities

Addressing Threats

In the case of threats, some possible strategies to consider may include:

- **Eliminate** or neutralize a threat
- **Minimize the likelihood** of a threat's occurrence
- **Minimize the effects** of a threat if an incident occurs

Recovery Sites

Types of offsite backup hardware facilities available include:

- Hot sites
- Warm sites
- Cold sites
- Mobile sites
- Duplicate sites
- Mirror sites

Criteria for selecting alternate sites include:

- The site should not be subject to the same natural disaster(s) as the primary site
- Ability to coordinate hardware/software strategies
- Assurance of resource ability
- Ability to agree concerning the priority of adding applications (workloads) until all the recovery resources are fully utilized
- Ability to test regularly

Basis for Recovery Site Selections

Response and recovery strategy should be based on the following considerations:

- Interruption window
- RTOs
- RPOs
- Services delivery objectives (SDOs)
- Maximum tolerable outages (MTOs)
- Proximity factors
- Location
- Nature of probable disruptions

Reciprocal Agreements

Alternatives available for securing backup hardware and physical facilities include:

- A vendor or third party
- Off-the-shelf-to make use of this approach, several strategies must be employed: ○ Avoiding the use of unusual and hard-to-get equipment ○ Regularly updating equipment to keep current
    - ○ Maintaining software compatibility to permit the operation of newer equipment
- **Recovery of IT facilities** involves telecommunications and network recovery
  • Methods used are:
    - ○ Alternative routing ○ Diverse routing ○ Long-haul network diversity ○ Protection of local resources ○ Voice recovery
    - ○ Availability of appropriate circuits and adequate bandwidth ○ Availability of out-of-band communications in case of failure of primary communications methods
- **Recovery strategies** must work for the entire period of recovery until all facilities are restored
- Strategies may include:
    - ○ **Doing nothing** until recovery facilities are ready
    - ○ Using **manual** procedures
    - ○ **Focusing** on the most important customers, suppliers, products, and systems with resources that are still available
    - ○ **Using PC-based systems** to capture data for later processing or performing simple local processing

Strategy Implementation

Plan development factors include:

- Pre-incident readiness
- Evacuation procedures
- How to declare a disaster
- Identification of the business processes and IT resources that should be recovered
- Identification of the responsibilities in the plan
- Identification of contact information
- The step-by-step explanation of the recovery options
- Identification of the various resources required for recovery and continued operations
- Ensuring that other logistics such as personnel relocation and temporary housing are considered

Integrating Recovery Objectives and Impact Analysis with Incident Response

Risk

- Is the combination of the probability of an event and its consequence (ISO/IEC 73)
- A basic understanding of security risk analysis and the effects on organizations of various types of risk are important components of incident management

Risk Tolerance

- Is the acceptable level if variation that management is willing to allow for any risk as the enterprise pursues its objectives
- Is the same as acceptable risk
- Must be determined by management

The ISM needs to:

- Oversee the development of response and recovery plans to ensure that they are properly designed and implemented
- Ensure resources required to continue the business are identified and recorded
- Identify and validate response and recovery strategies
- Obtain **senior management approval** of strategies
- Oversee the development of comprehensive response and recovery plans

- **Recovery time objective** is defined as the amount of time allowed for recovery of a business function or resource after a disaster occurs.

- Effective incident management includes resolving incidents with the **acceptable interruption window (AIW).**

- A **recovery point objective (RPO)** is a measurement of the point prior to an outage to which data are to be restored.

Notification Requirements

Plan should include a **call tree** with prioritized list of contacts:

- Representatives of equipment and software **vendors**
- **Contacts within companies** that have been designated to provide supplies and equipment or services
- **Contacts at recovery facilities**, including hot site representatives or predefined network communications rerouting services
- **Contacts at offsite** media storage facilities and the contacts within the company who are authorized to retrieve media from the offsite facility
- **Insurance** company agents
- Contact information for **regulatory bodies**
- Contacts at **human resources (HR)** and/or contract personnel services
- **Law enforcement** contacts

Methods for Providing Continuity of Network Services

- Redundancy
- Alternate routing
- Diverse routing
- Long-haul diversity
- Last mile circuit protection
- Voice recovery

