# Certified Information Security Manager Notes 2024

STUDY NOTES – CREATED BASED ON CYVITRIX COURSE

CYVITRIX, INSTRUCTOR AHMED

# Table of Content

# Contents

# Domain 1: Information Security Governance

## About Security Governance

- ➔ Governance is broadly defined as the rules that run the organization, including policies, standards, and procedures that are used to set the direction and control the organization's activities.
- ➔ Information security deals with all aspects of information in any medium (e.g., written, spoken, electronic). Information security governance is a subset of corporate governance.
- ➔ Senior management and the board of directors must be held accountable for information security governance.

## How do you establish an information security governance strategy?

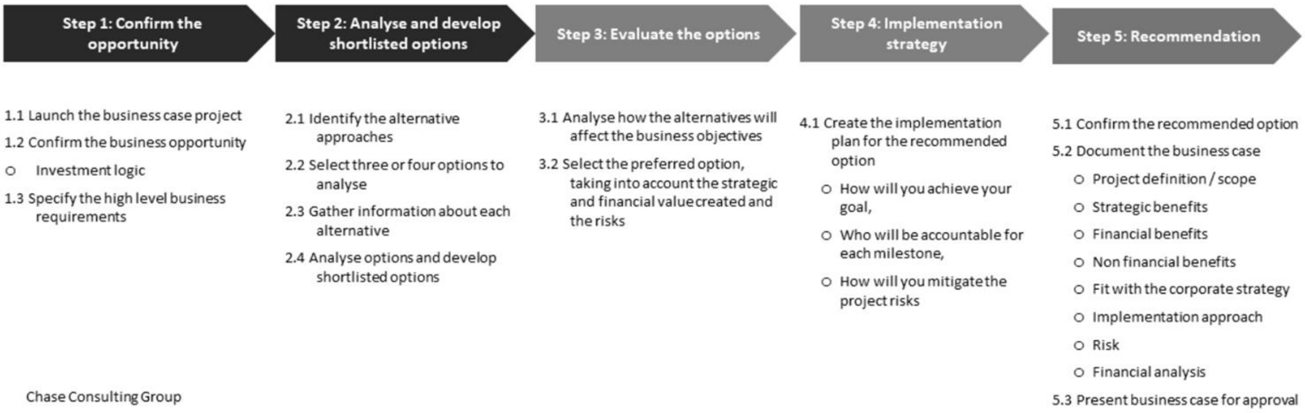
- ➔ Step in establishing InfoSec governance: -

- ✓ meetings with senior management and business unit leaders to determine outcomes they need. Output will be a series of specific objectives that, when achieved, will satisfy the requirements. The desired state is based on the outcomes set by senior management.
- ✓ determine what needs to be done to move from the current to the desired state by using a gap analysis.
- ✓ Create a road map to identify the specifics needed to achieve the objectives.
- ✓ identifying the resources needed to navigate the road map and implement the strategy.

- ➔ The strategy must be a living document with objectives, approaches, and methods changing to meet new conditions.
- ➔ The most likely outcome is that residual risk dropped to an acceptable level. The primary goal of security programs is to secure business assets.

## Why Business case is essential?

- ➔ Senior management support is needed for Incident response or strategy or any infosec initiative; this support can be secured by developing a business case.
- ➔ It documents the reasoning for initiating a project or task; procurement starts after accepting the business case.
- ➔ The business case should include all the factors that can materially affect the project's success or failure.
- ➔ It is important to avoid overconfidence, overly optimistic projections, and excessive precision.
- ➔ derived from a feasibility study, A business case provides the information required for an organization to decide whether a project should proceed through the cost-benefit analysis.
- ➔ The business case should also be a key element of the decision process throughout the life cycle of any project. If at any stage the business case is thought to be no longer valid, the project sponsor or IT steering committee should consider whether the project should proceed.
- ➔ How to develop a business case?



**Step 1: Confirm the opportunity**

1.1 Launch the business case project
1.2 Confirm the business opportunity
- Investment logic

1.3 Specify the high level business requirements

**Step 2: Analyse and develop shortlisted options**

2.1 Identify the alternative approaches
2.2 Select three or four options to analyse
2.3 Gather information about each alternative
2.4 Analyse options and develop shortlisted options

**Step 3: Evaluate the options**

3.1 Analyse how the alternatives will affect the business objectives
3.2 Select the preferred option, taking into account the strategic and financial value created and the risks

**Step 4: Implementation strategy**

4.1 Create the implementation plan for the recommended option
- How will you achieve your goal,
- Who will be accountable for each milestone,
- How will you mitigate the project risks

**Step 5: Recommendation**

5.1 Confirm the recommended option
5.2 Document the business case
- Project definition / scope
- Strategic benefits
- Financial benefits
- Non financial benefits
- Fit with the corporate strategy
- Implementation approach
- Risk
- Financial analysis

5.3 Present business case for approval

Chase Consulting Group

## Security governance Benefits and Outcomes

➔Security programs apply the strategy.

## Information Security governance provides the following benefit: -

1. civil or legal liability insurance to the organization.
2. assurance of policy compliance
3. lowering risk to definable and acceptable levels
4. optimize allocations of limited security resources
5. assurance that critical decisions are not based on faulty information.
6. firm foundation for efficient and effective risk management
7. process improvement, rapid incident response and continuity management.
8. Protecting the organization's reputation
9. Providing accountability for safeguarding information during critical business activities

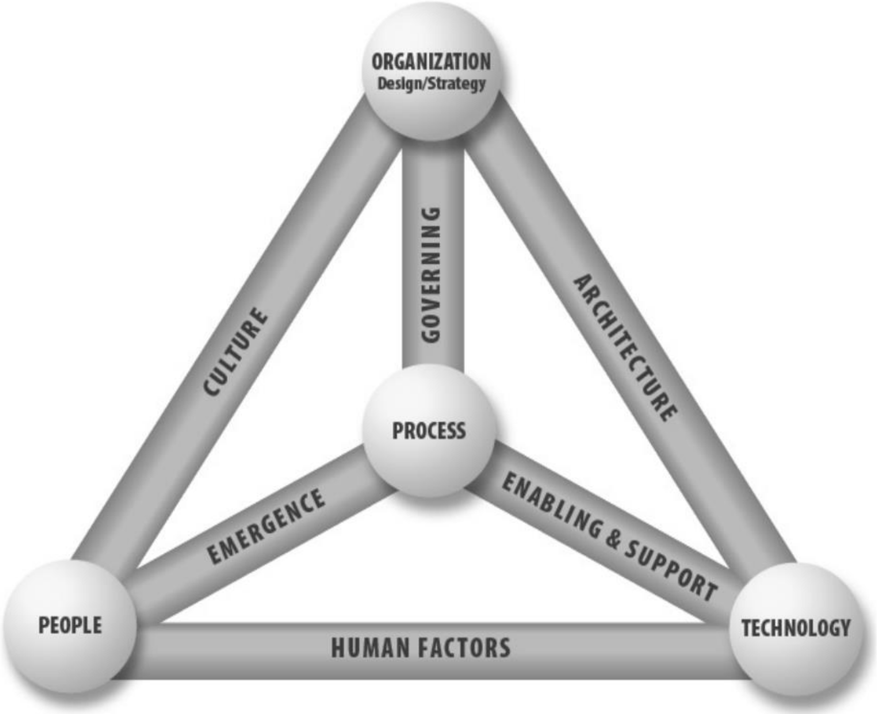
## Outcomes of Information Security governance (why to develop security strategy?) e.g., Program

1. Strategic alignment
2. Risk management.
3. Value delivery
4. Resource optimization
5. Performance measurement
6. Assurance process integration

- The strategy must also take into consideration that personnel safety is a priority and the subject of regulations in many jurisdictions.
- From a business perspective, a cost-benefit or other financial analysis is the most accepted approach to justifying expenditure and should be considered when developing a strategy.
- Security strategy is helpful in integrating development activities toward common goals.

## Business Model for Information Security

- The business model for Information systems has four elements with six interconnections.



1. Governance—Steering the enterprise and demanding strategic leadership.
2. Culture—A pattern of behaviors, beliefs, assumptions, attitudes, and ways of doing things.
3. Enablement and support—Connects the technology element to the process element.
4. Emergence— refers to patterns that arise in the life of the enterprise that appear to have no obvious cause and whose outcomes seem impossible to predict and control.
5. Human factors—Represents the interaction and gap between technology and people and, as such, is critical to an information security program.
6. Architecture—A comprehensive and formal encapsulation of the people, processes, policies, and technology that comprise an enterprise's security practices.

- Some indicators of a successful security culture are.
  1. the information security department being brought into projects at the appropriate times, end users.
  2. knowing how to identify and report incidents.
  3. the organization's ability to identify the security manager.
  4. people knowing their role in protecting the information assets of the organization and integrating information security into their daily practices.
  5. Risk management framework.

## Action plan to develop security strategy.

➔ Gap analysis

Annually

Work backward from endpoint to the current state.

Link business objectives with strategy

Appropriate authority

Appropriate security approvals.

➔ Policy development

➔ Standards development

➔ Training and awareness

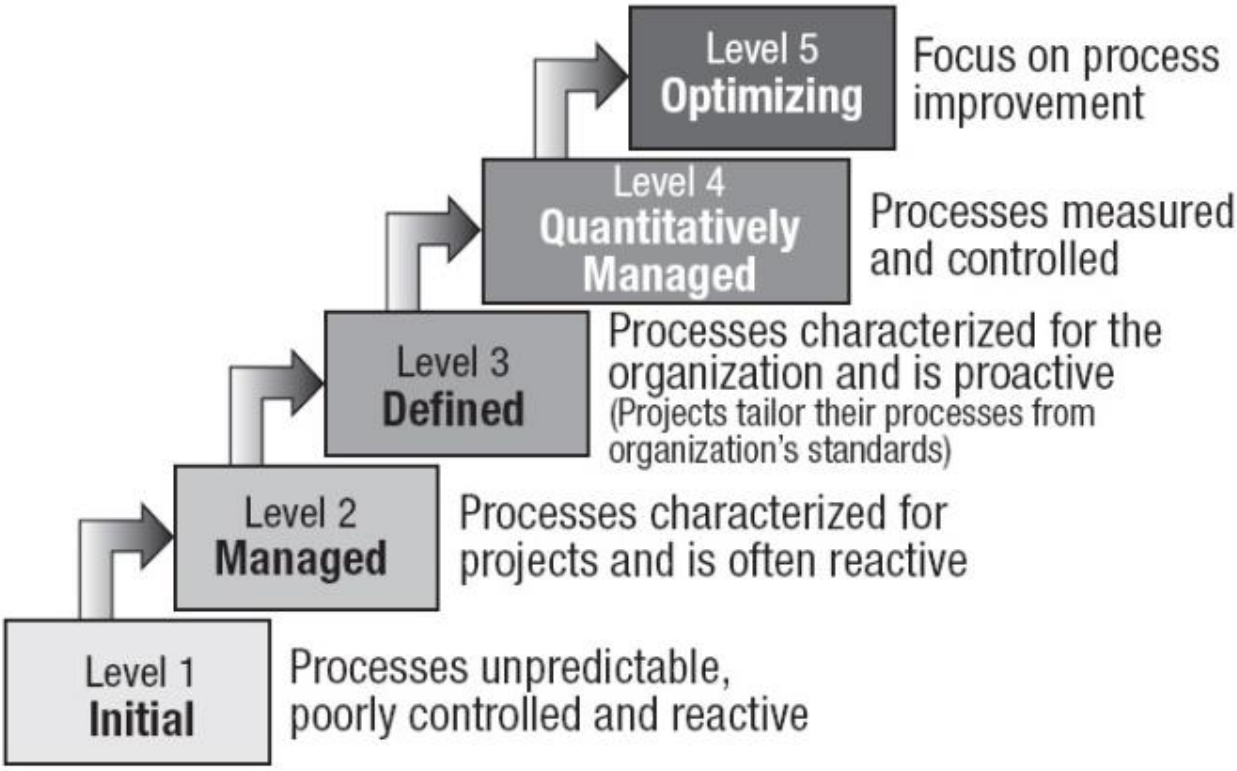
➔ Develop Metrics

## The need for metrics

➔ No profession or activity has achieved reliable and effective maturity prior to the development of a suite of good metrics. Metrics must be considered at three levels operational, management and strategic as what cannot be measured cannot be managed.

➔ The first step to establish a system of metrics is to determine what is meaningful to the recipients. Then those metrics must be monitored, evaluated, and communicated to the appropriate people on a timely basis.

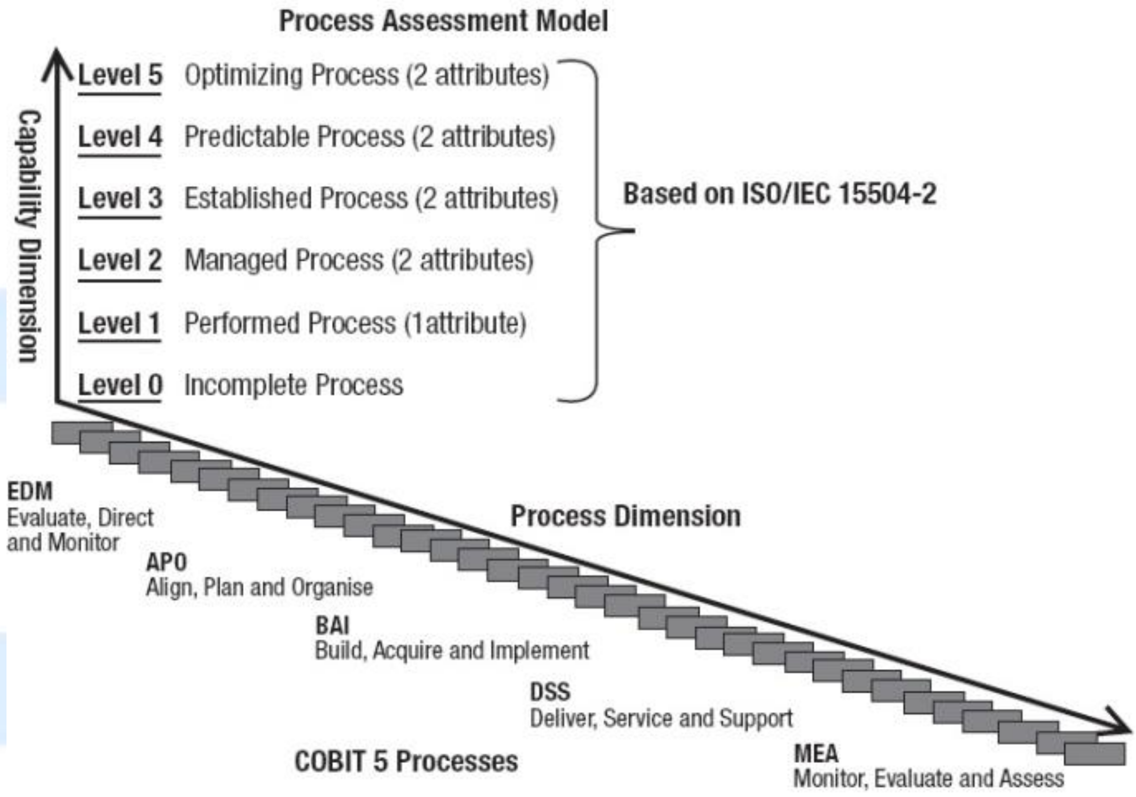
- ➔ Metric should be <u>specific, measurable, attainable, relevant, and timely</u>. They should tie into the information security program objectives as they support the objectives of the business.
- ➔ Capability Maturity Model Integration CMMI has five maturity levels. Each level builds on the previous for continuous improvement it used to determine target state compared to current state, it do not provide complete perspective.


Level 5
Optimizing
Focus on process improvement
Level 4
Quantitatively Managed
Processes measured and controlled
Level 3
Defined
Processes characterized for the organization and is proactive (Projects tailor their processes from organization's standards)
Level 2
Managed
Processes characterized for projects and is often reactive
Level 1
Initial
Processes unpredictable, poorly controlled and reactive

Disclaimer: Use for review after studying our CISM Course – https://cyvitrix.com

REACH OUT cyvitrix@gmail.com for any requests.

➔ COBIT 5 Process Assessment Model used as the basis for assessing the capability of each COBIT 5 process, resulting in a 0 to 5 level of maturity. The Process assessment model (PAM) provides a basis for performing ongoing gap analysis to determine progress toward achieving the goals, focus on process. (Also known as process performance and capabilities


Process Assessment Model
Capability Dimension
Level 5 Optimizing Process (2 attributes)
Level 4 Predictable Process (2 attributes)
Level 3 Established Process (2 attributes)
Level 2 Managed Process (2 attributes)
Level 1 Performed Process (1attribute)
Level 0 Incomplete Process
Based on ISO/IEC 15504-2
Process Dimension
EDM Evaluate, Direct and Monitor
APO Align, Plan and Organise
BAI Build, Acquire and Implement
DSS Deliver, Service and Support
MEA Monitor, Evaluate and Assess
COBIT 5 Processes

➔ Balanced Scorecard is a management system. It provides feedback around both the internal business processes and external outcomes, it also can be used for ***<u>determining target state progress</u>***, it shows if infosec objective is aligned with business objective.

## Critical Success Factors

➔ Critical Success Factors are certain steps must be accomplished to successfully meet the required objectives, including:

✓ Identifying, categorizing, and defining controls
✓ Defining appropriate tests to determine effectiveness.

- ✓ Committing resources to accomplish required testing.

## Key Performance Indicator

- ➔ Key Performance Indicators are critical performance factors necessary to achieve the objectives include:

- ✓ Control effectiveness testing plans.
- ✓ Progress in controls effectiveness testing
- ✓ Results of testing control effectiveness
- ✓ <u>Make sales with 1 BN $ - achieve security certificate.</u>

## Key Goal Indicator

- ➔ key goals are what organization aim to achieve as part of its objective, example of it could include:

- ✓ Achieving Sarbanes-Oxley controls testing compliance mandates
- ✓ Completing independent controls testing compliance validation and attestation
- ✓ Preparing the required statement of control effectiveness
- ✓ <u>Became the largest seller in region or become ISO 27001 certified.</u>

## Key Risk indicators

- ➔ KRIs can provide early warnings on issues or areas that pose particular risk, as it Indicate that a risk is developing or changing to show that investigation is needed to determine the nature and extent of a risk.
- ➔ Selection of KRIs, can be based on sources such as industry benchmarks, external threat reporting services, or any other factor that can be monitored that indicates changes in risk to the organization.
- ➔ KRIs are specific to each enterprise, and their selection depends on several parameters in the internal and external environment.
- ➔ Example of KRI is total devices with unsupported OS version or lack AV and so on.

➔ The criteria for selecting effective KRIs include:

- ✓ Impact—Indicators for risk with high potential impact are more likely to be KRIs.
- ✓ Effort to implement, measure and report—For indicators with equivalent sensitivity to changing risk, the ones that are easier to measure are preferred.
- ✓ Reliability—The indicator must possess a high correlation with the risk and be a good predictor or outcome measure.
- ✓ Sensitivity—The indicator must be representative of the risk and capable of accurately indicating variances in the risk level.

## Frameworks

➔ Enterprise architecture should describe a method for designing a target or desired state of the enterprise in terms of a set of building blocks, and for showing how the building blocks fit together.

➔ Governance comes first then EA.

➔ Frameworks provide guidance.

➔ The COBIT 5 framework describes seven categories of enablers.

1. *Principles, policies, and frameworks*
2. *Processes*
3. *Organizational structures*
4. *Culture, ethics, and behavior*
5. *Information*
6. *Services, infrastructure, and applications*
7. *People, skills, and competencies*

➔ To define an efficient framework, it is important to:

1. *Understand the background of the organization and its risk (e.g., its core processes, valuable assets, competitive areas)*
2. *Evaluate existing risk management activities and criteria for acceptable risk levels.*

3. *Develop a structure and process for the development of risk management initiatives and controls sufficient to achieve acceptable risk levels (control objectives)*
4. *The local market; the business; and the competitive, financial, and political environments*
5. *The law and regulatory environment*
6. *Social and cultural conditions*
7. *External stakeholders*

## Security strategy resources

➔ Security program is established to implement the information security strategy.

➔ The resources available to the organization need to be enumerated and considered when developing a security strategy: -

**1. Policies**

**2. Standards**

**3. Procedures**

**4. guidelines**

**5. Architecture(s)**

**6. Controls**

**7. Countermeasures**

**8. Layered defenses**

**9. Technologies**

**10. Personnel security**

**11. Organizational structure**

**12. Roles and responsibilities**

**13. Skills**

**14.Training**

**15. Awareness and education**

**16. Audits**

**17. Compliance enforcement**

**18.Threat assessment**

**19. Vulnerability assessment**

**20. BIA**

**21. Risk analysis**

**22. Resource dependency analysis**

**23. Third-party service providers**

**2ssurance provides.**

**25. Facilities**

**26. Environmental security**

## POLICIES AND STANDARDS

- ➔Security policies are designed to mitigate risk and are usually developed in response to an actual or perceived threat. Policies state management intent and direction at an elevated level.
- ➔Standards are developed or modified to set boundaries for people, processes, technologies.
- ➔Standards provide the basis for measurement and testing approaches for evaluating whether security baselines are being met by existing controls.
- ➔procedures “requires more effort” and technologies to maintain compliance with policies and support the achievement of the organization’s goals and objectives.
- ➔Standards must be disseminated to those governed by them as well as those impacted. Review and modification processes must be developed as well.
- ➔Policies provide an insight into the intent of senior management.
- ➔There are several attributes of good policies that should be considered:
  - Each policy should state only one general security mandate.
  - Policies must be clear and easily understood by all affected parties.
  - Policies should rarely be more than a few sentences long.
  - There should rarely be a reason to have more than two dozen policies.

## ENTERPRISE INFORMATION SECURITY ARCHITECTURE(S)

- ➔The choice of approaches may be limited by an existing organizational standard, but if one does not exist, the choice should be made based on form, fit and function.
- ➔The top-down model ensures adherence to overall strategy, down-top approach ensures BU objective is aligned with risks related to this BU.

## CONTROLS

- Corrective, detective, preventive, deterrent
- Procedural & Administrative, technical, non-IT
- Information security controls should be proportionate to the criticality of the system.
- Human life is the most important consideration in control policy.
- Controls are designed as part of the information risk management framework, which incorporates policies, standards, procedures, practices, and organizational structures.
- Countermeasures include any process that serves to counter specific threats and can be considered a targeted control.

## TECHNOLOGIES

- Layered defense or defense in depth.
- IT usually is not the owner of most of the information in its systems, instead they own the systems.

## PERSONNEL

- Background checks
- security is only as strong as the weakest link; everyone should have responsibilities related to information security or risk management.

## ORGANIZATIONAL STRUCTURE

- senior management promotes cooperation, **arbitrates differences** in perspective and is clear about priorities and responsible for ensuring that needed organizational functions, resources and supporting infrastructure are available and properly utilized to fulfill the information-security-related directives of the board, an effective risk management program that assesses and mitigates IT related mission risk requires the support and involvement of senior management.

- Board direct executive manager and does not interfere directly with operations. But the board is liable, so they are involved in an info sec program to ensure it complies with liability requirements.
- CISO is a regulatory role, he and infosec manager oversee the security program. Most frequently, information security being primarily a regulatory activity. CISO is responsible for policy enforcement.
- Chief risk officer—The chief risk officer (CRO) is charged with overall ERM.
- Chief information officer—The CIO is responsible for IT planning, budgeting, and performance, often focused on cost and performance of IT. CIOs and IT departments are usually under pressure to increase performance and cut costs.
- Security Steering committee oversees security programs, managed by executive level officer, best advocate security program.
- Effective communication between entities helps to identify events that may affect InfoSec for the organizations.
- The Chief compliance officer approves when deviation from standard happens.

## EMPLOYEE ROLES AND RESPONSIBILITIES

- The information security manager should work with the personnel director to define security roles and responsibilities. The related competencies required for each job position should also be defined and documented.
- Use RACI (Responsible, Accountable, Consulted, Informed) to define roles and responsibilities.
- Difference between roles and responsibility: -

  A role is a designation assigned to an individual by virtue of a job function or another label. A responsibility is a description of some procedure or function related to the role that someone is accountable to perform.
- Business owner = data owner = information owner

## SKILLS

- ➔ Choosing a strategy that uses skills already available is likely to be a more cost-effective option, but at times, skills may need to be developed or the required activities outsourced.
- ➔ It is important to understand the proficiencies of available personnel to ensure that they map to competencies required for program implementation.
- ➔ External resources, such as consultants, are often a more cost-effective choice for skills required for only a brief time for specific projects.

## AWARENESS AND EDUCATION

- ➔ Awareness education and training can serve to mitigate some of the most significant areas of organizational risk and achieve the most cost-effective improvement in risk and security.
- ➔ Employees cannot be expected to comply with policies or standards they are not aware of or follow procedures they do not understand.
- ➔ Awareness training for senior management should highlight liability, need for compliance, due care and due diligence, and the need to create the tone and culture of the organization through policy and good practice, and need to be reminded that they are the ones who own the risk.
- ➔ Ensuring users are educated in procedures and understand risk management processes is the responsibility of the information security manager.
- ➔ The training and awareness program should be targeted to different staffing and security levels.

## COMPLIANCE ENFORCEMENT

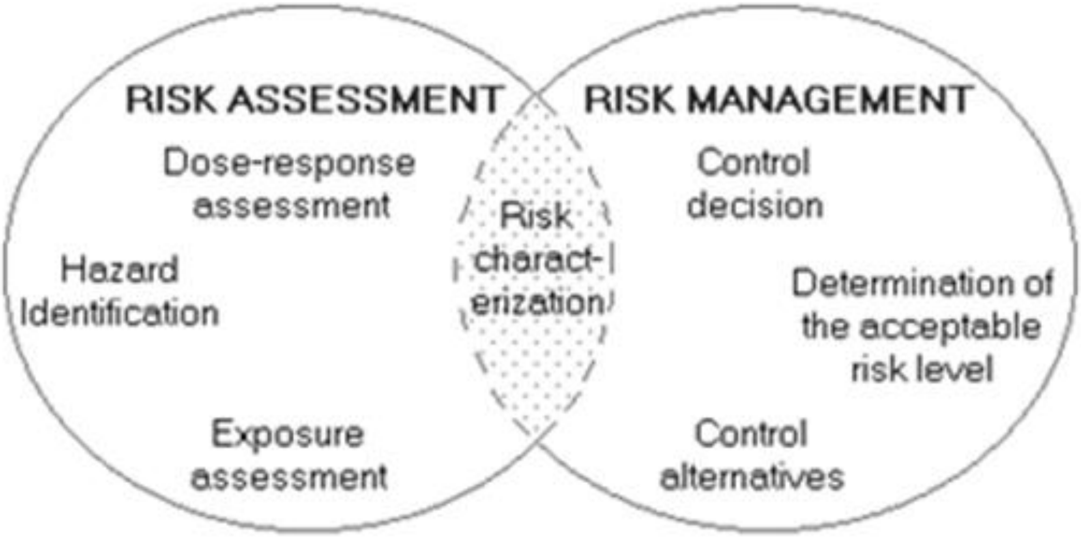
- ➔ From the perspective of the information security manager, regulatory compliance should be treated as any other risk and the extent of compliance is a business decision that must be made by senior management with input as to risk and potential impact.

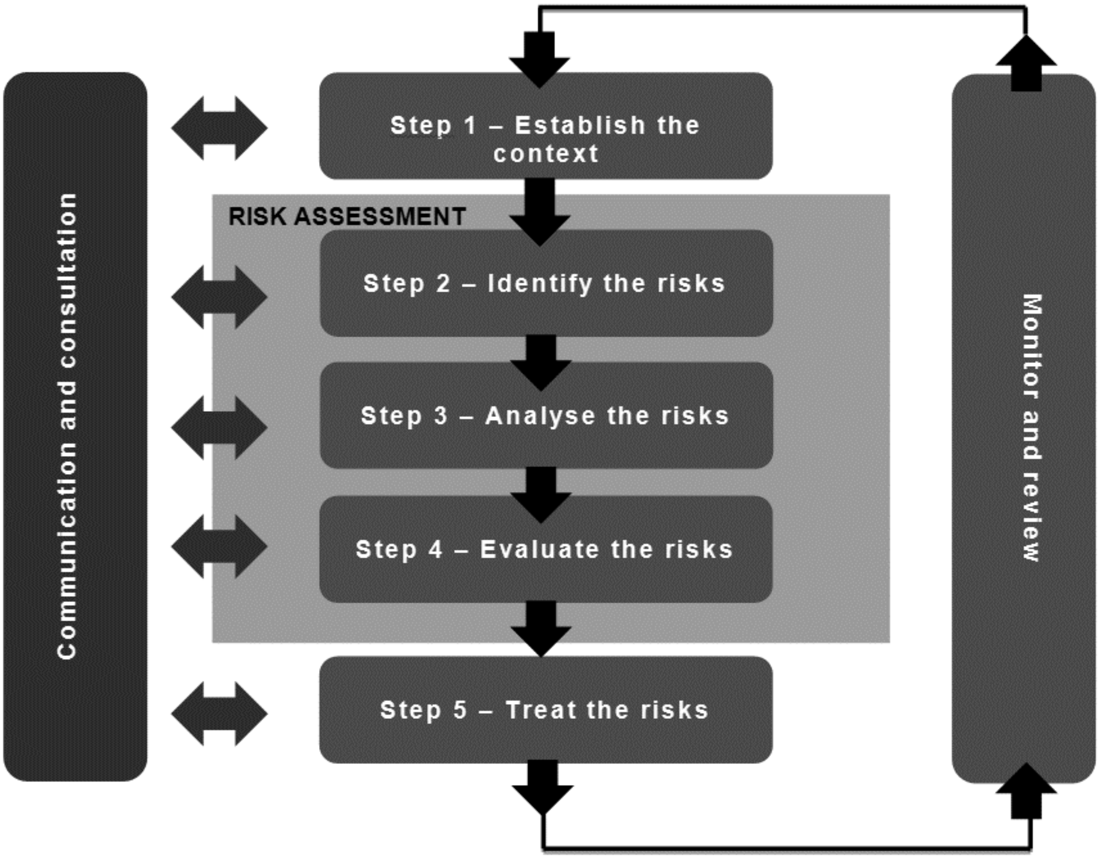
- ➔ Compliance is the process that records and monitors the policies, procedures and controls needed to ensure that policies and standards are adequately adhered to.
- ➔ IT GRC seeks to ensure proper operation and policy compliance of IT processes and maintain strong risk management process.
- ➔ Negotiate local version of organization standard in case legal aspect is different in one on Business units.
- ➔ Regulatory requirements typically are better addressed with standards and procedures.
- ➔ Business process owner is who should provide direction on the new impact of new regulatory requirement because we understand business better.
- ➔ regarding the content and retention of business records and compliance:
  - ✓ The business requirements for business records
  - ✓ The legal and regulatory requirements for records

## THREAT ASSESSMENT & VULNERABILITY ASSESSMENT

- ➔ strategy should consider viable threats regardless of whether a current vulnerability is known to exist.
- ➔ policy development should map to a threat profile.
- ➔ Comprehensive vulnerability assessments that include physical elements—such as procedures, practices, technologies, facilities, service level agreements, and legal and contractual requirement— Even if no known or apparent threats exist for weaknesses discovered during these assessments, cost-effective opportunities to address systemic weaknesses during strategy development should be considered.

# RISK ASSESSMENT




Communication and consultation
Step 1 – Establish the context
RISK ASSESSMENT
Step 2 – Identify the risks
Step 3 – Analyse the risks
Step 4 – Evaluate the risks
Step 5 – Treat the risks
Monitor and review

- ➔ Assessing risk is accomplished by determining the viable threats to information resources. The next consideration is the likelihood that these threats will materialize and their probable magnitude. The next step is to determine the extent of organizational weaknesses and exposure to these threats.
- ➔ The main requirement for IT is an adequate level of performance. information security, it is managing risk to an acceptable level.
- ➔ risk capacity is the tolerable risk that business can handle, board of directors of an organization set the risk appetite.
- ➔ Risk acceptance should not exceed the risk appetite of the organization, but it must not exceed the risk capacity.
- ➔ Risk appetite is determined by senior management and influenced by organizational culture which influences the overall security program design and implementation.
- ➔ Responses to risk are (Accept, Avoid, Transfer, Mitigate), risk calculation is subjective or qualitative.
- ➔ Operational risk management is always a trade-off: If there is a risk associated with taking a particular course of action, there is also a risk of not doing so, some methods for risk calculation: -

- **Value at Risk VAR** is used to compute maximum probable loss in a defined period (day, week, year)
- **Return on Security investment ROSI** is used to calculate the return on investment based on the reduction in losses resulting from security control compared to the cost of the control.
- **Annual loss expectancy ALE** provides the likely annualized loss based on probable frequency and magnitude of security compromise.

- ➔ Established risk management program is a good indicator for governance.

## INSURANCE

- ➔ Common types of insurance: -

- First-party insurance covers the organization in the event of damage from most sources and can include business interruption, direct loss, and recovery costs.
- Third-party insurance deals with potential liability to third parties and includes defense against lawsuits and covers damages up to predetermined limits.
- Fidelity insurance or bonding involves protection against employee or agent theft or embezzlement.

## BUSINESS IMPACT ANALYSIS

➔ A BIA is an exercise that **determines the consequences of losing the support of any resource to an organization and is a part of the risk assessment process.**

➔ General steps to perform business impact analysis: -

- Describe the business mission of each business/cost center.
- Identify the functions that characterize each business function.
- Determine dependencies such as required inputs from other operations.
- Determine subsequent operations dependent on the function.
- Identify critical processing cycles (in terms of time intervals) for each function.
- Estimate the impact of each type of incident on business operations.
- Determine required recovery time (i.e., RTO)
- Identify the resources and activities required to restore an acceptable level of operation.

➔ A mission impact assessment and analysis or BIA prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the criticality of those assets.

➔ To perform BIA is satisfactory manner, it is necessary to obtain the following information:

✓ System mission (e.g., objectives of the processes performed by the IT system or personnel)

✓ System (manual or technical) and data criticality (e.g., the system's value or importance to an organization)

- ✓ System, personnel, and data criticality (the impacts associated with unintended disclosure)
- ✓ Main ingredients of BIA are MTO and criticality of process.

➔ Some tangible impacts can be measured quantitatively, other impacts (e.g., loss of public confidence, loss of credibility) can be described qualitatively in terms of high, medium, and low impacts.

## RESOURCE DEPENDANCY ANALYSIS

➔ Resource dependency can provide another perspective on the criticality of information resources.

➔ It can be used instead of an impact analysis to ensure that the strategy considers resources critical to business operations.

## Security strategy constraints

1. *Legal—Laws and regulatory requirements*
2. *Physical—Capacity, space, environmental constraints*
3. *Ethics—Appropriate, reasonable, and customary*
4. *Culture—Both inside and outside the organization*
5. *Costs—Time, money*
6. *Personnel—Resistance to change, resentment against new constraints.*
7. *Organizational structure—How decisions are made and by whom.*
8. *Resources—Capital, technology, people*
9. *Capabilities—Knowledge, training, skills, expertise*
10. *Time—Window of opportunity, mandated compliance*
11. *Risk appetite—Threats, vulnerabilities, impacts.*

CIA Triad

- Confidentiality / Integrity / availability & non-repudiation
- A clear prioritization of the triad is needed to develop a control policy.

Disclaimer: Use for review after studying our CISM Course – https://cyvitrix.com

REACH OUT cyvitrix@gmail.com for any requests.

# Domain 2: Information Risk management

## Introduction to Risk Management

➔ Risk management is a process that aims to achieve an optimal balance between realizing opportunities for gain and minimizing vulnerabilities and loss.

➔ Risk management is different from managing risk, which is often used synonymously with risk mitigation or risk response.

➔ The structure of an organization's risk function can be centralized (better adherence) or decentralized (based on operational unit risk assessment)

➔ Risk management, BIA, information asset inventory and risk analysis are fundamental prerequisites to developing security strategy.

➔ At an elevated level, risk management is accomplished by balancing risk exposure against mitigation costs and implementing appropriate controls and countermeasures.

➔ risk management must operate at multiple levels, including the strategic, management and operational levels. IT related risks are best integrated with business processes.

➔ It is vital that participation includes representatives from all key business units.

➔ The foundation for effective risk management is a comprehensive risk assessment, the assessment of risk includes three distinct phases:

- ✓ Risk identification.
- ✓ Risk analysis.
- ✓ Risk evaluation.
- ✓ The next step is risk response: - (managing the risk)
    - ▪ Terminate the activity (avoid)
    - ▪ Reduce the risk (mitigate).
    - ▪ Transfer the risk (share).
    - ▪ Retain the risk (accept)

- ➔ The design and implementation of the risk management process in the organization will be influenced by the organization's:
  - ✓ Culture (risk averse or aggressive)
  - ✓ Mission and objectives
  - ✓ Organizational structure
  - ✓ Ability to absorb losses.
  - ✓ Products and services
  - ✓ Management and operation processes
  - ✓ Specific organizational practices
  - ✓ Physical, environmental, and regulatory conditions
- ➔ Outcomes that management will realize from effective risk management are: -
  - ✓ An understanding of the organization's threat, vulnerability, and risk profiles
  - ✓ An understanding of risk exposure and potential consequences of compromise
  - ✓ Awareness of risk management priorities based on potential consequences.
  - ✓ An organizational risk mitigation strategy sufficient to achieve acceptable consequences from residual risk.
  - ✓ Organizational acceptance/deference based on an understanding of the potential consequences of residual risk.
  - ✓ Measurable evidence that risk management resources are used in an appropriate and cost-effective manner.
  - ✓ Provide assurance that top mgmt. is doing their duty.
- ➔ Risk management strategy is the plan to achieve risk management objectives. Those objectives are to achieve an acceptable level of risk across the enterprise based on a variety of factors including:
  - ✓ The ability of the organization to absorb loss.
  - ✓ Management's risk appetite

- ✓ Costs to achieve acceptable risk levels.
- ✓ Risk-benefit ratios.

## Developing risk management program

- ➔ The board of directors and executive management set the tone for the risk management program.
- ➔ Establish Context and Purpose
  - ✓ defining the internal and external environment; organizational structure and lines of authority.
  - ✓ Determining the organization's risk appetite and tolerance
    - ▪ Risk appetite is what is considered by management to be an acceptable level of risk.
    - ▪ risk tolerance is the acceptable level of deviation from the acceptable risk level.
- ➔ Define Scope and Charter clearly.
  - ✓ define the scope of responsibility and authority that specifically falls to the information security manager and to other stakeholders. This helps prevent gaps in the process, improves overall consistency of risk management efforts and reduces unnecessary duplication of effort.
- ➔ Define Authority, Structure and Reporting
  - ✓ Authority to take certain actions and make decisions must be clearly defined.
  - ✓ A lack of clear governance and integration of risk management activities often results in dire consequences, and the information security manager should address such issues by assessing and presenting the risk and making recommendations to senior management.
- ➔ Ensure Asset Identification, Classification and Ownership
  - ✓ A complete and accurate information asset register is necessary to locate all instances of information assets as part of the asset identification process.

- ✓ assets need to be classified in terms of business value or sensitivity and criticality and have an identified owner. This will help promote accountability.
- ✓ Policies requiring asset and risk ownership should be in place, as well as processes established to assign ownership as assets are acquired, transferred, or created.

➔ Determine Objectives

- ✓ It will be necessary to set priorities for the program and prioritize risk accordingly.

➔ Determine Methodologies

- ✓ The information security manager should evaluate the available choices and seek to implement those that are the best for the organization.

➔ Designate Program Development Team

- ✓ designate an individual or team responsible for developing and implementing the information risk management program. Operations staff and board members should assist the risk management committee.

## Process of Risk Management

➔ The best party to perform risk analysis is the process owner as they know the system in depth.

➔ Risk management process effectiveness can be determined <u>based on the number of incidents related to unknown risks.</u>

➔ Establish scope and boundaries.

- ✓ Process for the establishment of global parameters for the performance of risk management within an organization. Both internal and external factors must be considered to provide context.

➔ Identify information assets and valuation.

- ✓ An information asset inventory and valuation process to determine assets at risk.

➔ Perform risk assessment.
  - ✓ A process consisting of risk identification, analysis, and evaluation, including:
    - Identifying viable threats, vulnerabilities, and exposures
    - Analyzing the level of risk and potential impact
    - Evaluating whether the risk meets the criteria for acceptance.
    - Determine risk treatment or response.

➔ Accept residual risk.
  - ✓ The decision and approval by management to accept the remaining risk after the treatment process, if needed.
  - ✓ Residual risk identified after applying new controls or countermeasures.

➔ Communicate about and monitor risk.
  - ✓ exchange and share information related to risk, as well as reviewing the effectiveness of the whole risk management process. Communication of risk is usually performed among decision makers and other stakeholders inside and outside the organization.

➔ Gap analysis in the context of risk management refers to determining the gap between existing controls and control objectives.

➔ Risk assessment should be conducted on an annual basis or whenever meaningful change occurs.

## Performing risk assessment

➔ Selection of proper assessment technique justify the conclusion of security manager regarding managing of risk (Risk response)

➔ Risk assessment should be started from the feasibility study phase of any project.

# Asset classification and control

## *Information asset valuation*

- ➔ Quantitative valuation methodologies are the most precise but can be quite complex once actual and downstream impacts have been analyzed.
- ➔ qualitative in nature, where an independent decision is made based on business knowledge, executive management directives, historical perspectives, business goals and environmental factors.
- ➔ The most straightforward approach is the monetary value that represents the purchase price, replacement cost or book value, if that is representative of the importance to the organization.
- ➔ Other approaches must be considered. If it is an asset that directly or indirectly generates revenue, a computer value such as net present value (NPV) may be a reasonable approach.
- ➔ Another approach is to consider value-add or other more intangible values. For example, an e-commerce application and server may have hardware and software costs of only US $50,000 but are an essential component in generating millions in revenue every month. In this situation, value may be computed in terms of revenue generation or the fiscal impact for any unanticipated downtime.
- ➔ Aggregated risk can happen where one threat vector can compromise many systems whether integrated or not. Aggregated risk can be assessed by penetration testing.
- ➔ Cascading risks happen to tightly integrated systems, causing failure of one element cause a sequence of failures.
- ➔ Cost of asset equal cost of replacement in risk management, and equal cost of opportunity of BIA

## *Assets classification*

- ➔ Information classification is required to determine the relative sensitivity and criticality of information assets. This will provide the basis for protection efforts, business continuity planning and user access control.

- ➔ The least effective option is a business dependency assessment, it can be used in case classification is not possible.
- ➔ dependency assessment identifies and prioritizes the critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions.
- ➔ The first step in the classification process is to ensure the information asset inventory is complete and the location of each asset is identified (internal or external)
- ➔ Risk assessment covers assets that are classified.
- ➔ The identification process must include determining the location of the data, the data owners, data users and data custodians. Data-owners are authorized to the entitlement process for inexperienced users.
- ➔ The rating should be done by the senior management, and a few levels of data is recommended.
- ➔ It is an accepted practice to focus on the impact that a loss of information assets has on the organization rather than on a specific adverse event.
- ➔ Classification should consider the impact of a security breach.
- ➔ Classification purpose is to dictate which security controls are to be implemented.