High-Availability Considerations

Plan must also address fault tolerant systems:

- Fail safe servers using clusters or load balancing
- Redundant array of Inexpensive Disks (RAID)

Insurance

Types of insurance coverage:

- IT equipment and facilities
- Media (software) reconstruction
- Extra expense
- Business interruption
- Valuable papers and record
- Errors and omissions
- Fidelity coverage
- Media transportation

Periodic Testing of the Response and Recovery Plans

Testing must include:

- Developing test objectives
- Executing the test
- Evaluating the test
- Developing recommendations to improve the effectiveness of testing processes as well as response and recovery plans
- Implementing a follow-up process to ensure that the recommendations are implemented

Testing for Infrastructure and Critical Business Applications

After test objectives have been defined, the ISM must:

- Ensure that an independent third-party observer is present to monitor and evaluate the test
- Implement a tracking process to ensure that any recommendations resulting from testing are implemented in a timely fashion
- Know about disaster recovery testing for infrastructure and critical business applications

Types of Tests

Tests that are progressively more challenging can include:

- **Table-top walk-through** of the plans
- Table-top walk-through with mock disaster scenarios

- **Testing the infrastructure** and communication components of the recovery plan
- Testing the infrastructure and recovery of the critical applications
- Testing the infrastructure, critical applications and involvement of the end users
- **Full restoration and recovery tests** with some personnel unfamiliar with the systems
- **Surprise tests**

Test Results

The test should strive to, at a minimum, accomplish the following tasks:

- **Verify the completeness** and precision of the response and recovery plan
- **Evaluate the performance** of the personnel involved in the exercise
- **Appraise** the demonstrated level of training and awareness of individuals who are not part of the recovery/response team
- Evaluate the coordination among the team members and external vendors and suppliers
- Measure the ability and capacity of the backup site to perform prescribed processing
- Assess the vital records retrieval capability
- Evaluate the state and quantity of equipment and supplies that have been relocated to the recovery site
- Measure the overall performance of operational and information systems processing activities related to maintaining the business entity

Ensuring Execution as Required

- A **facilitator-director** is needed to:

○ Direct the tasks within the plans ○ Oversee plan execution ○ Liaise with senior management ○ Make decisions as necessary

- Defining appropriate recovery strategies and alternatives is important in the overall process
- **Imperative plan maintenance** activities include:
  - Developing a schedule for periodic review and maintenance of the plan, and advising all personnel of their roles and the deadline for receiving revisions and comments

- Calling for revisions out of schedule when significant changes have occurred
- Reviewing revisions and comments, and updating the plan within a reasonable period after the review date
- Arranging and coordinating scheduled and unscheduled tests of the plan to evaluate its adequacy
- Participating in scheduled plan tests, which should be performed at least once each year
- Developing a schedule for training personnel in emergency end recovery procedures, as set forth in the plan
- Maintaining records of plan maintenance activities-testing, training and reviews
- Updating, at least quarterly, the notification directory to include all personnel changes, including phone numbers and responsibilities or status within the company

Post-Incident Activities and Investigation

- **Post-event reviews** are a very critical part of the incident management process
- The ISM should:
  - Manage post-event reviews to **learn from the completed tasks** and to use the information to improve the IMT's response procedures
  - Consider enlisting the help of **third-party specialists if detailed forensic skills are needed**

Establishing Procedures

If an incident occurs:

- The information security staff needs documented procedures so that information can be properly recorded and preserved
- The ISM should develop data/evidence preservation procedures
- The information systems staff must understand basic procedures, including taking no action that could change/modify/contaminate potential or actual evidence

The **initial response** by the system administrator should include:

- Retrieving information needed to confirm an incident
- Identifying the scope and size of the affected environment (e.g., networks, systems, applications)
- Determining the degree of loss, modification or damage (if any)

- Identifying the possible path or means of attack

Requirements for Evidence

The ISM must know:

- Requirements for collecting and presenting evidence
- Rules for evidence, admissibility of evidence, and quality and completeness of evidence
- The consequences of any contamination of evidence following a security incident

-END-