## Threats Identification

- ➔ Threats may be divided into multiple categories, including:
  - ✓ Physical
  - ✓ Natural events
  - ✓ Loss of essential services
  - ✓ Disturbance due to radiation
  - ✓ Compromise of information
  - ✓ Technical failures

- ✓ Unauthorized actions
- ✓ Compromise of functions

➔ Sources for information regarding threats are:

- ✓ Assessments
- ✓ Audits
- ✓ Business continuity plans
- ✓ Finance
- ✓ Government publications
- ✓ Human resources
- ✓ Insurance companies
- ✓ Management
- ✓ Media
- ✓ Product vendors
- ✓ Security companies
- ✓ Service providers.
- ✓ Threat monitoring agencies
- ✓ Users

➔ Risk related to internal users.

- ✓ Employees are the cause of a considerable number of business impacts, which can be intentional and unintentional.
- ✓ The solution is applying need-to-know and least privilege, but this is an imperfect solution. Any system has trusted insiders, and one of them choosing to violate trust is difficult to either predict or prevent. Collusion between employees can happen, but this normally does not always success.
- ✓ Throughout employment, employees should be reminded of organizational policies and their responsibilities through awareness sessions and regular management reviews.

➔ Advanced persistent threat Typical APT attacks have exhibited the following life cycle:

1. <u>Initial compromise</u>—Attackers use social engineering and spear phishing via email, using zero-day viruses. They may plant malware on a web site that the victimized employees are likely to visit.

2. Establish foothold—Attackers may plant remote administration software in the victim's network and/or create network back doors and tunnels that allow stealth access to network infrastructure.
3. Escalate privileges—APTs use exploits and password cracking to acquire administrator privileges over the victim's computer and expand it to Windows domain administrator accounts.
4. Internal reconnaissance—Attackers collect information on surrounding infrastructure, trust relationships and Windows domain structure.
5. Move laterally—They expand control to other workstations, servers and infrastructure elements and perform data harvesting on them.
6. Maintain presence—APTs ensure continued control over access channels and credentials acquired in previous steps.
7. Complete mission—Attackers exfiltrate stolen data from the victim's network

➔ Indications of emerging threats may include unusual activity on a system, repeated alarms, slow system, or network performance, or new or excessive activity in logs. In many cases, compromise organizations have evidence of emergent threats in their logs well in advance of the actual compromise, but the evidence is not noticed or acted on.

➔ Security review is used to determine the current state of security for various program components.

➔ Audits, security reviews, vulnerability scans and penetration tests are among the approaches that are usually helpful in identifying vulnerabilities. Some typical examples of vulnerabilities include:

- ✓ Defective software
- ✓ Improperly configured hardware/software
- ✓ Inadequate compliance enforcement

- ✓ Poor network design
- ✓ Uncontrolled or defective processes
- ✓ Inadequate governance or management
- ✓ Insufficient staff
- ✓ Lack of knowledge to support users or operations.
- ✓ Lack of security functionality
- ✓ Lack of proper maintenance
- ✓ Poor choice of passwords
- ✓ Transmission of unprotected communications
- ✓ Lack of redundancy
- ✓ Poor management communication

## Risk identification.

- ➔ Identification through: -
  one. Brainstorming
  2. Flow charting
  3. What if?
- ➔ A promising approach is FAIR which provides a reasoned and logical framework for the following:
  - ✓ A method for measuring the factors that drive information risk, including threat event frequency, vulnerability, and loss.
  - ✓ A computational engine that derives risk by mathematically simulating the relationships among the measured factors.
  - ✓ A simulation model that allows one to apply the taxonomy, measurement method and computational engine to build and analyze risk regardless of complexity.
- ➔ Probabilistic Risk Assessment
  - ✓ PRA is a systematic and comprehensive methodology to evaluate risk associated with every life cycle aspect of a complex engineered technological entity, from concept definition through design, construction, and operation, and up to removal from service.
  - ✓ The approach looks to answer three questions:

- What can go wrong? -
- How likely is it?
- What are the consequences?

➔ Risk identification is often accomplished through a knowledgeable group effort developing a variety of risk scenarios and what-ifs. a risk can be related to or characterized by:

- ✓ Its origin—Threat agents such as hostile employees, employees not professionally trained, competitors, governments.
- ✓ A certain activity, event, or incident (i.e., threat)—Unauthorized dissemination of confidential data, competitor deployment of an innovative marketing policy, new or revised data protection regulations, an extensive power failure
- ✓ Its consequences, results, or impact—Service unavailability, loss or increase of market share/profits, increase in regulation, increase, or decrease in competitiveness, penalties.
- ✓ A specific reason for its occurrence—System design error,
- ✓ Protective mechanisms, exposure, and controls (together with an estimate of effectiveness)—Access control and detection systems, policies, security training, market research and surveillance of market
- ✓ Time and place of occurrence—A flood in the computer room during extreme environmental conditions

➔ In selecting a risk identification methodology, the following techniques should be considered:

- ✓ Team-based brainstorming, where workshops can prove effective in building commitment and making use of different experiences.
- ✓ Structured techniques such as flowcharting, system design review, systems analysis, hazard and operability studies, and operational modeling
- ✓ What-if and scenario analysis for less clearly defined situations
- ✓ Threats identified internally and externally mapped to identified and suspected vulnerabilities.

## Risk Ranking

- ➔ Risk ranking is to place risk in an order that can be used to direct the risk response effort.
- ➔ A manager or senior official in the organization must be identified as its owner.
- ➔ A risk owner is accountable for accepting risk based on the organizational risk appetite and should be someone with the budget, authority, and mandate to select the appropriate risk response based on analyses and guidance provided by the information security manager.
- ➔ The owner of a risk also owns any controls associated with that risk and is accountable for ensuring monitoring of their effectiveness.

## Risk Likelihood measurement.

- ➔ The likelihood, or probability, is a measure of the frequency that an event may occur. When identifying risk, likelihood is used to calculate the level of risk based on the number of events, combined with the impact that may occur in a given time, usually a year.
- ➔ Determining likelihood requires consideration of a variety of factors including:
  - ✓ **Volatility**—The probability of a risk may vary depending on the period, the volatility of the situation. When conditions vary a great deal, there may be times when the risk is greater than at other times, increasing unpredictability and, therefore, requiring a higher estimation of risk.
  - ✓ **Velocity**—In this context, velocity is a consideration of the extent of warning of an event and the amount of time between an event occurrence and the subsequent impact.
  - ✓ **Proximity**—This is a term used to indicate the time between an event and the impact (i.e., the greater the velocity, the closer the proximity).

- ✓ **Interdependency**—It is important not to consider risk in isolation, but rather in the organizational context and in relationship to other assets and functions. The materialization of several types of risk might affect the organization differently depending in part on whether the risky events occur concurrently or sequentially.
- ✓ **Motivation**—The extent of an attacker's motivation will affect the chances of success. The nature of the motivation affects, to some extent, the type of assets at risk (i.e., politically motivated nation states will typically target different assets than criminals seeking financial gain, thereby affecting the risk to assets).
- ✓ **Skill**—The level of skill of potential attackers will typically determine the type and value of assets attacked. (i.e., high-value assets are likely to attract more skilled attackers).
- ✓ **Visibility**—High-visibility targets are more likely to be attacked.

➔ Qualitative impact analysis

- ✓ The main advantage of the qualitative impact analysis is that it prioritizes the risk and identifies areas for immediate improvement in addressing the vulnerabilities.
- ✓ The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult.

## Qualitative risk assessment

➔ In qualitative analysis, the magnitude and likelihood of potential consequences are presented and described in detail. Qualitative analysis may be used:

- ✓ An initial assessment to identify risk that will be the subject of further, detailed analysis.
- ✓ Where nontangible aspects of risk are to be considered (e.g., reputation, culture, image)

  - ✓ Where there is a lack of adequate information and numerical data or resources necessary

➔ statistically acceptable quantitative approach can be accomplished by using a five-by-five matrix, semiquantitative analysis, the objective is to assign values to the scales used in the qualitative assessment. These values are usually indicative and not real, which is the prerequisite of the quantitative approach.

➔ The use of semiquantitative analysis may lead to various inconsistencies since the numbers chosen may not accurately reflect analogies among risks, particularly when either consequences or likelihood are extreme.

➔ Typical values for impact are:

- ✓ Insignificant (value = 1): No meaningful impact, or of limited consequence
- ✓ Minor (value = 2): Impact on a small part of the business only, or less than US $1 million impact
- ✓ Major (value = 3): Impact on the organization’s brand, or more than US $1 million impact
- ✓ Material (value = 4): Impact more than US $200 million and requiring external reporting
- ✓ Catastrophic (value = 5): Failure or significant downsizing of the organization

➔ Typical values for likelihood are:

- ✓ Rare (value = 1)
- ✓ Unlikely (value = 2): Not seen within the last five years
- ✓ Moderate (value = 3): Seen within the last five years but not within the last year
- ✓ Likely (value = 4): Seen within the last year
- ✓ Frequent (value = 5): Happens on a regular basis

➔ One of methods to enhance subjective aspect of RA is train or calibrate the assessor, training helps to improve accuracy and reduces subjectivity.

## Quantitative risk assessment

➔ numerical values are assigned to both impact and likelihood. These values are derived from a variety of sources. The quality of the entire analysis depends on the accuracy of the assigned values and the validity of the statistical models used.

➔ Consequences may be expressed in various terms of:

- ✓ Monetary (loss of power, loss of frame-relay)
- ✓ Technical
- ✓ Operational
- ✓ Human impact criteria

➔ Quantitative risk assessments attempt to arrive at a numerical value, the most common forms are: -

- ✓ SLE is the product of the asset value (AV) multiplied by the exposure factor (EF): SLE = AV × EF.
- ✓ ALE adds the annualized rate of occurrence (ARO) to the equation with the result that multiple occurrences will result in greater potential losses. ALE is usually expressed as: ALE = SLE × ARO.
- ✓ ARO is the number of times a threat on a single asset is estimated to occur. The higher the risk associated with the threat, the higher the ARO.
- ✓ VAR is a computation based on historical data of the probability distribution of loss for a given period at a certainty factor typically of 95 percent or 99 percent.

➔ The major advantage of a quantitative impact analysis is that it provides a measurement of the impacts' magnitude, which can be used in the cost-benefit analysis of recommended controls.

➔ The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner.

- One of the characteristics of quantitative method is it contains percentage estimate.

## Risk analysis methods.

- The OCTAVE methodology is process-driven and used to identify, prioritize, and manage information security risk. It helps organizations:
  - ✓ Develop qualitative risk evaluation criteria based on operational risk tolerance.
  - ✓ Identify assets that are critical to the mission of the organization.
  - ✓ Identify vulnerabilities and threats to critical assets.
  - ✓ Determine and evaluate potential consequences to the organization if threats are realized.
  - ✓ Initiate corrective actions to mitigate risk and create practice-based protection strategy.
- OCTAVE focuses on critical assets and the risk to those assets using a comprehensive, systematic, context-driven, and self-directed evaluation approach.
- The OCTAVE process is based on three phases:
  - ✓ Phase 1: Build asset-based threat profiles (organizational evaluation)—
  - ✓ Phase 2: Identify infrastructure vulnerabilities.
  - ✓ Phase 3: Develop security strategy and mitigation plans.
- Other Risk Analysis Methods
  - ✓ Bayesian analysis—A Bayesian analysis is a method of statistical inference that uses prior distribution data to determine the probability of a result. This technique's effectiveness and accuracy rely on the accuracy of the prior distribution data.

- ✓ Bow tie analysis—A bow tie analysis provides a diagram to communicate risk assessment results by displaying links among probable causes, controls, and consequences.
- ✓ Delphi method—The Delphi method uses expert opinion, which is often received using two or more rounds of questionnaires. After each round of questioning, the results are summarized and communicated to the experts by a facilitator. This collaborative technique is often used to build a consensus among the experts.
- ✓ Event tree analysis—An event tree analysis is a forward-looking, bottom-up model that uses inductive reasoning to assess the probability of different events resulting in outcomes.
- ✓ Fault tree analysis—A fault tree analysis starts with an event and examines the means for the event to occur (top down) and displays these results in a logical tree diagram.
- ✓ Markov analysis—A Markov analysis is used to analyze systems that can exist in multiple states. The Markov model assumes that future events are independent of past events.
- ✓ Monte-Carlo analysis—used to establish the aggregate variation in a system resulting from variations in the system, for several inputs, where each input has a defined distribution, and the inputs are related to the output via defined relationships. The analysis can be used for a specific model where the interactions of the various inputs can be mathematically defined. Risk ranking.

## Risk Response

## Risk transfer.

- ➔ Third-party agreements and contracts must specifically address the liability and responsibilities of both parties in specific indemnification clauses.
- ➔ Indemnity agreements that can be part of an outsourced service agreement provide a level of protection or reduce the impact against

harmful incidents, the legal responsibility for the consequences of compromise cannot be transferred.

➔ Risk is typically transferred to insurance companies when the probability of an incident is low, but the impact is high.

## Risk acceptance.

➔ Acceptance of risk should be regularly reviewed to ensure that the rationale for the initial acceptance is still valid within the current business context and ensure that residual risk is equal to the organization's criteria for acceptable risk and risk tolerance.

➔ The essential concept is that the cost of protection should be proportional to the value of the asset and should not exceed the value of the asset being protected (cost benefit analysis as per GASSP & GAISP)

➔ Final acceptance of residual risk considers:

- ✓ Regulatory compliance
- ✓ Organizational policy
- ✓ Sensitivity and criticality of relevant assets
- ✓ Acceptable levels of potential impacts
- ✓ Uncertainty inherent in the risk assessment approach
- ✓ Cost and effectiveness of implementation

➔ When consider cost of asset; the Total cost of ownership (TCO) must be considered for the full life cycle of the control or countermeasure. This can include elements such as:

- ✓ Acquisition costs
- ✓ Deployment and implementation costs
- ✓ Recurring maintenance costs
- ✓ Testing and assessment costs
- ✓ Compliance monitoring and enforcement
- ✓ Inconvenience to users.
- ✓ Reduced throughput of controlled processes
- ✓ Training in new procedures or technologies as applicable

- ✓ End-of-life decommissioning.

## RTO RPO SDO - MTO - AIW

- ➔ RTOs are determined by performing a BIA in coordination with developing a BCP.
- ➔ Once the RTOs are known, the organization can identify and develop contingency strategies that will meet the RTOs of the information resources.
- ➔ RTOs will drive the order of priority for restoration of services and, in certain cases, the selection of specific recovery technologies in situations where the RTO is short.
- ➔ In general, the cost of recovery is less if the RTO for a given resource is longer.
- ➔ The RPO is determined based on the acceptable data loss in case of disruption of operations. Higher levels of service will require greater resources as well as more current RPOs.
- ➔ SDOs are defined as the minimal level of service that must be restored after an event to meet business requirements until normal operations can be resumed.
- ➔ MTO refers to the maximum time an organization can operate in alternate (or recovery) mode. Numerous factors may affect the MTO, such as accessibility of a recovery site that might be located remotely and limited operational capacity of the recovery site.
- ➔ AIW is the amount of time the normal operations can be down before the organization faces major financial difficulties that threaten its existence.
- ➔ MTO is larger than AIW.

## Third Party relationship and Risk Management

- ➔ Outsourced information resources may present an information security manager with other challenges, including external

Disclaimer: Use for review after studying our CISM Course – https://cyvitrix.com

organizations that may be reluctant to share technical details on the nature and extent of their information protection mechanisms.

- ✓ This makes it critical to ensure that adequate specified levels of protection are included in SLAs and other outsourcing contracts.
- ✓ One common approach is to specify requirements for specific audits such as SOC 2
- ✓ Note that SOC 2 reports are often not sufficient on their own because the criteria have been defined by the organization in question.

- ➔ For high-risk relationships, it is preferable to rely on periodic compliance assessments conducted directly by the sourcing organization or a contracted third party.
- ➔ From a risk management perspective, it is also important that incident management and response, BCP/DRP, and testing include all important outsourced services and functions.
- ➔ For regulated organizations such as financial institutions, a time frame for notification of regulatory agencies regarding suspicious events involving regulated information is often in place.
- ➔ Because outsourcing contracts are often awarded to low-cost bidders, the risk of the outsourcing organization continuing to operate according to the contract and to honor any indemnity agreements may be a function of their financial capabilities.
- ➔ Some portion of risk associated with outsourced information services can be transferred by incorporating indemnity clauses in SLAs.
- ➔ Key clauses that should be part of a third-party contract must include, but are not restricted to:
  - ✓ Right to source code in event of default of provider (e.g., source code escrow)
  - ✓ Requirement that the vendor remain timely with compliance to requirements.
  - ✓ Right to audit the vendor's books of accounts and premises

- ✓ Right to review the vendor's processes
- ✓ Insistence on standard operating procedures (SOPs)
- ✓ Right to assess the skill sets of the vendor resources.
- ✓ Advance information if the resources deployed are to be changed.

➔ The information security manager has several considerations to address when outsourcing, including:

- ✓ Ensuring that the organization has appropriate controls and processes in place to facilitate outsourcing.
- ✓ Ensuring that there are appropriate information risk management clauses in the outsourcing contract.
- ✓ Ensuring that a risk assessment is performed for the process to be outsourced.
- ✓ Ensuring that an appropriate level of due diligence is performed prior to contract signature, due diligence is closely related to standard care which means this action would be taken by a person in similar circumstances.
- ✓ Managing the information risk for outsourced services on a day-to-day basis
- ✓ Ensuring that material changes to the relationship are flagged and new risk assessments are performed as required.
- ✓ Ensuring that proper processes are followed when relationships are ended.

➔ The disconnection between control definition and control implementation makes managing the risk associated with outsourcing business functions complex and renders the outsourcing contract essential in managing information risk.

➔ When managing relations with third party, the goal is to reduce the exposure as much as possible.

## Change management and RA.

- ➔The information security manager must be aware of these change management activities and ensure that security is well entrenched in the change process.
- ➔information security management to participate as a member of the change management committee and ensure that all significant changes are subject to review and meet requirements.
- ➔The change management process must include facilities management with respect to data center infrastructure and any other area that may impact overall information security.
- ➔Effective risk management must be fully integrated into the system development life cycle (SDLC).
- ➔Employing a life-cycle-based risk management approach and integration with change management improves costs in that a full risk assessment does not have to be performed periodically.

## Security baseline

- ➔A baseline is defined as "an initial set of critical observations or data used for comparison or a control.," it sets the minimum-security requirements throughout the organization, so they are consistent with acceptable risk levels.
- ➔To establish control baselines, security managers can refer to standards.
- ➔Controls suitable for the organization must be developed based on a variety of factors such as culture, structure, risk appetite and tolerance.

- ➔The effectiveness of security measures or controls should be assessed against control objectives and/or security baselines. Acceptable risk determines control objectives, which become the main objectives of the strategy.

## Metrics and reporting

- ➔ Effective metrics for risk management, including evaluating controls, can be selected based on the best ranking of the following characteristics:
  - ✓ Specific Based on a clearly understood goal; clear and concise.
  - ✓ Measurable—Able to be measured; quantifiable (objective), not subjective.
  - ✓ Attainable—Realistic; based on important goals and values.
  - ✓ Relevant—Directly related to a specific activity or goal.
  - ✓ Timely Grounded in a specific time frame
  - ✓ Meaningful Understood by the recipients.
  - ✓ Accurate—A reasonable degree of accuracy
  - ✓ Cost-effective—Not too expensive to acquire or maintain.
  - ✓ Repeatable—Able to be acquired reliably over time.
  - ✓ Predictive—Indicative of outcomes
  - ✓ Actionable—Clear to the recipient what action must be taken.
- ➔ Communication channels must be established both for reporting and disseminating information relevant to managing risk as well as providing the information security manager with information about risk-related activities throughout the enterprise, which includes reporting significant changes in risk, training, and awareness.
- ➔ Senior management will typically have little interest in technical details and are likely to want an overview of the status and indicators of any immediate or impending threat that requires attention. Red-amber-green reports, often referred to as security dashboards, heat charts or stoplight charts, quickly and clearly show the status of remediation efforts.

## Risk Management deliverable.

- ➔ Appropriate documentation that is readily available regarding risk management policies and standards, as well as other relevant risk-related matters, is required to effectively manage risk.

➔ All documentation should be subject to an effective version control process as well as a standard approach to marking and handling. Documentation should be conspicuously labeled with classification level, revision date and number, effective dates, and document owner.

➔ documentation should include:

- ✓ Objectives
- ✓ Audience
- ✓ Information resources
- ✓ Assumptions
- ✓ Decisions

➔ A risk management policy document includes information such as:

- ✓ Objectives of the policy and rationale for managing risk
- ✓ Scope and charter of information risk management
- ✓ Links between the risk management policy and the organization's business plans.
- ✓ Extent and range of issues to which the policy applies.
- ✓ Guidance on what is considered acceptable risk levels.
- ✓ Risk management responsibilities.
- ✓ Support expertise available to assist those responsible for managing risk.
- ✓ Level of documentation required for various risk-management-related activities.
- ✓ A plan for reviewing compliance with the risk management policy.
- ✓ Incident and event severity levels
- ✓ Risk reporting and escalation procedures.

➔ Typical documentations include: -

- ✓ A risk register, which serve as a central repository for all information security risks including: -

  - Source of risk
  - Nature of risk
  - Risk owner.
  - Risk ranking by severity.

  - Selected treatment option
  - Existing controls
  - Recommended controls not implemented and why not implemented.
- ✓ Consequences and likelihood of compromise, including:
  - Income loss
  - Unexpected expense
  - Legal risk (compliance and contractual)
  - Interdependent processes
  - Loss of public reputation or public confidence
- ✓ Initial risk rating
- ✓ Vulnerability to external/internal factors
- ✓ An inventory of information assets, including IT and telecommunication assets, that lists:
  - Description of the asset
  - Technical specifications
  - Number/quantity.
  - Location
  - Special licensing requirements if any
- ✓ A risk mitigation and action plan, providing:
  - Who has responsibility for implementing the plan?
  - Resources to be utilized.
  - Budget allocation
  - Timetable for implementation.
  - Details of mechanism/control measures
  - Policy compliance requirements
- ✓ Monitoring and audit documents, which include:

- Outcomes of audits/reviews and other monitoring procedures
- Follow-up of review recommendations and implementation status

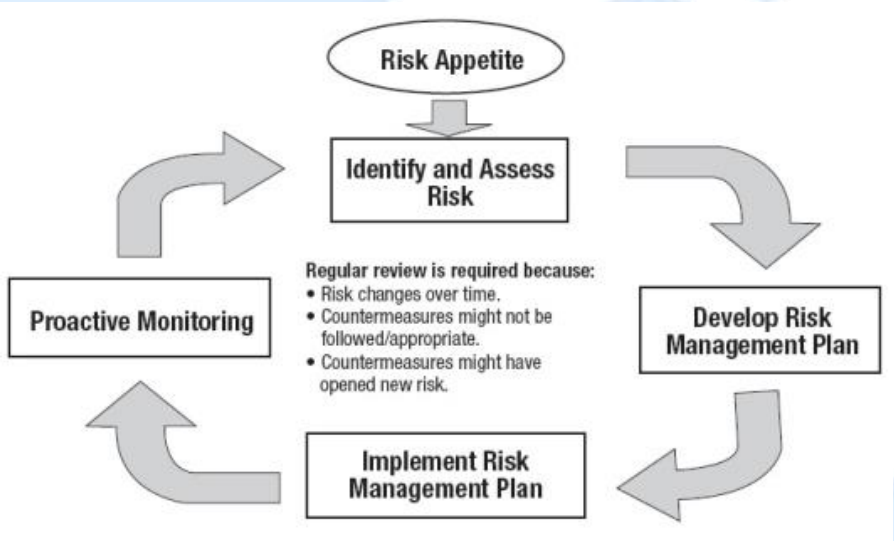
➔ Privacy policy must contain notification information in case of leakage or disclosure, also how information will be collected and used.

➔ Reducing exposure will reduce the likelihood.

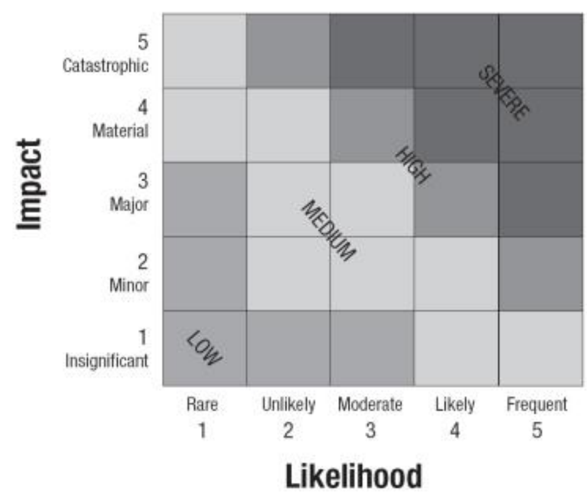
➔ Assurance process integration provide effective risk management across the corporate

➔ Workflow analysis will be the first step in integrating risk management with business.

➔ Consequence means impact, frequency means likelihood.



Regular review is required because:
- Risk changes over time.
- Countermeasures might not be followed/appropriate.
- Countermeasures might have opened new risk.



## NIST approach

one. System characterization

two. Threat identification

three. Vulnerability identification

control analysis

five. Likelihood determination

six. Impact analysis

seven. Risk determination

eight. Control recommendations

nine. Results documentation

## Security principles

1. Data classification
2. Least privilege.
3. Separation of duties
4. Multi-person control
5. Mandatory vacations
6. Job rotation
7. Due diligence -> carefully planned and thought.
8. Due care -> performed actions to prevent bad actions.

You can link this principle by what infosec can provide for each business entity.

## Security investments

1. Training
2. Anticipated features/upgrades
3. Compliance
4. Business strategy
5. Security strategy
6. Incremental investments

## Questions to consider when thinking about a new investment.

1. Is there a valid business needs or requirement for modern technology?
2. Is this the right solution to fulfill the business need?
3. What is the cost versus benefit of implementing modern technology?

Example of Detective controls, it discovers the attack and triggers the preventive control.

1. Audit trails.
2. IDS

Example of deterrent controls, it reduces likelihood of occurrence.

1. User Policy
2. Restricted access sign

Example of corrective controls < it decreases impact>

1. Data correction
2. Error correction

Example of compensating controls, it reduces likelihood of occurrence.

1. DLP
2. Insurance

Awareness training and SOD are preventive controls, it reduces impact and protects vulnerability.

# Domain 3: Security Program Development

## Introduction

➔ Primary drivers for an information security program include:

✓ The ever-increasing requirements for regulatory compliance

✓ Higher frequency and cost related to security incidents.

✓ Concerns over reputational damage

✓ Growing commercial demands of Payment Card Industry Data Security Standard

✓ Business processes or objectives that may increase organizational risk.

➔ CSFs of successful Security program

✓ The program must be the execution of a well-developed information security strategy closely aligned with and supporting organizational objectives.

✓ The program must be well designed with cooperation and support from management.

✓ Effective metrics must be developed for program design and implementation phases as well as the subsequent ongoing security program management phases to provide the feedback necessary to guide program execution to achieve the defined outcomes.

➔ objectives should be explicitly linked to organizational objectives.

➔ The information security manager must develop defined objectives for the information security program and gain management and stakeholder consensus and devise effective information security management metrics.

➔ Program can fulfill Strategic Alignment requirements by: -

✓ Assessing organizational information risk

✓ Selection of appropriate control objectives and standards

✓ Gaining agreement on acceptable risk and risk tolerance

- ✓ Definitions of financial, operational, and other constraints

➔ An information security program includes a core set of common objectives:

- ✓ Achieve acceptable levels of risk and loss related to information security issues.
- ✓ Support achievement of overall organizational objectives.
- ✓ Support organizational achievement of compliance.
- ✓ Maximize the program's operational productivity.
- ✓ Maximize security cost-effectiveness.
- ✓ Establish and maintain organizational security awareness.
- ✓ Facilitate effective logical, technical, and operational security architectures.
- ✓ Maximize effectiveness of program framework and resources.
- ✓ Measure and manage operational performance.

➔ There are several different frameworks that can be used.

- ✓ COBIT 5 is based on five key principles.
- ✓ ISO/IEC 27002:2013:
  - ▪ The 114 control in the fourteen domains of ISO/IEC 27001:2013 can be mapped to COBIT, but they are less business-oriented and comprehensive and do not provide complete tool sets. it includes fourteen broad control areas:
    - ➢ A.5: Information security policies
    - ➢ A.6: Organization of information security
    - ➢ A.7: Human resource security (before, during or after employment)
    - ➢ A.8: Asset management
    - ➢ A.9: Access control
    - ➢ A.10: Cryptography
    - ➢ A.11: Physical and environmental security

- A.12: Operations security
- A.13: Communications security
- A.14: System acquisition, development, and maintenance
- A.15: Supplier relationships
- A.16: Information security incident management
- A.17: Information security aspects of business continuity management
- A.18: Compliance

## Program preparation.

- members of the information security steering committee hold functional roles that can promote awareness of the policy and conduct internal security reviews to see if they comply.
- The information security manager can begin the work of building consensus around roles and responsibilities, processes, and procedures in support of the policy.
- Construction of specific projects and initiatives must be planned, along with budgets, timetables, personnel, and other tactical project management aspects that will result collectively in achieving the strategy objectives. It is like the differences between the architecture of a house and the tasks required to build the house.
- An important skill to have in developing an information security program road map is the ability to thoroughly review the security level of existing data, applications, systems, facilities, and processes.
- An implementation road map can be a high-level project plan (or set of project plans) or an architectural design that can serve the same purpose.
- road map should include various milestones that will provide KGIs, indicate KPIs and define critical success factors (CSFs).
- Those executing new processes and procedures should concentrate on KGIs and KPIs, frequently validating that control objectives are

being met and progress toward control objectives achieves information security program goals.

## Risk Management

- ➔ Managing the risk to information assets is a primary responsibility of the information security manager and provides the foundation for all information security activities.
- ➔ Risk analysis must be based on business requirements and an understanding of the organization’s processes, culture, and technology.
- ➔ acceptable risk at an acceptable cost can be determined by developing (RTOs), which will serve to balance the cost of restoration against acceptable outages.

## Security Management Framework

- ➔ The various components that make up the management framework can be broken to: -

## Technical Components

- ✓ Many of the key controls identified in the framework will address risk associated with the technical components, including their configuration, monitoring, maintenance, and operation.
- ✓ It is essential that all technology components have an identified owner and that there are no “orphan systems.” This is necessary to ensure responsibility and accountability.
- ✓ The information security function must adequately regulate the IT function and provide oversight to ensure policy compliance sufficient to achieve acceptable risk levels consistent with the information security strategy objectives.

## Operational Components

- ✓ Operational components of a security program are the ongoing management and administrative activities that must be performed to provide the required level of security assurance.
- ✓ The information security manager should ensure that procedures for log maintenance, issue escalation, management oversight, and periodic risk assessment and quality assurance reviews are developed and implemented.

## Management Components

- ✓ The information security manager needs to consider several management components. These typically include strategic implementation activities such as standards development or modification, policy reviews, and oversight of initiatives or program execution.
- ✓ less frequently than operational components It should be considered that early versions are often too permissive, too restrictive or misaligned with operational realities. As a result, the information security manager is well advised to exercise flexibility in adjusting standards and policy interpretation during the initial stages of a security program.

## Administrative Components

- ✓ personnel and financial aspects involved. information security management must address the same business administration activities as other business units.
- ✓ Financial administration functions consist of budgeting, timeline planning, total cost of ownership (TCO) analysis/management, return on investment (ROI) analysis/management, acquisition/purchasing and inventory management.
- ✓ It is the role of the information security manager to document and ensure that executive management understands the risk implications

of moving an initiative ahead without full security diligence; it is up to executive management to decide if the initiative is important enough to warrant the risk. If this situation occurs, the information security manager should make every effort to utilize the first available opportunity to revisit systems or initiatives that are not certified or accredited.

- ✓ To ensure that the existing security environment operates as needed, security operational resources should be diverted to project efforts only if they are not fully utilized. Even in this situation, it needs to be clearly communicated that operational security resources are provided ad hoc, and a spike in operational activities (e.g., an intrusion) requires the immediate attention of the operational staff.

## Educational and Informational Components

- ✓ The information security manager should collaborate with HR and business units to identify information security education needs.
- ✓ Interactive education techniques such as online testing and role-playing are often more effective than a purely informational approach. Examples of these types of training include incident response and contingency plan training and exercises.
- ✓ awareness is required to educate those affected by security policy on their roles and responsibilities. should fit in with the culture of the organization and management’s preferred method of communication. parallel approaches are likely to be most effective.
- ✓ Pertinent metrics (e.g., average employee quiz scores) should be tracked and communicated to the steering committee and executive management.
- ✓ It may be most effective to develop a road map for the information security program in stages, starting with simple objectives designed to demonstrate the value of the program and provide feedback on achievement of the key goals.

- ✓ To get started, an information security manager can interview stakeholders such as department heads in HR, legal, finance and major business units to determine important organizational issues and concerns. Information taken from such interviews will point to candidates for information security steering committee members.

## Enterprise Information Security Architecture

- ➔ Enterprise InfoSec Arch "EISA" objective is not just to manage security technology but to address the related elements of business structure, performance management and security processes as well.
- ➔ Architecture can serve to define logical, physical, and operational components and process relationships. It can also clarify potential issues and provide traceability from concept to implementation and operation.
- ➔ Architecture should be aligned with Business objectives and goals.

## EISA Objective

- ✓ Provide overarching structure, coherence, and cohesiveness.
- ✓ Serve as a program development road map.
- ✓ Ensure strategic alignment between business and security.
- ✓ Support and enable achievement of business strategy.
- ✓ Implement security policies and strategy.
- ✓ Ensure traceability back to the business strategy, specific business requirements.
- ✓ Provide a level of abstraction independent of specific technologies and
- ✓ Establish a common language for information security within the organization.
- ✓ Allow many individual contributors to work together to achieve objectives.

## Common architecture approaches

➔These approaches fall into three basic categories: process approaches, frameworks, and reference models.

- ✓ The essence of the frameworks is to describe the elements of architecture and how they must relate to each other.
- ✓ Process models are more directive in the processes used for the various elements.
- ✓ Reference models are a small-scale representation of the actual implementation.

➔The TOGAF Architecture Development Method (ADM) phases: -

- ✓ Preliminary phase—Deals with the definition of the architecture framework, as well as the architecture principles. In addition, the overall scope, constraints, objectives, and assumptions are identified.
- ✓ Architecture vision—Deals with defining the vision and scope of architecture.
- ✓ Business architecture—Addresses the description of the as-is business architecture domain, the development of the to-be business architecture and the gap analysis.
- ✓ Information systems architecture—Provides the description of the as-is and to be data, applications domains and conducting the gap analyses.
- ✓ Technology architecture—Deals with the description of the as-is and to-be technology domains and conducting a gap analysis.
- ✓ Opportunities and solutions—Deals with the formulation of a high-level implementation and migration strategy to transform the as-is architectures into the to-be architecture.
- ✓ Migration planning—Deals with formulation of a detailed implementation and migration road map, including the analysis of costs, benefits, and risk.

- ✓ Implementation governance—Ensures that the implementation projects conform to the defined architecture.
- ✓ Architecture change management—Deals with keeping the architecture up to date and ensures that the architecture responds to the needs of the enterprise, as changes arise.
- ✓ Requirements management—Ensures that the architecture projects are based on business requirements and the business requirements are validated against the architecture.

➔ There are four commonly accepted subsets of an overall enterprise architecture: -

- ✓ A business (or business process) architecture defines the business strategy, governance, organization, and key business processes.
- ✓ A data architecture describes the structure of an organization's logical and physical data assets and data management resources.
- ✓ An applications architecture provides a blueprint for the individual application systems to be deployed, their interactions and their relationships to the core business processes of the organization.
- ✓ A technology architecture describes the architectural principles, component relationships, and hardware and software infrastructure intended to support the deployment of core, mission-critical applications.

➔ An effective approach must start with the enterprise business architecture. The subsequent designs, such as application, security and data architectures, function as subsets to ensure alignment with and support of business strategy and objectives.

➔ The contextual architecture serves to define the relationships among various required business attributes. These include who, what, when, where and how, which drives the next layer, the conceptual layer, which integrates the architectural design concepts with the business requirements.

- ➔ The next layer, the logical architecture, describes the same elements in terms of the relationships of logical elements. This is followed by a physical layer, which identifies the relationships among various security mechanisms that will execute the logical relationships and the component architecture consisting of the actual devices and their interconnections. Finally, there is the operational architecture, describing how security service delivery is organized.
- ➔ One of the key functions of architecture as a tool is to provide a framework within which complexity can be managed successfully.
- ➔ Architecture also acts as a road map for a collection of smaller projects and services that must be integrated into a single homogenous whole.
- ➔ Information systems architecture must, therefore, take account of:

- ✓ The goals that are to be achieved through the systems.
- ✓ The environment in which the systems will be built and used.
- ✓ The technical capabilities of the people to construct and operate the systems and their component subsystems.

- ➔ Information systems architecture is concerned with much more than technical factors. It is concerned with what the enterprise wants to achieve and with the environmental factors that will influence those achievements.
- ➔ It may be useful for the information security manager to consider the following checklist for a comprehensive, well-managed security program:

- ✓ A security strategy intrinsically linked with business objectives that has senior management acceptance and support.
- ✓ Security policy and supporting standards that are complete and consistent with strategy.
- ✓ Complete and accurate security procedures for all important operations

- ✓ Clear assignment of roles and responsibilities
- ✓ Established method to ensure continued alignment with business goals and objectives such as a security steering committee.
- ✓ Information assets that have been identified and classified by criticality and sensitivity.
- ✓ Security architecture that is complete and consistent with strategy, and in line with business objectives
- ✓ Effective controls that have been well-designed, implemented and maintained.
- ✓ Effective monitoring processes in place
- ✓ Tested and functional incident and emergency response capabilities
- ✓ Tested business continuity/disaster recovery plans.
- ✓ Appropriate information security involvement in change management, SDLC and project management processes
- ✓ Established processes to ensure that risk is properly identified, evaluated, communicated, and managed.
- ✓ Established security awareness training for all users.
- ✓ Established activities that create and sustain a corporate culture that values information security.
- ✓ Established processes to maintain awareness of current and emerging regulatory and legal issues.
- ✓ Effective integration with procurement and third-party management processes
- ✓ Resolution of noncompliance issues and other variances in a timely manner
- ✓ Processes to ensure ongoing interaction with business process owners.
- ✓ Business-supported processes for risk and business impact assessments, development of risk mitigation strategies, and enforcement of policy and regulatory compliance

- ✓ Established operational, tactical, and strategic metrics that monitor utilization and effectiveness of security resources.
- ✓ Established methods for knowledge capture and dissemination.
- ✓ Effective communication and integration with other organizational assurance providers

- ➔ Some outcomes that may indicate a successful security culture are: The information security department is brought into projects at the appropriate times, end users know how to identify and report incidents, the organization can identify the security manager, and people know their role in protecting the information assets of the organization and integrating information security into their daily practices.
- ➔ An effective way of assisting these general users in understanding security-related responsibilities is the development of an acceptable use policy.
- ➔ This policy can detail, in everyday terms and a straightforward and concise manner, the obligations and responsibilities of all users.
- ➔ Codes of ethics and conduct should be reviewed and acknowledged by each employee involved in information security management and other applicable duties. The signed acceptance of the code should be kept as a part of employee records.
- ➔ Documents that commonly pertain to the program include:

- ✓ Policies, standards, procedures, and guidelines
- ✓ Technical diagrams of infrastructure and architectures, applications, and data flows
- ✓ Training and awareness documentation
- ✓ Risk analyses, recommendations, and related documentation.
- ✓ Security system designs, configuration policies and maintenance documentation

- ✓ Operational records such as shift reports and incident tracking reports.
- ✓ Operational procedures and process flows
- ✓ Organizational documentation such as organization charts, staff performance objectives and RACI models

➔ Many costs associated with an information security program are straightforward. Elements of each project that should be considered include:

- ✓ Employee time
- ✓ Contractor and consultant fees
- ✓ Equipment (hardware, software) costs
- ✓ Space requirements (data center rack space, etc.)
- ✓ Testing resources (personnel, system time, etc.)
- ✓ Training costs (staff, users, etc.)
- ✓ Travel
- ✓ Creation of supporting documentation
- ✓ Ongoing maintenance
- ✓ Contingencies for unexpected costs

➔ Problem management is focused on ascertaining the root causes of issues. Mitigating controls that may have to be employed if the primary security control fails.

➔ release management reduces the chances of operational failure by ensuring adequate testing has been performed and required conditions exist for the correct operation of new software, devices, or systems.

➔ Rather than allowing the security vulnerability to put the organization at risk, it may be necessary for the information security manager to take alternative actions to protect the information resources until the problem is resolved.

➔ While the information security manager must determine the most appropriate scope for assessing current state, the following section outlines several critical areas for evaluation: -

- **Program Objectives**

✓ Has an information security strategy and development road map been developed?
✓ Have criteria for acceptable risk and impact been determined?
✓ Do complete and current policies, standards and procedures exist?
✓ Are program goals aligned with governance objectives?
✓ Are objectives measurable, realistic, and associated with specific timelines?
✓ Do program objectives align with organizational goals, initiatives, compliance needs and operational environment?
✓ Is there consensus on program objectives? Were objectives developed collaboratively?
✓ Have metrics been implemented to measure program objective success and shortfalls?
✓ Are there regular management reviews of objectives and accomplishments?

- **Compliance Requirements**

✓ Has management determined the level of compliance the organization will undertake as well as timelines and milestones?
✓ Is there facilitation of close communication between compliance and information security groups?
✓ Are information security compliance requirements clearly defined?
✓ Does the information security program specifically integrate compliance requirements into policies, standards, procedures, operations, and success metrics?

- ✓ Do the program's technical, operational, and managerial components align with the components required by regulatory standards?
- ✓ What have been the results of recent audit and compliance reviews of the information security program?
- ✓ Are program compliance deficiencies tracked, reported, and addressed timely?
- ✓ Are compliance management technologies used to increase the efficiency of fulfilling security compliance demands?

- **Program Management**

- ✓ 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 organizations understand and engage in their responsibilities?
- ✓ Are responsibilities for information security represented in business managers' individual objectives and part of their individual performance rating?
- ✓ Are policies and standards complete, 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 (e.g., budgeting, fiscal management, HR management, knowledge management)?
- ✓ 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?

- **Security Operations Management**

- ✓ Are security requirements and processes included in security, technology, and business unit standard operating procedures (SOPs)?
- ✓ Do security-related SOPs provide accountability, process visibility and management oversight?
- ✓ Are there documented SOPs for security-related activities such as configuration management, access management, security systems maintenance, event analysis and incident response?
- ✓ Is there a schedule of regularly performed procedures (e.g., technical configuration review)? Does the program provide records of scheduled activities?
- ✓ Is there segregation of duties (SoD) among system implementers, security administrators and compliance personnel?
- ✓ Does the program provide for effective operational, tactical, and strategic metrics reporting that provides management with needed information for oversight? Are other oversight mechanisms in place?
- ✓ Does management regularly review security operations? Is there a forum for operational issues to be escalated to management for resolution?

- **Technical Security Management**

- ✓ Are there technical standards for the security configuration of individual network, system, application, and other technology components?
- ✓ Do standards exist that address architectural security issues such as topology, communication protocols and compartmentalization of critical systems?
- ✓ Do standards support and enforce high-level policies and requirements? Are standards a collaborative effort among technology, operations, and security staff?
- ✓ Are technical standards uniformly implemented? Do procedures exist to regularly evaluate and report on compliance with technical standards?
- ✓ Is there a formal process to manage exceptions?
- ✓ Is there continuous monitoring of key controls? Do controls provide notification of failure?
- ✓ Is separation of development, test and production environments enforced?
- ✓ Do systems enforce SoD, especially where elevated levels of administrative access are concerned?
- ✓ Is there reliable and comprehensive visibility (logging) into system activities, configurations, accessibility, and security-related events? Is this visibility continual or intermittent?
- ✓ Are proper decommissioning processes in place to prevent data leakage?

➔ Resource Levels available of CISO: -

- **Financial resources:**

- ✓ What is the current funding level for the program?
- ✓ Is a comprehensive capital and operating budget maintained?
- ✓ Do financial allocations align with program budget expectations?
- ✓ Are there links between resource allocation and business objectives?

Disclaimer: Use for review after studying our CISM Course – https://cyvitrix.com

REACH OUT cyvitrix@gmail.com for any requests.

- ✓ Are functions within the program prioritized in terms of finance?
- ✓ Which functions are likely to suffer from underfunding?

- **HR:**

- ✓ Does the program implement a workload management methodology?
- ✓ What is the current staffing level for the program?
- ✓ Are existing resources fully utilized in terms of time and skills?
- ✓ Are existing resources adequately skilled for the roles they are in?
- ✓ Are there low-value tasks that other resources could be leveraged to complete?
- ✓ What other human resources (e.g., IT staff) is the program dependent on to operate effectively?
- ✓ Is information security a formal part of these resources' job descriptions and activity plans?

- **Technical resources:**

- ✓ What technologies currently support information security program objectives?
- ✓ Is the capacity of supporting technologies sufficient to support current demands? Will these technologies scale to meet future needs?
- ✓ Does the program account for maintenance, administration, and eventual replacement of supporting technologies?
- ✓ Are there other technologies that could make the program more efficient or effective?

- ❖ The unique dependency on the effective, efficient management of a business process such as information security lends itself to the concepts and methodologies encompassed within the total quality management (TQM) system. TQM is based on cycle made up of four primary processes, plan-do-check-act (PDCA).

- ❖ The basic elements of a governance methodology include a strategic vision, objectives, KGIs, CSFs, KPIs, and key actions or tactical and annual action plans.
- ❖ The impacted department will be the most knowledgeable about legal and regulatory issues.
- ❖ the information security manager must ensure that physical security policies, standards and activities are sufficient to not jeopardize information security efforts.
- ❖ Access should be provided on an as-needed basis. Locating critical systems in areas with unstable environments or in proximity to water pipes or other potential hazards should be avoided.
- ❖ The information security manager should also consider a clean desk policy to prevent unauthorized access to sensitive information in less secure office areas.
- ❖ Some of the logistic issues that the information security manager needs to be able to manage include:
  - ✓ Cross-organizational strategic planning and execution
  - ✓ Project and task management
  - ✓ Coordination of committee meetings and activities
  - ✓ Development of schedules of regularly performed procedures.
  - ✓ Resource prioritization and workload management
  - ✓ Coordination of security resources and activities with larger projects and operations

## Business relationships for Security Program

➔ it is essential for an effective information security manager to maintain ongoing relationships with several other groups and departments in the organization such as: -

## Physical/Corporate Security

- ✓ These departments are typically managed by individuals from law enforcement and often have limited exposure to information security. In many small organizations, physical security is handled as a part of facilities management.

- ✓ It is essential for the information security manager to understand the physical security operation, including the relevant policies, standards, procedures, and practices, to avoid a situation where inadequate physical security undermines the information security program.

## IT Audit

- ✓ These auditors will have findings on information security based on what they consider good or acceptable practices. Depending on the expertise of the auditors, these findings may or may not agree with the information security manager’s perspective, and this underscores the necessity for complete governance documentation.
- ✓ It is essential for the information security manager to develop and maintain a good working relationship with internal audits. A good relationship with internal audit can also provide considerable support for achieving information security objectives.
- ✓ information security managers understand that audits are both an essential assurance process and a critical and influential ally in achieving good security governance and compliance. They can be instrumental in implementing security standards by providing feedback to senior management through audit findings that can serve to influence the tone at the top and create high-level support for security activities.
- ✓ In some cases, a deficiency identified by an auditor may not be applicable to the information security manager’s specific organization. If concerns are identified during an audit, the information security manager should work with the auditors to agree on associated risk, mitigating factors and satisfactory control objectives.

## IT Department

- ✓ An organization’s IT department has a critical role in information security program development and management. It is important for the information security manager to develop a strong working relationship with the IT department to foster rapport, trust, understanding of common goals and open communication.

## Business Unit Managers & Steering committee

- ✓ The information security manager should engage business unit management when developing the information security program and continue to develop those relationships in ongoing security management activities. This provides the basis for ensuring the ongoing alignment of information security with business objectives.
- ✓ It is important that the information security manager engages in the development process for any products or services related to the organization’s information resources—in other words, all such initiatives. The product development business unit should use an established baseline of standing security requirements (e.g., authentication controls, activity logging) for any new development project and work with the information security manager to develop additional controls to safeguard against application-specific risk.
- ✓ manager must understand the organization’s risk appetite and should refer to industry and regional sources to determine a baseline set of security functions appropriate to organizational policies and acceptable risk levels. They also must understand that there will always be trade-offs among security requirements, performance, costs, and other demands.

## Human Resources

- ✓ The information security manager must ensure that the HR and legal departments are intimately involved in any action involving monitoring of an employee's actions or suspected abuse of computing resources.

- ✓ A senior representative of the HR department should be assigned to the information security steering committee.

## Legal Department

- ✓ It is essential that the information security manager is in the loop to ensure the inclusion of adequate security considerations. The information security manager should liaise with a representative of the legal department, who should also be on security.
- ✓ Employees' first line of defense is the security of information. It is essential that appropriate security training on relevant policies, standards and applicable procedures is provided periodically or as needed.
- ✓ Employees should be trained to report potential threats and incidents and offer suggestions for improvement to the information security program, based on their day-to-day involvement with the program.
- ✓ Noncompliance issues may result in risk to the organization, so it is important to develop specific processes to deal with these issues in an effective and timely manner. A timetable is developed to document each noncompliance item and responsibility for addressing it is assigned and recorded. Regular follow-up is important to ensure that the noncompliance issue and other variances are satisfactorily addressed in a timely manner.

## Procurement

- ✓ Most organizations use a formal procurement process that can have consequences for information security in terms of product acquisitions. The information security manager must have a visibility for the process and be able to provide input into acquisition practices.

## Insurance

- ✓ It is incumbent on the information security manager to understand the kinds and extent of insurance the organization must include it in risk analysis and management and recovery planning because it serves as a compensating control.

## Third-party Management

- ✓ It is important that the information security manager understands what functions or services are provided by external parties and the associated risk.
- ✓ Managing risk to acceptable levels in these situations can pose a challenge and may require a variety of preventive, detective and compensatory controls including oversight and monitoring.
- ✓ Due diligence regarding placement of appropriate security language into contracts and agreements with third parties, as well as subsequent third-party performance against security requirements, must also take place.
- ✓ There must also be clear and tested escalation processes if things go wrong and, in all cases, strong authentication, authorization and network segmentation must be used to ensure that external parties have access to only what they need to meet their responsibilities.
- ✓ The fundamental purpose of contracts is two-fold: 1) to ensure that the parties to the agreement are aware of their responsibilities and rights within the relationship and 2) to provide the means to address disagreements once the contract is in force.
- ✓ Providing access to third parties must be based on clearly defined methods of access, access rights and level of functionality, and access must require the approval of the asset owner.
- ✓ Anomalies noticed should be immediately reported to the asset owner and escalation conditions specified wherever required. The access rights given to third parties should be removed immediately after the contract expires.

- ✓ Service provider architecture should be reviewed to ensure it supports the organization’s business requirements.

## Project Management Office

- ✓ It is important that the information security manager or representatives have an awareness of all projects, particularly IT projects, across the organization. Creating and maintaining a relationship with the PMO helps to ensure that the information security team will be able to review projects to provide insight into any potential risk and/or required security measures.

- ➔ An important part of program development is the review, modification and/or creation of policies required to establish a framework for the development of organizational standards with respect to security.
- ➔ Policy documents identify management intent and direction and form the basis for the organizational standards that comply with management and regulatory objectives for data confidentiality, integrity, and availability.

## Security Review

- ➔ a security review process like an audit. As with standard approaches to auditing
- ➔ While performing security reviews, an information security manager can gather data about not only policy and process at various levels of the organization, but also specific control weaknesses that may put information at risk. This data can be used to help prioritize program development efforts.
- ➔ The compliance gaps identified in the security reviews can be used to effect change, and an approach to monitor the organizational policy compliance strategy can be simultaneously developed.
- ➔ Security review steps

- **An objective**
  - is a statement of what is to be determined during a review.
- **A scope**
  - refers to the mapping of the objective to the aspect that is to be reviewed. Thus, the review objective dictates scope. If the scope is hard to describe, the review objective should be clarified to ensure that the result of the review will be well defined and actionable.
- **Constraints**
  - Constraints defined as the situation within which a reviewer operates that may impact aspects of conducting the review. It may or may not hinder his/her ability to review the entire scope and complete the review objective. In the example, a constraint may be a prohibition on accessing the application during business hours. An information security manager must evaluate his/her ability to fulfill the objective of the review in the context of constraints.
- **An approach**
  - Approach is a set of activities that cover the scope in a way that meets the objective of the review, given the constraints. There are usually alternative sets of activities that can cover the scope and objective.
- **A result**
  - The result is an assessment of whether the review objective was met. It is an answer to the question, “Is this secure?” If it is not possible to answer the question with any level of assurance, the review should be declared incomplete.

➔ With this information in hand, the information security manager may craft one or more potential solutions that fit the organization's operational, financial, and technical environment. Any combination of mitigating or compensating controls that enforce the agreed-on control objectives should satisfy the issue.

➔ Although information security spans technical, operational, and managerial domains, a sizable portion of the actual implementation of the information security program is likely to be technical.

➔ Regardless of operating level, all information systems managers should have a thorough understanding of security architecture, control implementation principles, and commonly implemented security processes and mechanisms.

➔ Highly integrated and tightly coupled systems, such as enterprise resource planning (ERP) implementations, can create an additional challenge; the entire system must be considered from a security perspective because compromise of one element can disrupt the operations of the entire enterprise. It is important that the information security manager understands and plans for the potential domino effect of cascading risk.

➔ Due diligence is a term related to the notion of the "standard of due care." It is the idea that there are steps that should be taken by a reasonable person of similar competency in similar circumstances.

➔ When a reasonable security program is in place. Following should be observed in the organization:

✓ Senior management support
✓ Comprehensive policies, standards, and procedures
✓ Appropriate security education, training, and awareness throughout the organization
✓ Periodic risk assessments
✓ Effective backup and recovery processes
✓ Implementation of adequate security controls

- ✓ Effective monitoring and metrics of the security program
- ✓ Effective compliance efforts
- ✓ Tested business continuity and disaster recovery plans.
- ✓ Protection of data (in transit and at rest)

## Threat Assessment

- ➔ Technical and behavioral threats to an organization evolve because of internal and external factors. Implementation of modern technologies, granting broader network and application access to partners and customers, and the ever-growing capabilities of attackers warrant periodic reassessment of the threat landscape an organization faces.
- ➔ The information security manager should perform this analysis at least annually by evaluating changes in the technical and operating environments of the organization, particularly where external entities are granted access to organizational resources. Internal factors such as new business units, new or upgraded technologies, changes to products and services, and changes in roles and responsibilities represent areas where the level of threat may increase, or new threats may emerge.
- ➔ Risk assessment is used to identify, analyze, and evaluate risk; the probability of compromise; and its potential impact on an organization in quantitative or qualitative terms. types of residual risk might be low, collectively, they can be disastrous.
- ➔ A BIA is an exercise that determines the impact of losing the availability of any resource to an organization; it establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and supporting systems.
- ➔ A business resource dependency assessment is based on determining the various applications and infrastructure used by a business for

day-to-day operations. It does not capture the financial and operational impact of potential disruptions and does not replace a BIA. If resources or other constraints do not allow for comprehensive BIAs, a business resource dependency assessment is a less expensive alternative to provide the basis for allocating available resources based on the criticality of the function.

## Cloud Computing

### Characteristics of the cloud

- ✓ On-demand self-service—Computing capabilities can be provisioned without human interaction from the service provider.
- ✓ Broad network access—Computing capabilities are available over the network and can be accessed by diverse client platforms.
- ✓ Resource pooling—Computer resources are pooled to support a multitenant model.
- ✓ Elasticity—Resources can scale up or down rapidly and, in some cases, automatically, in response to business demands.
- ✓ Measured service—Resource utilization can be optimized by leveraging charge-per-use capabilities.

## Cloud services

### SECaaS

- ✓ The cloud service provider (CSP) provides stand-alone managed security services ranging from antivirus scanning and mail security to full deployment of end-point security.
- ✓ The CSP offloads appliance utilization for the client, and CPU-and memory intensive activities are moved to cloud services. For example, antivirus activities on unified threat management (UTM) devices are often offloaded to a SecaaS provider to reduce the number of chassis at the client site. The advantage to clients is minimized risk when applying patches or updates, because they are no longer linked to the device.

## DRaaS

- ✓ disaster recovery as a service (DRaaS), the CSP offers its cloud infrastructure to provide an enterprise with a disaster recovery (DR) solution. In most cases, the CSP not only provides backup equipment and storage, but also provides services for a BCP if it is not yet available.

## IDaaS

Identity as a service (IDaaS) is a new cloud service and currently has two interpretations:

- ✓ The management of identities in the cloud that is separated from the users and applications that use the identities. This can be either managed identity services, including provisioning, or management for both onsite and offsite services. Delivering a single sign-on (SSO) solution can also be part of the cloud service offering.
- ✓ The delivery of an identity and access management (IAM) solution. IDaaS is often a hybrid solution where access and roles are configured by the CSP, and users are authorized by enterprise internal solutions. This is known as a federated model.

## IaaS

- ✓ Information as a service (IaaS) builds on the big data concept—rather than providing the raw data or the algorithms that are used for trending, IaaS provides the required information. With this new service, the result of a query is more important than the query itself.

## IPaaS

- ✓ Integration platform as a service (IPaaS), also called “cloud integrator” by some, is defined by Gartner as “a suite of cloud services enabling development, execution and governance of integration flows connecting any combination of on premises and cloud-based processes, services, applications and data within individual or across multiple organizations."

## Forensics as a service (FRaaS)

- ✓ establishes a cloud forensic investigative process, which can be implemented within a cloud ecosystem, integrated with tolls that should ensure relevant information gathered, verified, and stored in a manner that is forensically sound and legally defensible."

- ➔ Cloud access security brokers (CASBs) are control points located between the consumer and service provider and primarily serve to enforce the consumer's policies. These may include authentication, authorization, SSO, tokenization, logging, notification and alerts, malware detection and prevention, and others depending on the vendor. It is likely that CASBs will see substantial adoption in the coming years because they offload several security issues and simplify security for cloud-based services.

## Controls and countermeasures

## Control practices.

- ➔ There are two categories of controls, general and application-level, application level is specific and should be used when general control is not sufficient.
- ➔ Some common control practices that make it hard for users to bypass controls are mechanisms that embody these principles:

- ✓ Access Control, has two sub-options to design: -
    - ▪ MAC refers to a means of restricting access to data based on security requirements for information contained in the data and the corresponding security clearance of users. MAC is typically used for military applications where, for example, a secret clearance is required to access data classified as "secret."

  - DAC refers to means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that rules may allow a subject with certain access permission to pass that permission on to another subject DAC present administrative overhead because it is based on everyone rather than group of individuals.
  - RBAC Role based access control, rely on groups, much simpler in administration.

- ✓ Secure failure— Secure failure as a control policy must be carefully considered because it affects availability. consider here fail-open or fail-close.
- ✓ Principle of least privilege— Compartmentalize to minimize damage— capacity of system architecture to contain access to subsets of system resources by requiring a separate set of authorization controls per subset.
- ✓ Segregation of duties (SoD) two persons do the task not only one person can request and approve or approve and implement.
- ✓ Transparency—This refers to the ability of the average layperson to understand how system security is supposed to work so that all stakeholders can easily see what effect their activities have on systems security.
- ✓ Trust—This refers to a design strategy that includes the existence of a security mechanism whereby the identity of a user can be determined by its relationship to an identity provider that is trusted by a relying party. A typical application is the use of a trusted third party in PKI architecture known as the certificate authority (CA), which attests to the identity of an entity by issuing a certificate.
- ✓ Trust no one—This refers to a design strategy that includes oversight controls, like CCTV in all offices.

Disclaimer: Use for review after studying our CISM Course – https://cyvitrix.com

REACH OUT cyvitrix@gmail.com for any requests.

## Security Controls

➔ control objectives must be based on individual organizational objectives and risk appetite and tolerance tailored to achieve the desired outcomes.

➔ Security controls encompass the use of technical and nontechnical methods. These include administrative, technical, and physical controls.

➔ The strength of a control can be measured in terms of its inherent design, strength, and the likelihood of its effectiveness. An example of an inherently strong control is balancing the books to account for all cash and/or segregating accounting responsibilities among multiple employees. An example of an inherently strong control by design is requiring dual control to access sensitive areas or materials.

➔ The following factors should be considered in recommending controls and alternative solutions to reduce identified risk to acceptable levels:

- Effectiveness of recommended options
- Compatibility with other impacted systems, processes, and controls
- Relevant legislation and regulation
- Organizational policy and standards
- Organizational structure and culture
- Operational impact
- Safety and reliability
- A cost-benefit analysis should be conducted for the proposed controls to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk or impact.

➔ When performing TCO calculation it is important to include:

- Costs to administer controls.

- Training costs
- Maintenance costs
- Monitoring costs
- Update fees.
- Consultant or help desk fees.
- Fees associated with other interrelated systems may have been modified to accommodate security objectives.

## Countermeasures

➔ the information security manager may occasionally require a control against a specific threat. Such a control is called a countermeasure. Countermeasures often provide specific protection, making them more effective, but less efficient, they may be preventive, detective or corrective, or any combination of the three. Countermeasures can be nontechnical as well, such as offering a reward for information leading to the arrest of hackers. Their deployment should commence only with clear justification and due caution, and only when an existing or more general control cannot adequately mitigate the threat.

## Technological controls (Technical)

➔ Technologies typically fall under one of three distinct categories in terms of the type of controls that are available: native, supplemental and support control technologies.

✓ Native control technologies are out-of-the-box security features that are integrated with business information systems. For example, most web servers include functions providing authentication capabilities, access logging and SSL transport encryption. All these controls would be considered native to the web server technology.

✓ Supplemental control technologies are usually components that are added on to an information systems environment.

  - ▪ They often provide some function that is not available from native components (e.g., network intrusion detection), Supplemental control technologies tend to be more specialized than native control technologies and, therefore, they are often operated by security specialists.
  - ▪ In some cases, it may be appropriate to share responsibility for a particular supplemental control technology, particularly if it is deeply embedded in both the security and business application domains.
  - ▪ Typical supplemental control technologies include Federated identity management systems, SSO, IPSs, Firewalls

✓ Support control technologies serve to automate a security-related procedure, provide management information processing, or otherwise increase management efficiency or capabilities.

  - ▪ support security operations are commonly implemented and operated by the information security group in relative independence from the IT department.
  - ▪ Some of the most common supporting technologies include: SIEM systems, Compliance monitoring and management tools, Access management workflow systems, Vulnerability scanning tools, Security configuration monitoring tools, Policy management and distribution systems.

## Software development process

➔ Defined baseline security controls should be a standing requirement for all new systems development. Baseline security requirements should be defined and documented; baseline define the minimum-security requirements.

➔ Adequate traceability of the security requirements should be ensured and supported across the distinct phases of the life cycle.

- ➔ During the quality and acceptance phases, the information security manager should coordinate testing of originally established functional security requirements in addition to testing system interfaces for vulnerabilities.
- ➔ The information security manager should ensure that appropriate segregation of duties is considered throughout the SDLC. Testing and QA plans must also be subject to review by the information security manager to ensure that the security elements are properly tested and certified.
- ➔ It may be necessary to perform a code review in addition to the QA testing process to ensure there are no unexpected vulnerabilities. Code reviews are often outsourced for an independent review.

## Security Program metrics

- ➔ Effective management requires effective metrics and monitoring.
- ➔ When analyzing technical security architecture, the information security manager should use a clearly defined set of measurable criteria to enable tracking of performance metrics. A common approach to the development of metrics is to pose questions that need to be answered and then develop methods to provide answers.
- ➔ measurements without a reference in the form of objectives or goals are not metrics and not likely to be useful Metrics need to provide information at one or more of the following three levels:

- ✓ Strategic metrics are often a compilation of other management metrics designed to indicate that the security program is on track, on target and on budget to achieve the desired outcomes.
- ✓ Management (or tactical) metrics are those needed to manage the security program such as the level of policy and standards compliance, incident management and response effectiveness, and workforce and resource utilization.

✓ Operational metrics are the more common technical and procedural metrics such as open vulnerabilities and patch management status.

---

- Security standards must be explicitly approved by Information security management.
- The primary objective of information security awareness is to influence employee behavior.
- Architecture helps to manage complexity.
- In Pretty good privacy “PGP,” no CA is needed as client attest each other’s identity.
- The goal of the information security program is to implement strategy.
- Awareness program should be customized, its goal is to reduce the threat likelihood. Awareness also can be performed to some influencers and make them your program ambassadors.
- Periodic awareness is needed as threats and vulnerabilities change. Training comes first then reward and disciplinary actions. Active awareness influences the residual risk by lowering the possible vulnerabilities.
- Gaining senior management support can be secured through good relations with business.
- CA Private key is considered as the Single point of failure for PKI.
- The registration authority private key is the weakest link in the PKI as it is usually stored on a device or smartcard with password protection.
- System owner is the best to implement and maintain security controls, security manager approves standards.
- The steering committee is the best advocate for security program.

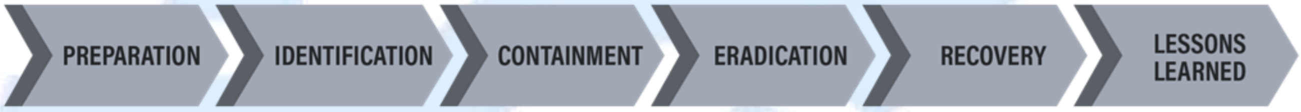
- Native database auditing could affect database performance. The top concern when selecting monitoring or auditing software is the possible overhead on monitored services.
- Security review is equal to risk assessment after gaining top management support, also program comes after strategy.
- Program oversight mechanism maintains the currency and coverage of information security program.
- Ultimate responsibility is always with top management.
- Metrics are to set during the design phase.
- In database, application-level encryption encrypts data stored on database, make it only readable by the application.
- The right to audit is the best guarantee for third party compliance, and the independent security review.
- The top-down approach also refers to top management support.
- XSRF CSF is using cookies as the sole authentication mechanism.
- Blackbox more time in discovery, white box more time in exploitation
- The percentage of controls objective achieve is an indication of effectiveness.
- Information security is important, but keeping business is Important too.
- Metrics should be developed based on security objectives.
- The most effective password protection mechanism is encryption.
- Stakeholders sign-off on policies must be obtained first prior communicating or enforcing it.
- Digital certificate should be managed by independent third party (certificate authority)

- Intranet server should be placed at the internal network, while extranet in DMZ “or screened subnet.”
- DMZ is the top control to prevent external users from attacking internal resources.
- Key benefit of VDI from security perspective is VDI separate personal and business data, user can use his own laptop “which contains personal data” to access corporate workspace using application “isolated” and perform his job without being able to move data between the two systems.
- The key risk of data encryption is the keys used in encryption fall with wrong hand, key management is the weakest link in encryption process.
- MITM is not only using mac address, but also DNS or NETBIOS, hence Static mac is not the only solution. IPv6 IPSEC prevents such attacks completely by including source/destination IP address.
- Encryption/VPN is the best way to assure confidentiality, while digital signature to ensure non-repudiation, hashing to ensure integrity.
- Rather than disable USB ports “as it may be used by mouse or other peripherals, restrict the available drive allocation.
- Emergency change can bypass scheduling, but it is still documented, authorized, and tested.
- Business case -> RFP -> Project budget development -> management approval
- Metrics support steady improvement.
- Access control matrix is the best way to assure BU adheres to data access requirement.
- Skill inventory is the best to use to define the current skills available for security programs, and plan for training to preserve the needed skills.

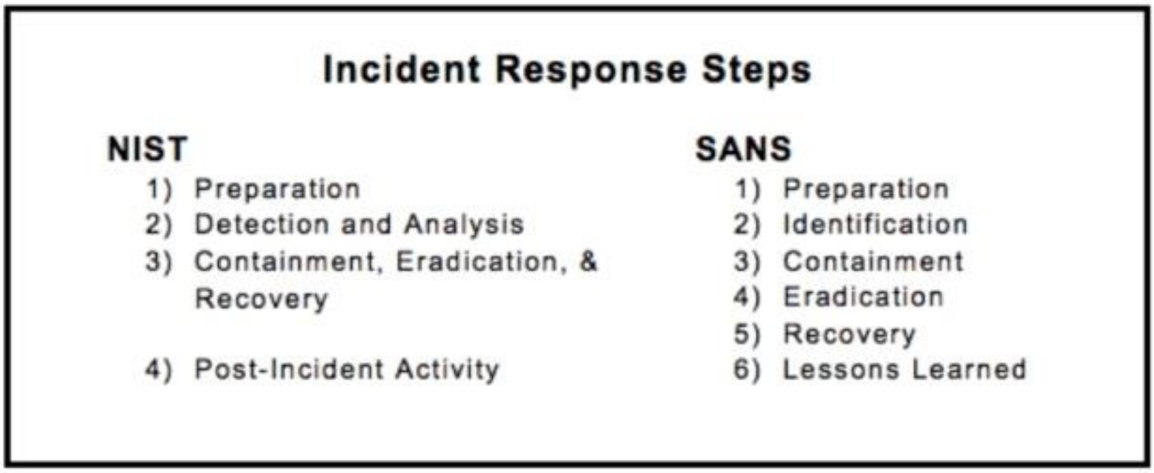
- Firewall should be placed between you and internet, IDS should be placed between firewall and internal LAN or at DMZ, the reason why for this is that most of threats can be stopped by firewall.
- Control failure policies are either fail-close or fail-open, for fail-open controls, a layered control is needed.
- REVISE THE PROCESS OF RFP AND procurement.
- BSC assesses whether the objective is met or not, while gap analysis provides comparison between both current and desired state.

# Domain 4: Incident Management

- ➔ Event is change in state, when it incurs disruption, the event became incident.
- ➔ Incident management is a component of risk management that can provide an optimal balance between prevention, containment, and restoration.
- ➔ Incident management involves all the actions taken prior to (including testing and planning), during and after an information security incident occurs.



- ✓ In the preparation stage for example, a proactive evaluation is invoked to test systems and plan for proper controls to them.
- ✓ Incident response steps may vary from vendor to vendor but include the same general outlines.



**Incident Response Steps**

**NIST**

1) Preparation
2) Detection and Analysis
3) Containment, Eradication, & Recovery
4) Post-Incident Activity

**SANS**

1) Preparation
2) Identification
3) Containment
4) Eradication
5) Recovery
6) Lessons Learned

- ➔ The purpose of incident management is to identify and respond to unexpected disruptive events with the objective of controlling impacts within acceptable levels.

- ➔ risk assessments and business impact analyses (BIAs) form the basis for determining the priority of resource protection and response activities.
- ➔ The objective of incident management is to prevent incidents from becoming problems and problems from becoming disasters.
- ➔ The goals of incident management and response activities can be summarized as the following:

- ✓ Detect incidents quickly.
- ✓ Diagnose incidents accurately.
- ✓ Contain and minimize damage.
- ✓ Restore affected services.
- ✓ Determine root causes.
- ✓ Implement improvements to prevent recurrence.
- ✓ Document and report.

- ➔ It is critical to achieve stakeholder consensus and senior management support for an effective incident management capability.
- ➔ Severity criteria should be consistent, concisely described, and easy to understand so severity levels of similar events are uniformly determined.
- ➔ Personnel must be trained to recognize potential incidents and provide proper classification, and they must be trained in notification, reporting and escalation requirements.

## Incident Management

- ➔ necessity of effective incident management includes:

- ✓ The trend of both increased occurrences and escalating losses resulting from information security incidents
- ✓ The increase of vulnerabilities in software or systems affecting large parts of an organization’s infrastructure and impact operations
- ✓ Failure of security controls to prevent incidents.

Disclaimer: Use for review after studying our CISM Course – https://cyvitrix.com

REACH OUT cyvitrix@gmail.com for any requests.

- ✓ Legal and regulatory mandates requiring the development of incident management capability.
- ✓ The growing sophistication and capabilities of profit-oriented and nation-state attackers
- ✓ Advanced persistent threats (APT)
- ✓ Increasing zero-day attacks

## Outcomes of Incident Management

include the following:

- ➔ The organization can deal effectively with unanticipated events that might threaten to disrupt the business.
- ➔ The organization will have sufficient detection and monitoring capabilities to ensure that incidents are detected in a timely manner.
- ➔ Well-defined severity and declaration criteria will be in place, as will defined escalation and notification processes.
- ➔ Personnel will be trained in the recognition of incidents, the application of severity criteria, and proper reporting and escalation procedures.
- ➔ The organization will have response capabilities that demonstrably support the business strategy by being responsive to the criticality and sensitivity of the resources protected.
- ➔ The organization will serve to proactively manage the risk of incidents appropriately in a cost-effective manner and will provide integration of security-related organizational functions to maximize effectiveness.
- ➔ The organization will provide monitoring and metrics to gauge performance of incident management and response capabilities, and it will periodically test its capabilities and ensure that information and plans are updated regularly, current, and accessible when needed. These monitoring and metrics activities will ensure that:

- ✓ Information assets are adequately protected, and the risk level is within acceptable limits.
- ✓ Professionally trained and equipped incident management and response teams are in place.
- ✓ Effective IRPs are in place and understood by relevant stakeholders (e.g., management, IT departments, end users, incident handlers).
- ✓ Incidents are quickly identified, categorized correctly, and contained, and the root cause is addressed to allow recovery within an acceptable interruption window (AIW).
- ✓ Communication flows to different stakeholders and external parties are well controlled, as documented in the communication plan.
- ✓ Lessons learned are documented and shared with stakeholders to increase the level of security awareness and serve as a basis for improvement.
- ✓ Assurance is provided to internal and external stakeholders (e.g., customers, suppliers, business partners) that the organization has adequate control and is prepared to ensure business survivability in the long term.

## The Role of The Information Security Manager in Incident Management

- ➔ The information security manager has, at a minimum, responsibility as first responder to information-security-related incidents.
- ➔ It is important for the information security manager to have a good conceptual and practical understanding of what is required to adequately address those responsibilities. In addition, there must be a good understanding of the BC and DR processes.

## Incident Response Concepts

- ➔ Incident handling is a service that involves all the processes or tasks associated with handling events and incidents. It involves multiple functions:

- ✓ Detection and reporting—The ability to receive and review event information, incident reports and alerts.
- ✓ Triage—The action taken to categorize, prioritize and assign events and incidents to maximize the effectiveness of limited resources.
- ✓ Analysis—The attempt to determine what has happened, the impact and threat, the damage that has resulted, and the recovery or mitigation steps that should be followed.
- ✓ Incident response—The action taken to resolve or mitigate an incident, coordinate, and disseminate information, and implement follow-up strategies to prevent recurring incidents Effective incident management ensures that incidents are detected, recorded, and managed to limit impacts.

- ➔ Recording is also required to properly document information that potentially includes forensics data that can be used to pursue disciplinary or legal options.
- ➔ Incident management includes initial support processes that allow new incidents to be checked against known errors and problems so that any previously identified workarounds can be quickly identified.
- ➔ Incident response is the last step in an incident-handling process that encompasses the planning, coordination and execution of appropriate mitigation, containment, and recovery strategies and actions.
- ➔ The information security manager also must be aware of the possibility of nontechnical incidents that must be planned for and addressed. These incidents can include social engineering, lost or stolen backup tapes or laptop computers, physical theft of sensitive materials, and natural disasters.

## Incident Management Systems

- ➔ These systems automate many manual processes that provide filtered information that can identify possible technical incidents and alert the incident management team (IMT).
- ➔ An example of a centralized incident management system is a security information and event manager (SIEM). This tool is an automated log reader that combines critical events and logs from many different systems and devices and correlates them into more meaningful incident information. An effective SIEM will:

- ✓ Consolidate and correlate inputs from multiple systems.
- ✓ Identify incidents or potential incidents.
- ✓ Notify staff.
- ✓ 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.

- ➔ There are potential efficiencies and cost savings that can be realized using automated incident management systems once they are properly configured. Some considerations for the information security manager can include:

- ✓ Operating costs—In the absence of an automated and centralized incident management system, information security staff may be required to monitor different security devices, correlate events, and process the information manually.
- ✓ Recovery costs—An automated system, when configured properly, can detect and escalate incidents significantly faster than when a manual process is used. The amount of damage can be controlled, and further damage prevented when the recovery actions are initiated earlier rather than later.

## Incident Management Organization

- ➔ The incident management capability in an organization acts as the first responder for a variety of incidents, including information processing and processes. It responds to and manages incidents to contain and minimize damage, limit disruptions to business processes, and restore operations as quickly as possible.
- ➔ Incident management is, nominally, a component of risk management and can be considered the operational and reactive element.
- ➔ The information security manager should understand the various activities involved in a response and recovery program. This includes meeting with emergency management officials (e.g., federal, state/provincial, municipal/local) to understand what governmental capabilities are available.
- ➔ Emergency management activities also include measures to assure the safety of personnel, such as evacuation plans and creation of a command center from which emergency procedures can be executed. It also is important that information about an incident be communicated only on a need-to-know basis to control exposure of potentially sensitive information.

## Responsibilities

- ➔ responsibilities that the information security manager must undertake, including:

- ✓ Developing information security incident management and response plans
- ✓ Handling and coordinating information security incident response activities effectively and efficiently.
- ✓ Validating, verifying, and reporting protective or countermeasure solutions, both technical and administrative

- ✓ Planning, budgeting, and program development for all matters related to information security incident management and response.

➔ The approach to incident response varies depending on the situation and types of events that may occur, but the goals are constant and include:

- ✓ Maintaining incident response readiness
- ✓ Containing and minimizing the effects of the incident so 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

## Senior Management Commitment

➔ senior management commitment is critical to the success of incident management and response A business case can show that, under many circumstances, effective incident management and response may be a less costly option than attempting to implement controls for all conditions.

## Incident Management Resources

## Policies and Standards

➔ standards and procedures are important to:

- ✓ Ensure that incident management activities are aligned with the IMT mission.
- ✓ Set correct expectations.
- ✓ Provide guidance for operational needs.
- ✓ Maintain consistency and reliability of services.

- ✓ Clearly understand roles and responsibilities
- ✓ Set requirements for identified alternate personnel for all essential functions.

## Personnel

- ➔ The information security manager usually leads the team. In larger organizations, it may be more effective to appoint a separate IRT leader/manager who focuses on responding to incidents.
- ➔ a security steering group (SSG), function is responsible for approving the charter and serves as an escalation point for the IMT. The SSG also approves deviations and exceptions to normal practice.
- ➔ Incident Response Team Organization

- ✓ Central IRT—A single IRT handles all incidents for the organization, typically used in a small organization or one that is centrally located.
- ✓ Distributed IRT—Each of several teams is responsible for a logical or physical segment of the infrastructure, usually of a large organization or one that is geographically dispersed.
- ✓ Coordinating IRT—The central team may provide guidance to distribute IRTs, develop policies and standards, provide training, conduct exercises, and coordinate or support response to specific incidents. Distributed teams manage and implement incident response.
- ✓ Outsourced IRT—Successful IRTs may be comprised entirely of employees of the organization or may be fully or partially outsourced. Permanent team members may include incident handlers, investigators and forensics experts, and IT and physical security specialists.
- ✓ Virtual team members normally consist of business representatives (e.g., middle management), legal staff, communications staff (e.g., PR), HR staff, other security groups (e.g., physical security), risk management and IT specialists.

## Roles and Responsibilities

➔ Security steering group Highest structure of an organization’s functions related to information security.

- ✓ Takes responsibility for overall incident management and response concept.
- ✓ Approves IMT charter.
- ✓ Approves exceptions/deviations.
- ✓ makes final decisions.

➔ Information security manager IMT leader and main interface to SSG

- ✓ Develops and maintains incident management and response capability.
- ✓ Effectively manages risk and incidents.
- ✓ Performs proactive and reactive measures to control information risk level.

➔ Incident response manager IRT leader

- ✓ Supervises incident response tasks.
- ✓ Coordinates resources to effectively perform incident response tasks.
- ✓ Takes responsibility for successful execution of IRP.
- ✓ resents incident response report and lessons learned to SSG members.

➔ Incident handler IMT/IRT team member

Performs incident response tasks to contain exposures from an incident.

- ✓ Documents steps taken when executing the IRP.
- ✓ Maintains chain of custody and observes incident handling procedures for court purposes.
- ✓ rites incident response report and lessons learned.

➔ Investigator IMT/IRT team member

- ✓ Performs investigative tasks for a specific incident.
- ✓ Finds root cause of an incident.
- ✓ Authors report of investigation findings

➔ IT security specialist IMT/IRT team member; subject matter expert in IT security

- ✓ Performs complex and in-depth IT security-related tasks as part of the IRP.
- ✓ Performs IT security assessment/audit as initiative-taking measure and part of vulnerability management (i.e., performing routine vulnerability scans and associated remediation)

➔ Business managers Business function owners; information assets/system owners

- ✓ Make decisions on matters related to information assets/systems when an incident happens, based on IMT/IRT recommendations.

➔ IT specialists/representatives Subject matter experts in IT services

- ✓ Provide support to IMT/IRT when resolving an incident.
- ✓ Maintain information systems in a good condition per company policy and good practices.

➔ Legal representative Subject matter expert in legal

- ✓ Ensures that incident response actions and procedures comply with legal and regulatory requirements.
- ✓ Acts as the liaison to law enforcement and outside agencies.

➔ HR Subject matter expert in HR area

- ✓ Helps in incident management/response when there is a need to investigate an employee suspected of causing an incident.

- ✓ Integrates HR policy to support incident management/response (sanctions to employees found to violate acceptable use of policy o involved in an incident)

➔ PR representative Subject matter expert in PR area

- ✓ Provides controlled communication to internal and external stakeholders to minimize any adverse impact to ongoing incident response activities and protect an organization's brand and reputation.
- ✓ Helps IMT/IRT in communication issues, thus relieving the team to work on critical issues on resolving an incident.

➔ Risk management specialist Subject matter expert in risk Management.

- ✓ Works closely with business managers and senior management to determine and manage risk.
- ✓ Provides input (e.g., BIA, risk management strategy) to incident management.

➔ Physical security/facilities Manager

- ✓ Knowledgeable about physical plant and emergency capabilities
- ✓ Responsible for physical plant and facilities
- ✓ Ensures physical security during incidents.

## Skills

➔ Communication—The ability to communicate effectively is a critical component of the skills needed by IRTs. They need to be good listeners, understanding what is said (or not said), to enable them to gain details about an incident that is being reported.

➔ Leadership skills—Members of an IRT are often faced with directing and getting support of other members of the organization, so leadership is an important attribute.

- ➔Presentation skills—An IRT's skills are needed for technical presentations, management or sponsor briefings, a panel discussion at a conference, or some other form of public speaking engagement. The specialist member's skills might extend to providing expert testimony in legal or other proceedings on behalf of the team or users.
- ➔Ability to follow policies and procedures—Team members need the ability to follow and support the established policies and procedures for incident response management.
- ➔Team skills—IRT members must have the ability to work in a team environment, as productive and cordial collaborators; be aware of responsibilities; contribute to the goals of the team; and work together to share information, workload, and experiences.
- ➔Integrity—Team members often deal with information that is sensitive and, occasionally, they may have access to information that is newsworthy.
- ➔Self-understanding—Team members must be able to recognize their limitations and actively seek support from their team members, other experts, or management.
- ➔Coping with stress—The IRT is likely to face stressful situations. The members need to be able to recognize when they are becoming stressed, be willing to make their fellow team members aware of the situation and take the necessary steps to control and maintain their composure.
- ➔Problem solving—Without good critical thinking skills, team members could become overwhelmed with the volumes of data related to incidents and other tasks that need to be handled. Critical thinking skills also include an ability to think freely or look at issues from multiple perspectives to identify relevant information or data.
- ➔Time management—Team members might be confronted with a multitude of tasks, ranging from analyzing, coordinating, and

responding to incidents, to performing duties such as prioritizing their workload, attending and/or preparing for meetings, completing time sheets, collecting statistics, conducting research, giving briefings and presentations, traveling to conferences, providing onsite technical support, and prioritizing tasks. Team members must be able to balance efforts between completing the tasks and recognizing when to seek help or guidance.

## Awareness and Education

- ➔ Periodically, a skills assessment is useful to determine whether the required expertise is available in the organization for the IRT. If an organization is unable to find internal experts or hire/train staff to provide the necessary incident response specialist skills, the organization may be able to develop relationships with experts in the field to provide the necessary skills.

## Audits

- ➔ Internal and external audits are performed to verify compliance with policies, standards and procedures defined for an organization. Audits can also provide an objective.
- ➔ view of the overall completeness and functionality of the incident management and response plans and provide assurance that major gaps in the processes do not exist.

## Outsourced Security Providers

- ➔ Outsourcing incident management capability may be a cost-effective option especially for smaller organizations even if components of incident management are outsourced. It will be essential to clearly understand the outsourcer's capabilities, response times, etc., and develop proper SLAs containing appropriate indemnity clauses.
- ➔ The information security manager should consider the following when security functions are fully or partially outsourced:

- ✓ Matching the organization's incident reference numbers with the vendors for each applicable incident: This ensures a mutual understanding of incident details between organizations. This also helps to identify the actual organizational recovery time.
- ✓ Integration of the organization's change management functions with the vendor's (to the extent possible): Depending on the nature of the service provided, the organization's change management functions may be linked via leaders on the change advisory board or have a platform where the security group can view the vendor's changes and follow-up with key points of contact from the vendor.
- ✓ Requirement from the vendor for periodic review of incidents that occur on a regular basis (e.g., monthly, annually): Page 512 Follow-up items are taken from these meetings to help prevent incidents from recurring.

## Incident Management Objectives

- ➔ Handle incidents when they occur so the exposure can be contained or eradicated to enable recovery within the recovery time objectives (RTOs)
- ➔ Restore systems to normal operations.
- ➔ Prevent previous incidents from recurring by documenting and learning from past incidents.
- ➔ Deploy proactive countermeasures to prevent/minimize the probability of incidents taking place.

## Strategic Alignment

- ➔ Constituency—To whom does the IMT provide services? It is important to know who the stakeholders are for this function and identify their expectations and information needs. Financial institutions may be bound by Basel III or another regulation. Thus, the IMT should meet certain performance and reporting requirements.

- ➔Mission—The mission defines the purpose of the team and the primary objectives and goals that are provided by IMT.
- ➔Services—Services provided by IMT should be clearly defined to manage stakeholder expectations.
- ➔Organizational structure—The structure of the IMT should effectively support the organization's structure. The best structure would provide the business with the maximum availability of IMT services on the most cost-effective basis.
- ➔Resources—Sufficient staffing is needed to be effective. Because incident management covers a wide range of services, most of the time it is not possible to have all the resources available within one IMT. One way to solve this issue is to establish virtual team members and/or complement the team with external resources.
- ➔Funding—The IMT usually consists of highly specialized members. The equipment they use while providing services may also be specialized, requiring greater capital expenditures. In view of this, sufficient funding is required to ensure the continuity of critical incident response services.
- ➔Management buy-in—Senior management buy-in is essential for establishing and supporting the incident management function. The lack of buy-in normally results in suboptimal IMT performance because there may be significant limitation in budgets or the availability of suitable personnel.

## Risk Management

- ➔Any risk that materializes that is not prevented by the organization's internal controls constitutes an incident that must be managed and responded to with the intent that it does not escalate into a disaster.

## Assurance Process Integration

- ➔It is important to ensure incident management and recovery plans actively incorporate and integrate those functions where required.

Disclaimer: Use for review after studying our CISM Course – https://cyvitrix.com

An effective outcome is a set of plans that defines which departments are involved in various incident management and response activities and specifies that those linkages have been tested under realistic conditions.

## Value Delivery

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

- ➔ Incident management and response activities consume resources that must be managed to achieve optimal effectiveness. This is accomplished by ensuring appropriate oversight, monitoring of resources and regular reporting.

## Incident Management Metrics and Indicators

- ➔ Metrics based on key performance indicators (KPIs) and program goals (KGIs) established for incident management should be presented to senior management as a basis of justification for continuous support and funding. It enables senior management to understand the incident management capability of the organization and areas of risk that need to be addressed.
- ➔ KPIs are a quantifiable activity measure (e.g., the number of incidents per year resolved within two minutes of occurrence). KGIs are either

quantitative or qualitative, depending on the situation, and are intended to show progress toward or relating to a predefined goal.

- ✓ Common criteria that are used as part of incident management metrics may include:
- ✓ Total number of reported incidents
- ✓ Total number of detected incidents
- ✓ Number of days without incident
- ✓ Average time to respond to an incident relative to the RTO.
- ✓ Average time to resolve an incident.
- ✓ Total number of incidents successfully resolved.
- ✓ Incidents have not been resolved successfully.
- ✓ Proactive and preventive measures taken.
- ✓ Total number of employees receiving security awareness training
- ✓ Total damage from reported and detected incidents if incident response was not effective or not performed.
- ✓ Total savings from potential damages from incidents resolved.
- ✓ Total labor responding to incidents.
- ✓ Detection and notification times

## Defining Incident Management Procedures

➔ Prepare/improve/sustain (prepare)—This process defines all preparation work that must be completed prior to having any capability to respond to incidents. It contains subprocesses to evaluate incident-handling capability and postmortem review of incidents for improvements. Subprocesses include:

- ✓ Coordinate 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 defined resources.
  - . Evaluate incident management capability.
  - . Conduct postmortem review.
  - . Determine incident management process changes.
  - . Implement incident management process changes.
- ✓ Protect infrastructure (protect)—The protect process aims to protect and secure critical data and computing infrastructure and its constituency when responding to incidents. It also proposes improvement on a predetermined schedule while keeping the appropriate security context in consideration. Subprocesses include:
  - Implement changes to computing infrastructure to mitigate ongoing or potential incidents.
  - Implement 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 (detect)—The detect process identifies unusual/suspicious activity that might compromise critical business functions or infrastructure. Subprocesses include:
  - Proactive detection—The detection process is conducted regularly prior to an incident. The IMT monitors various information from online/periodic vulnerability scanning, network monitoring, antivirus and personal security system

alerts, commercial vulnerability alert services, risk analysis, and security audit/assessment.

- Reactive detection—The detection process is conducted when there are reports from system users or other organizations. Users may notice unusual or suspicious activity and report it to the IMT. It is also possible that another organization's IMT will provide advisories when its system has received malicious activity from your organization.
- For the IMT to receive the report promptly, there should be multiple communication channels from end users to the IMT. This can be in the form of phone calls, faxes, email messages, web-form reporting and automated intrusion detection systems (IDSs).

✓ Triage events (triage)—Triage is a process of sorting, categorizing, correlating, prioritizing, and assigning incoming reports/events into (typically) three categories: the problems that cannot be readily resolved, those that can wait and those that can be efficiently addressed with the resources available. When there are multiple incident reports coming into the IMT, triage allows events to be prioritized appropriately, thus maximizing response effectiveness. It can also serve as a single point of entry for any IMT communication and information. Triage prioritization can be done at two levels: Tactical Based on a set of criteria Strategic Based on the impact of business Subprocesses include:

- . Categorization—This is the use of predetermined criteria to classify all incoming reports/events.
- . Correlation—This subprocess correlates a report/event with other relevant information. A higher correlation of a

report/event provides more information that is useful for the IMT to decide on the appropriate response.

- . Prioritization—In an ideal world, every undesirable event is followed up.
- as soon as possible. However, resources are limited, and it may not always be possible. To ensure minimal impact to critical business functions or information assets, incidents are usually prioritized based on their potential impact rather than a specific set of criteria.
- . Assignment—When an incident or potential incident has been identified, it is assigned to the IMT to initiate the response effort. Assignment may be based on:
  - - Workload of IMT members
  - - IMT members who have handled similar incidents
  - - Category or priority of the event
  - - Relevant business unit

✓ Respond—The response process includes steps taken to address, resolve or mitigate an incident. CMU SEI defines three types of response activities:

- Technical response—It is appropriate for technical IMT members, such as incident handlers and IT representatives, to analyze and resolve an incident.
- Technical response forms include the following:
  - . Collecting data for further analysis
  - . Analyzing incident-supporting information such as log files
  - . Researching corresponding technical mitigation strategies and recovery options
  - . Consulting telephone or email technical assistance
  - . Securing onsite assistance
  - . Analyzing logs

- . Developing and deploying patches and workarounds

- Management response—The management response includes activities that require supervisory or management intervention, notification, interaction, escalation, or approval as part of response effort.
- Legal response—The legal response is associated with activity that relates to investigation, prosecution, liability, copyright and privacy issues, laws, regulations, and nondisclosure agreements. Because this response may require in-depth knowledge of legal matters, it is usually referred to by the corporate legal team.

## Current State of Incident Response Capability

➔ The information security manager must identify what is already in place as a basis for understanding the current state. There are many ways to do this, including:

- ✓ Survey of senior management, business managers and IT representatives
- ✓ Self-assessment—Self-assessment is conducted by the IMT against a set of criteria to develop an understanding of current capabilities. The disadvantage of this method is that it may provide only a limited view on current capability and aspects that stakeholders may consider important.
- ✓ External assessment or audit—This is the most comprehensive option, and it combines interviews, surveys, simulation, and other assessment techniques in the assessment. This option is normally used for an organization that already has an adequate incident management capability but is further improving it or reengineering the processes.

# Developing an Incident Response Plan

## Elements of An Incident Response Plan

➔ Preparation—This phase prepares an organization to develop an IRP prior to an incident. Sufficient preparation facilitates 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 a communication plan to stakeholders
✓ Developing criteria on when to report an incident to authorities.
✓ Developing a process to activate the IMT.
✓ Establishing a secure location to execute the IRP.
✓ Ensuring equipment needed is available.

➔ Identification—This phase aims to verify if an incident has happened and find out more details about it. Reports on incidents may come from information systems, end users or other organizations. Not all reports are valid incidents; 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 IMT/IRT to contain the incident.
- ✓ Notifying appropriate stakeholders affected by the incident.
- ✓ Obtaining agreement on actions taken that may affect availability of a service or risk 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 PR 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 several ways: restoring backups to achieve a clean state of the system, removing the root cause, improving defenses, and 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 or 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 BCP. The time constraint up to this phase is documented in the RTO. Activities in this phase include:

- ✓ Restoring operations as defined in the SDO.
- ✓ Validating that actions taken on restored systems were successful.
- ✓ Getting involvement of system owners to test the system.
- ✓ Facilitating system owners to declare normal operation.

➔ Lessons learned—At the end of the incident response process, a report should always be developed to share what has happened, what measures were taken and the results after the plan was executed. Part of the report should contain lessons learned that provide the IMT and other stakeholders with valuable learning points of what could have been done better. These lessons should be developed into a plan to enhance the incident management capability and the documentation of the IRP. Activities in this phase include:

- ✓ 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 provides information on the gap between current incident response capabilities and the desired level. By comparing the two levels, improvements in capabilities, skills and technology can be identified, the resulting gap analysis report can be used for planning purposes to determine the steps needed to resolve the gap between the current state and the desired state. It can also be useful in determining the most effective strategy to achieve the objectives and prioritize efforts.

## Business Impact Analysis

- ➔ The next step in the incident response management process, after identifying all events, is to consider the potential impact of each type of incident that may occur.
- ➔ A BIA must:

- ✓ 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. The impact may be in the form of a qualitative (rating) or quantitative (monetary) value.

- ➔ A successful BIA requires participation from business process owners, senior management, IT, physical security, and end users.
- ➔ BIAs have three primary goals:

- ✓ Criticality prioritization—Every critical business unit process must be identified and prioritized. The impact of an incident must be evaluated—the higher the impact, the higher the priority.
- ✓ Downtime estimation—The assessment is also used to estimate the maximum tolerable downtime (MTD) or maximum tolerable outage (MTO) that the business can endure and remain viable. This can also mean the longest period of unavailability of critical processes/services/information assets before the company may cease to operate (i.e., AIW).
- ✓ Resource requirement—Resource requirements for critical processes are also identified currently, with the most time-sensitive and highest-impact processes receiving the highest priority for resource allocation.

- ➔ An assessment includes the following activities:

- ✓ Gathering assessment material—The initial step of the BIA is to identify which business units are critical to an organization. This step can be drilled down to the critical tasks that must be performed and the resources needed to ensure business survival.
- ✓ Analyzing the information compiled—During this phase, several activities take place, such as documenting required processes and resources, identifying interdependencies, and determining the acceptable period of interruption. Tasks in this phase include:
    - ▪ Identify interdependencies among the functions and departments classified as critical or high impact.
    - ▪ Discover all disruptions that could affect the mechanism necessary to allow these departments to function together.
    - ▪ Identify and document potential threats that could disrupt interdepartmental communication.
    - ▪ Gather quantitative and qualitative information pertaining to those threats.
    - ▪ Provide alternative methods of restoring functionality and communication.
    - ▪ Provide a brief statement of rationale for each threat and corresponding information.
- ✓ Documenting the result and presenting recommendations—The last step of an assessment is documenting assessment results from the previous activities and creating a report for business units and senior management.

➔ Elements of a Business Impact Analysis The way in which BIAs are conducted varies from organization to organization. However, there are commonalities. In general, BIAs:

- ✓ Describe the business mission of each business/cost center.
- ✓ Identify the functions that characterize each business function.

- ✓ Determine dependencies such as required inputs from other operations.
- ✓ Determine subsequent operations dependent on the function.
- ✓ Identify critical processing cycles (in terms of time intervals) for each function.
- ✓ Estimate the impact of each type of incident on business operations.
- ✓ Determine required recovery time (i.e., RTO)
- ✓ Identify the resources and activities required to restore an acceptable level of operation.
- ✓ Determine the amount of data that can be lost and must be re-created to determine RPOs.
- ✓ Determine work-around possibilities such as manual or PC-based operation, or workload shifting.
- ✓ Estimate the amount of time that recovering from each type of incident is likely to take in relation to the RTO. If the estimated time is greater than the RTO, additional resources may be needed for recovery. This includes restoration of all required dependencies as well.

## Escalation Process for Effective Incident Management

- ➔ As part of the emergency management and incident management policies and procedures, a detailed description of the escalation process and who must authorize various recovery actions or disaster declaration must be clear and documented.
- ➔ The information security manager should develop these escalation processes and decision authority through consultation with PR, legal counsel, and appropriate senior management. This process should also include vendors and utility services.

## Help/Service Desk Processes for Identifying Security Incidents

- ➔ The information security manager should have processes defined for help/service desk personnel to distinguish a typical request from a security incident.
- ➔ Prompt recognition of an incident in progress and quick referral to appropriate parties are critical to minimizing the damage resulting from such incidents.
- ➔ By defining appropriate criteria and improving the awareness of help/service desk personnel, the information security manager develops another important method to detect a security incident. Proper training also helps to reduce the risk that the help/service desk could be successfully targeted in a social engineering attack designed to obtain access to accounts, such as a perpetrator pretending to be a user who has been locked out and requires immediate access to the system.

## Incident Management and Response Teams

- ➔ Teams included.

- ✓ Emergency action team—Designated first responders whose function is to deal with fires or other emergency response scenarios.
- ✓ Damage assessment team—Qualified individuals who assess the extent of damage to physical assets and make an initial determination regarding what is a complete loss vs. what is restorable or salvageable.
- ✓ Emergency management team—Responsible for coordinating the activities of all other recovery teams and handling key decision making.
- ✓ Relocation team—Responsible for coordinating the process of moving from the affected location to an alternate site or to the restored original location.

- ✓ Security team—Often called a CSIRT; responsible for monitoring the security of systems and communication links, containing any ongoing security threats, resolving any security issues that impede the expeditious recovery of the system(s), and assuring the proper installation and functioning of every security software package.

➔ Several key decisions must be agreed on during the planning, implementation and evaluation phases of the response and recovery plan. These include:

- ✓ Goals/requirements/products for each phase
- ✓ KGIs and KPIs
- ✓ Reporting criteria
- ✓ Critical success factors and critical path aspects of implementation
- ✓ Alternate facilities in which tasks and operations can be performed.
- ✓ Critical information resources to deploy (e.g., data and systems)
- ✓ Decision authority and persons responsible for completion
- ✓ Available resources—including financial, personnel and technical—to aid in deployment.
- ✓ Scheduling of activities with established priorities

## Organizing, Training and Equipping the Response Staff

➔ IMT members should undergo the following training program:

- ✓ Induction to the IMT—The induction should provide the essential information required to be an effective IMT member.
- ✓ Mentoring team members regarding roles, responsibilities, and procedures —Existing IMT members can provide valuable knowledge to aid new members after induction. To facilitate effective mentoring, the buddy system can be used, pairing new members with experienced members.

- ✓ On-the-job training—This may serve to provide an understanding of company policies, standards, procedures, available tools and applications, acceptable code of conduct, etc.
- ✓ Formal training—Team members may require formal training to attain an adequate level of competence necessary to support the overall incident management capability.

## Incident Notification Process

- ➔ Notification mechanisms that enable an automated detection system or monitor to send email or phone messages should be used whenever possible.
- ➔ Notification activities are effective only if knowledgeable personnel understand their responsibilities and perform them in an efficient and timely manner.
- ➔ The information security manager therefore needs to define the responsibilities and communicate them to key personnel.

## Challenges in Developing an Incident Management Plan

- ➔ Lack of management buy-in and organizational consensus— This may happen when senior management and other stakeholders or constituents are not involved in incident management planning and implementation. Senior management is usually occupied with business matters at this stage and may not be able to invest time in incident management. It is the responsibility of the IMT to identify any critical issues and make these known to executive management.
- ➔ the lack of regular meetings between the IMT and constituents. A sense of ownership among constituents in incident management helps to ensure that sufficient resources and support are available for the IMT.
- ➔ Mismatch to organizational goals and structure—Business operates at an accelerated rate and may change significantly over a brief period. A round of discussions may be needed to identify critical

business functions and local stakeholders and understand local regulations.

- ➔Incident management may not be able to cope with the speed or nature of changes happening within the organization.
- ➔IMT member turnover— The champion of incident management, who is normally either a member of senior management or the information security manager, may leave the company unexpectedly, causing any planning or development efforts to come to a halt.
- ➔The lack of a champion is likely to reduce the focus and resources devoted to implementing the plan.
- ➔Lack of communication process—Ineffective communication processes may result either in under communication or overcommunication. In the case of under communication, relevant stakeholders may not receive the information they need.
- ➔Complex and broad plan—The proposed plan may be good and cover many issues, but it is too complex and too broad. Constituents may not be prepared to participate and commit to plans that appear overreaching.

## Business Continuity and Disaster Recovery Procedures

- ➔business continuity is defined as “preventing, mitigating, and recovering from disruption. The terms ‘business resumption planning,’ ‘disaster recovery planning’ and ‘contingency planning’ also may be used in this context.
- ➔The relationship between BC and DR is such that the DRP is a subset of the BCP. Specifically, while BCP goals include incident prevention and mitigation, the DRP is focused on what must be done to restore operations after an incident has already taken place.
- ➔A BCP may be a continuous process that is actively implemented in business-as-usual scenarios, while the DRP is reactive in nature and is implemented only upon satisfaction of a specific set of conditions (i.e., the business has incurred an incident).

## Recovery Planning and Business Recovery Processes

- ➔ Planning includes documenting the requirements for declaring a disaster (i.e., determining when an incident cannot be resolved by the available recovery processes).
- ➔ The declaration of a disaster pursuant to defined declaration criteria requires moving operations to the alternate processing site. planning processes typically includes several main phases, including:

- ✓ Conducting a risk assessment and BIA
- ✓ Defining a response and recovery strategy
- ✓ Documenting response and recovery plans
- ✓ Training that covers response and recovery procedures
- ✓ Updating response and recovery plans
- ✓ Testing response and recovery plans
- ✓ Auditing response and recovery plans

## Recovery Operations

- ➔ It is important to remember that information resources must still be protected, even during the potentially chaotic environment of a business interruption or disaster.
- ➔ A focused risk assessment should be conducted to make management aware of the extent and potential impacts of the security risk introduced by execution of the plan.
- ➔ A realistic plan should cover all aspects of reestablishing the operations at the primary site, including people, facilities, and technology areas.

## Recovery Strategies

- ➔ The total cost of a recovery capability is the cost of preparing for disruptions (e.g., purchasing, maintaining, and regularly testing redundant computers, and maintaining alternate network routing, training, and personnel costs) and the cost of putting these into effect in the event of an incident.

- ➔Impacts of disruptions can, to some extent, be mitigated by various forms of business interruption insurance, which should be considered as a strategy option.
- ➔The information security manager should understand that the development of an incident management and response plan is likely to be a difficult and expensive process that may take considerable time.
- ➔It may be prudent to consider outsourcing some or all the needed capabilities and determine associated costs for the purpose of comparisons.
- ➔Once the decision is made for which strategy best meets management's objectives, that strategy provides the basis for the development of detailed incident management and response plans.

## Addressing Threats

some possible proactive strategies that may be considered as a part of incident management may include:

- ➔Eliminate or neutralize a threat—Although removing or neutralizing a threat might seem like the best alternative, doing so when the threat is external is an unrealistic goal. If the threat is internal and specific, it may be possible to eliminate it.
- ➔Minimize the likelihood of a threat's occurrence—The best alternative is often to minimize the likelihood of a threat's occurrence by reducing or eliminating vulnerabilities or exposure. This goal can be achieved by implementing the appropriate set of physical, environmental and/or security controls. Reducing exposure may be achieved by compartmentalization, such as network segmentation.
- ➔Minimize the effects of a threat if an incident occurs—There are usually several ways to minimize impact if an incident occurs, such as effective incident management and response, insurance, redundant

systems with automatic failover, or other compensating or corrective controls.

## Recovery Sites

- ➔ The most appropriate alternatives for a recovery site must be based on probability of major outages occurring, the nature and extent of impact on the organization's ability to continue operations, and overall cost.
- ➔ The types of offsite backup facilities that can be considered include:

- ✓ Hot sites—Hot sites are configured fully and ready to operate within several hours. The equipment, network and systems software must be compatible with the primary installation being backed up. The only additional needs are staff, programs, data files and documentation.
  cost of rebuild is the crucial factor when deciding whether to build or subscribe to a third-party facility. Hot site must include all needed hardware available (on-floor).
- ✓ Warm sites—Warm sites are complete infrastructures, but are partially configured in terms of IT, usually with network connections and essential peripheral equipment such as disk drives, tape drives and controllers. Sometimes a warm site is equipped with a less powerful central processing unit (CPU) than the primary site.
- ✓ Cold sites—Cold sites are a viable option only when organizations can afford long downtime. Cold sites have only the basic environment (electrical wiring, air conditioning, flooring, etc.) to operate an information processing facility (IPF). The cold site is ready to receive equipment but does not offer any components at the site in advance of the need. Activation of the site may take several weeks. Because data and software are required for these strategies, special arrangements need to be considered for their backup to removable

media and their safe, secure storage offsite. Several options for equipping a cold site exist:

- Vendor or third party—Hardware vendors are usually the best source for replacement equipment. However, this may often involve a waiting period that is not acceptable for critical operations. It is unlikely that any vendor will guarantee a specific reaction to a crisis. Vendor arrangements are used best when an organization plans to move from a hot site to a warm or cold site, so advance planning is critical. Another source of equipment replacement is the used hardware market. This market can supply critical components or entire systems on short notice, often at a reduced cost. Establishing relationships with dealers well in advance of any actual emergency is critical.
- Off-the-shelf—Such components are often available from the inventory of suppliers on short notice but may require special arrangements. To make use of this approach, several strategies must be used, including:

  - . 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.

✓ Mobile sites—Mobile sites are specially designed trailers that can be quickly transported to a business location or an alternate site to provide a ready conditioned IPF. These mobile sites can be attached to form larger work areas and can be preconfigured with servers, desktop computers, communications equipment, and microwave and satellite data links. They are a useful alternative when there are no recovery facilities in the immediate geographic area. They are also useful in case of a widespread disaster and may be a cost-effective alternative for duplicate IPFs for a multisite organization.

✓ Duplicate sites—These facilities are dedicated recovery sites that are functionally similar or identical to the primary site that can quickly take over for the primary site. They range from a standby hot site to facilities available through a reciprocal agreement with another company. The assumption is that there are fewer problems in coordinating compatibility and availability in the case of duplicate sites. Large organizations with multiple data facilities can often develop failover capabilities among their own geographically dispersed data centers provided the following principles are followed:

  - The site chosen should be located so it is not subject to the same disaster event as the primary site. If, for example, the primary site is in an area subject to hurricanes, the recovery site should not be subject to the same hurricanes.
  - Coordination of hardware/software strategies is necessary. A reasonable degree of hardware and software compatibility must exist to serve as a basis for backup.
  - Resource availability must be assured. The workloads of the sites must be monitored to ensure that sufficient availability for emergency backup use exists.
  - There must be agreement concerning the priority of adding applications (workloads) until all the recovery resources are fully used.
  - Regular testing is necessary. Whether duplicate sites are under common ownership or under the same management, testing of the backup operation on a regular basis is necessary to ensure that it will work in the event of a disaster.

- ✓ Mirror sites—If continuous uptime and availability are required, a mirror site may be the best option. By definition, a mirror site is remarkably similar or identical to the primary site. The mirror site is operational in concert with the primary site on a load-sharing basis. Typically, applications are launched by an automatic scheduler that balances the loads between the sites based on available operational capacity and applications can be executed in either one.
- ✓ Reciprocal agreements— (Note that although reciprocal agreements were once common, they are now seldom used.) Under the typical agreement, participants promise to provide computing time and network operations to each other when an emergency arises.

➔ part of the recovery of IT facilities involves telecommunications, for which the strategies usually considered include elements of network disaster prevention:

- ✓ 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

## Basis for Recovery Site Selections

To prepare a suitable recovery strategy, the information security manager must balance all these parameters with the capabilities of diverse types of recovery sites, their costs, and locations.

➔ AIW—The total time that the organization can wait from the point of failure to the restoration of critical services/applications. After this time, the cumulative losses caused by the interruption may threaten the existence of the organization.

- ➔RTO—The length of time from the interruption to the time that the process must be functioning at a service level sufficient to limit financial and operational impacts to an acceptable level. Some organizations express it as partial moments (i.e., from point of failure to technical recovery, or point of disaster declaration to full operations).
- ➔RPO—The age of the data the organization needs to be able to restore in the event of a disaster (i.e., the amount of data that can be lost and needs to be recreated). Sometimes this is expressed as the point of last known good data. This will be the starting point for operations at the recovery site. If full backups are infrequent, it may take too much time to re-create the amount of data lost and the result would be RTOs not being met.
- ➔SDO—Level of services to be supported during the alternate process mode until the normal situation is restored. This must be related to business needs.
- ➔MTO—The maximum time the organization can support processing in the alternate mode. Numerous factors will determine the MTO, including increasing backlogs of deferred processing. This, in turn, is affected by the SDO if it is less than that required during normal operations.
- ➔Proximity factors—The distance from potential hazards, which can include flooding risk from nearby waterways, hazardous material manufacturing or storage, or other situations that may pose a risk to the operation of a recovery site.
- ➔Location—Sufficient distance needed to minimize the likelihood of both the primary and recovery facilities being subject to the same occurrence of an environmental event. When planning, consideration should be given to the typical impact area of the types of events that

have a higher likelihood of occurrence for a given location. For example, in the case of hurricanes vs. tornados, the impact area of a hurricane is typically much larger than the impact area of a tornado, requiring greater distance between sites for a location where hurricanes frequently occur.

➔ Nature of probable disruptions—This must be considered in terms of the MTO. For example, a major earthquake is likely to render a primary site inoperable for several months. The MTO in an area subject to this disruption must be greater than the probable duration of such an event.

## Response and Recovery Strategy

➔ The response and recovery plan should be documented and written in simple language that is clear and easy to read. It is also common to identify teams of personnel who are responsible for specific tasks in case of incidents or disasters.

➔ Copies of the plan must be kept offsite to ensure that it is available when needed; this includes at the recovery facility, the media storage facility, and the homes of key decision-making personnel.

## Response and Recovery Plan

➔ The IRP should include the following elements:

✓ Mission
✓ Strategies and goals
✓ Senior management approval
✓ Organizational approach to incident response
✓ Key decision-making personnel and responsibilities
✓ Communication with the rest of the organization and with other organizations
✓ Metrics for measuring the incident response capability and its effectiveness.
✓ Road map for maturing the incident response capability.

✓ How the program fits into the overall organization

## Integrating Incident Response with Business Continuity

➔ The incident management and recovery plan must be consistent with and support the overall IT plan of the organization. Business continuity planning, disaster recovery and incident response do not necessarily have to be combined into a single plan; however, each must be consistent with the other and integrated so that transition on declaration of a disaster is effective.

➔ Risk tolerance is the acceptable degree of variance to acceptable risk that, finally, must be determined by management.

➔ RTO is defined as the amount of time allowed for the recovery of a business function or resource to a predefined operational level after a disaster occurs.

➔ RPO is defined as a measurement of the point prior to an outage to which data are to be restored; that is, the last point of known good data. RTO and RPO must be intricately linked to facilitate effective incident management and response.

➔ The SDO is the level of acceptable service that must be achieved within the RTO. In many cases, an acceptable level may be less than normal operations, less costly and easier to achieve.

➔ MTO is the total time that operations can be sustained at an alternate site.

## Notification Requirements

➔ The recovery plan must cover notification responsibilities and requirements. It should also include a directory of key decision-making personnel, IRT members, information systems owners, end users, and others required to initiate and carry out response efforts.

➔ The decision to bring in law enforcement during such an incident rests solely with senior management.

## Supplies

- ➔The plan must include provisions for all supplies necessary for continuing normal business activities during the recovery effort. If the data entry function is dependent on certain hardware devices and/or software programs, these programs and equipment, including specialized electronic data interchange (EDI) equipment and programs, must also be provided at the recovery site.

## Communication Networks

- ➔The plan must contain details of the organization's telecommunication networks needed to restore business operations. Because of the criticality of these networks, the procedures to ensure continuous telecommunication capabilities should be given a high priority.
- ➔The local exchange carrier is typically not responsible for providing backup services. Although many carriers normally back up main components within their systems, the organization should make provisions for backing up its own telecommunication facilities.

## Methods for Providing Continuity of Network Services

Methods for providing continuity of network services include:

- ➔Redundancy—Achieving redundancy involves a variety of solutions, including:

- ✓ Providing extra capacity with a plan to use the surplus capacity should the normal primary transmission capability not be available. In the case of a LAN, a second cable could be installed through an alternate route for use if the primary cable is damaged.
- ✓ Providing multiple paths between routers
- ✓ Using special dynamic routing protocols such as the Open Shortest Path First (OSPF) and External Gateway Routing Protocol (EGRP)

- ✓ Providing failover devices to avoid single points of failure in routers, switches, firewalls, etc.
- ✓ Saving configuration files for recovery of network devices, such as routers and switches, if they fail

- ➔ Alternative routing—Alternative routing means routing information via an alternate medium such as copper cable or fiber optics. This involves use of different networks, circuits, or end points if the normal network is unavailable.
- ➔ Diverse routing—This is the method of routing traffic through split cable facilities or duplicate cable facilities. This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and, therefore, subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer's premises may be in the same conduit.
- ➔ Long-haul network diversity—Many vendors of recovery facilities provide diverse long-distance network availability, using high-speed data circuits among the major long-distance carriers. This ensures long-distance access if any single carrier experiences a network failure. Several of the major carriers have now installed automatic rerouting software and redundant lines that provide instantaneous recovery if a break in their lines occurs.
- ➔ Last-mile circuit protection—Many recovery facilities provide a redundant combination of local carrier high-speed data circuits, microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local carrier routing is also used.
- ➔ Voice recovery—Many service, financial and retail industries dependent on voice communication. Therefore, their recovery plans

should provide for redundant cabling and alternative routing for voice communication lines as well as data communication lines.

## High-Availability Considerations

- ➔Compatible with DAS, NAS and SAN storage solutions, a redundant array of inexpensive (or independent) disks (RAID) provides performance improvements and fault-tolerant capabilities via hardware or software solutions, breaking up data and writing them to a series of multiple disks to improve performance and/or save large files simultaneously. These systems provide the potential for cost-effective continuous data availability onsite or offsite.
- ➔distributed processing of a server load—a concept referred to as “load balancing” or “clustering”—where all servers take part in processing. In this arrangement, an intelligent cluster unit provides load balancing for improved performance. This type of server architecture is transparent to users. The only thing that may be noticeable to a user is performance degradation if a server fails.
- ➔The information security manager must be aware of the prohibitive costs associated with fault-tolerant solutions and difficulties in achieving this state of data availability. For example, in a virtual environment, multiple instances (copies) of a virtual machine (VM) running in parallel must exist. Any change in the state of the primary VM (such as modification of a file) must be applied on all the secondary VMs in real time.

## Insurance

The IRP should include information regarding the organization’s insurance plans, including general coverage, cyber insurance, or IT-related insurance. Some elements of the organization’s coverage, such as a business interruption policy, may provide some level of protection and should be considered as part of the plan.

It should be noted that an organization cannot typically not insure against failure to comply with legal and regulatory requirements or any other breach of the law. Some of the specific types of coverage that are available include:

Professional and commercial liability—Protection from third-party claims for losses and damages caused by the insured.

Valuable papers and records—Covers the actual cash value of papers and records (not defined as media) on the insured's premises against unauthorized disclosure, direct physical loss, or damage.

Fidelity coverage—Usually takes the form of banker's blanket bonds, excess fidelity insurance and commercial blanket bonds, and covers loss from dishonest or fraudulent acts by employees. This type of coverage is prevalent in financial institutions operating their own IPF.

## Updating Recovery Plans

Plans and strategies for response and recovery should be reviewed and updated according to a schedule to reflect continuing recognition of changing requirements.

The responsibility for maintaining the BCP/DRP often falls to a BCP coordinator, and the information security manager may be responsible for maintaining the IRP.

## Testing Incident Response and Business Continuity/Disaster Recovery Plans

- ➔ The main objective of testing is to ensure that executing the plans will result in the successful recovery of the infrastructure and critical business processes.
- ➔ Testing should focus on:

- ✓ Identifying gaps
- ✓ Verifying assumptions

Disclaimer: Use for review after studying our CISM Course – https://cyvitrix.com

- ✓ Testing timelines
- ✓ Determining the effectiveness of strategies
- ✓ Evaluating the performance of personnel
- ✓ Determining the accuracy and currency of plan information

➔ Testing must be carefully planned and controlled to avoid placing the business at increased risk. To ensure that all plans are regularly tested, the information security manager should maintain a "testing schedule" of dates and tests to be conducted for all critical functions.

➔ Prior to each test, the security manager should ensure that:

- ✓ The risk and impact of disruption from testing is minimized.
- ✓ The business understands and accepts the risk inherent in testing.
- ✓ Fallback arrangements exist to restore operations at any point during the test.

## Types of Tests

➔ Types of basic tests include:

- ✓ Checklist review—This is a preliminary step to a real test. Recovery checklists are distributed to all members of a recovery team to review and ensure that the checklist is current.
- ✓ Structured walkthrough—Team members physically implement the plans on paper and review each step to assess its effectiveness and identify enhancements, constraints, and deficiencies.
- ✓ Simulation test—The recovery team role-plays a prepared disaster scenario without activating processing at the recovery site.
- ✓ Parallel test—The recovery site is brought to a state of operational readiness, but operations at the primary site continue normally.
- ✓ Full interruption test—Operations are shut down at the primary site and shifted to the recovery site in accordance with the recovery plan; this is the most rigorous form of testing, but it is also expensive and potentially disruptive. Disruptive testing should be scheduled during

a time that will minimize impact on normal operations. Weekends are an enjoyable time to conduct tests. It is important for all key recovery team members to be involved in the recovery test process. The test should address all critical components and simulate actual prime-time processing conditions, even if the test is conducted during off hours.

➔ Testing should start simply and increase gradually, stretching the objectives and success criteria of previous tests to build confidence and minimize risk to the business. At a minimum, "full interruption" tests should be performed annually after individual plans have been tested separately with satisfactory results.

➔ There are three main recovery testing categories:

✓ Paper tests—Paper tests are an on-paper walkthrough of the plan involving the major players in the plan's execution who reason out what might happen in a particular type of service disruption. They may walk through the entire plan or just a portion. The paper test usually precedes preparedness tests.

✓ Preparedness tests—Preparedness tests are usually localized versions of a full test; wherein actual resources are expended in the simulation of a system crash. These tests are performed regularly on various aspects of the plan and can be a cost-effective way to gradually obtain evidence about how good the plan is. They also provide a means to improve the plan in increments.

✓ Full operational tests—These tests are one step away from an actual service disruption. An organization should have tested the plan well on paper and locally before endeavoring to completely shut down operations. For purposes of BCP testing, the full operational testing scenario is a disaster.

## Test Results

➔ A recovery 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.

➔ To perform preparedness or operational recovery testing, each of the following test phases should be completed:

- ✓ Pretest—The pretest consists of the set of actions necessary to set the stage for the actual test. This ranges from placing tables in the proper operations recovery area to transporting and installing backup telephone equipment. These activities are outside the realm of those that would take place in the case of a real emergency, in which there is no forewarning of the event and thus, no time to take preparatory action.
- ✓ Test—Actual operational activities are executed to test the specific objectives of the plan. Data entry; telephone calls; information systems processing; handling orders; and movement of personnel,

equipment and suppliers should take place. Evaluators should review staff members as they perform the designated tasks. This is the actual test of preparedness to respond to an emergency.

- ✓ Posttest—The posttest is the cleanup of group activities. This phase comprises assignments such as returning all resources to their proper place, disconnecting equipment, returning personnel to their normal locations, and deleting all company data from third-party systems. The posttest cleanup also includes formally evaluating the plan and implementing indicated improvements.

## Recovery Test Metrics

- ➔ Results should be recorded and evaluated quantitatively, as opposed to an evaluation based only on verbal descriptions.
- ➔ Although specific measurements vary depending on the test and the organization, the following general types of metrics usually apply:

- ✓ Time—Elapsed time for completion of prescribed tasks, delivery of equipment, assembly of personnel and arrival at a predetermined site. This is essential to refine the response time estimated for every task in the escalation process.
- ✓ Amount—Amount of work performed at the backup site by clerical personnel and the amount of information systems processing operations.
- ✓ Percentage and/or number—The number of vital records successfully carried to the backup site vs. the required number, and the number of supplies and equipment requested vs. received. The number of critical systems successfully recovered can be measured with the number of transactions processed.
- ✓ Accuracy—Accuracy of the data entry at the recovery site vs. normal accuracy (as a percentage). The accuracy of actual processing cycles can be determined by comparing output results with those for the same period processed under normal conditions.

## Executing Response and Recovery Plans

- ➔To ensure the response and recovery plans are executed as required, the plans need a facilitator or director to direct the tasks within the plans, oversee their execution, liaise with senior management, and make decisions, as necessary. must be certain the role is assigned to someone who can perform this critical function.
- ➔The information security manager should also appoint an independent observer to record progress and document any exceptions that occur during testing and an actual event. Through a post event review, the information security manager and key recovery personnel can then review the observations and adjust the plan accordingly.
- ➔A serious incident is typically chaotic. Good documentation will prove invaluable in post incident investigation and forensics and may also be helpful in incident resolution.
- ➔information security manager can develop procedures to handle security events in a manner that preserves evidence, ensures legally sufficient chain of custody and is appropriate to meet business objectives.

## Requirements for Evidence

- ➔The usual recommendation for a computer that has been compromised is to disconnect the power to maximize the preservation of evidence on the hard disk.
- ➔This approach is the recommendation of law enforcement based on the risk of the evidence being compromised. This can occur because of the system swap files overwriting evidence or an intruder or malware erasing evidence of compromise.
- ➔There is also the risk of contaminating evidence. This approach is not universally accepted as the best solution. One argument against disconnecting power is that data in memory are lost and sudden power loss may result in corruption of critical information on the

hard disk. Because some malware is only memory-resident, the cause of an incident and the avenue of attack may be difficult to establish.

➔ Whichever procedure is used to secure a compromised system, trained personnel must use forensic tools to create a bit-by-bit copy (or disk image) of any evidence that may exist on hard drives and other media to ensure legal admissibility.

➔ testing or data analysis should be conducted using this copy. The original should be given to a designated evidence custodian who must store it in a safe location. The original media must remain unchanged and a record of who has had custody of it—the chain of custody—must be maintained for the evidence to be admissible in court.

➔ When taking a copy of a hard drive, the technician should take a bit-level image of all the data on the drive, using a cable with a write-protect diode to prevent writing anything back onto the source drive. Hash values of both the source and destination drive should be calculated to ensure that the copied drive is an exact image of the original.

## Legal Aspects of Forensic Evidence

➔ Procedures for initiating a forensics investigation need to be agreed to, documented, followed carefully, and understood by everyone in the enterprise. The information security manager should work with management and HR (and other stakeholders) to establish a process that ensures that all investigations are fair, unbiased, and well documented.

➔ It is important to be aware that legal requirements vary in different jurisdictions. As a result, informed legal advice for appropriate processes that meet judicial standards will be required.

## General Comments

- ➔ Incident management is defined as the capability to effectively manage unexpected operationally disruptive events to the organization with the objective of minimizing impacts and maintaining or restoring normal operations within defined time limits.
- ➔ Incident response is the operational capability of incident management that identifies, prepares for, and responds to incidents incident response is the responsibility of the information security manager.
- ➔ for developing and testing the incident management and response plans and ensuring it correlates with the business continuity and disaster recovery plans in case incident response is insufficient to resolve an event.
- ➔ Decoy files is another synonym for honeypots.
- ➔ formal (approved) incident response plan (IRP) is established and maintained for multiple objectives, such as:

- ✓ Demonstrating that incident response efforts have senior management support.
- ✓ Ensuring that the IRP is in a communicable form to allow for organizational distribution, review and revision based on incident-handling experience and organizational changes.
- ✓ Outlining the goals for a consistent and systematic approach in addressing and remediating incidents in a timely manner that is consistent with business Objectives Timeliness, as a component of effectiveness when identifying information security incidents, is the time that passes between incident identification and acceptance as a valid incident.
- ✓ Escalation procedures must be set up that include alternates in the event some stakeholders cannot be reached or the incident remediation effort encounters complications.

- ✓ Communication plans should be formally documented, and resource listings maintained.
- ✓ To properly address root causes, form lessons learned and maintain an accurate archive of incident events, the information security manager must establish a formal post incident review process.
- ✓ SIEM quality relies on use cases.
- ✓ Top management participation is required for DR testing; however, it is not much needed in actual BCP execution.
- ✓ Interruption tests provide full assurance, while simulation provides assurance without impacting production.
- ✓ Distribution of key process documentation.
- ✓ When notified about an incident or threat, the security manager must determine if the claim is true.
- ✓ Awareness training aids in the incident identification process.
- ✓ Incident management should support problem management by spending time in identification and understanding the root cause of threat.
- ✓ The purpose of a well-structured incident response plan is to provide a basis for legal and liability matters.
- ✓ The most key point in incident management is the expertise of resources.
- ✓ Conducting a business impact analysis is the first step in the incident response management process.
- ✓ Better governance would have vested adequate authority in the network manager to take the appropriate action.
- ✓ A disaster recovery plan (DRP) for the overall organization is a governance issue; therefore, it is the responsibility of the board of directors to ensure that a DRP is in place.
- ✓ When policies are strictly enforced, the total cost of security increases.

- ✓ Resilience refers to the ability of the business to withstand disruption.
- ✓ Post incident review aims to enhance response, identify lesson learned, while in eradication, root cause is eliminated.

## Post CISM Exam notes.

### *Domain 1*

- Types of Law at US

1. Criminal Law
2. Administrative Law
3. Civil Law
4. Intellectual property (Trade Secret)

- The most important part regarding policies is the notification.
- Awareness training aids in modifying behavior, make employees more accountable and raise collective awareness.
- CISSP exam mindset
    1. You are a risk advisor? -> you advise only with what is approved by Policy, advise to tune it.
    2. Who is accountable for Security? -> Senior management is accountable, but all are responsible
    3. How much security is enough? -> enough security is what is reasonable for your scenario based on risk management decision.
    4. All decisions start with Risk management.
    5. Think "End Game" -> find answer best satisfies the requirements.
    6. Security Transcends technology -> security comes first, security is bigger than technology.
    7. Physical safety is always first.

8. Technical questions are for managers, Management questions are for technicians (best practices, and real environment)
9. Incorporate security in design.
10. Apply layered defense, do not rely on one device, layered defenses should be (Layering, Limiting, diversity "if the two are the same, the same bypass will occur," obscurity "error messages should not reveal what control you implement," simplicity)

- SOC 1 report includes finance reporting, SOC 2 report internal technical controls and require NDA from receiving party, SOC 3 report technical aspects but for public.
- Mirrored site is usually ours, while rest might be supplied by 3rd party.
- MOU and MOA, A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.

## Software development Security

| | |
|---|---|
| Reduce the attack surface | - User input validation<br>- Protocol/service/interface.<br>- Resource files<br>- Named pipes/ open sockets.<br>- How many items are accessible?<br>- Dynamic webpage (ASP)<br>- Guest accounts and non-used accounts and change default name or password.<br>- ACL configurations |

| | |
|---|---|
| Threat modeling | - Identify security objectives from legal/contractual, business objective point of view.<br>- CIA triad + no repudiation<br>- Use data flow diagram and Use/Misuse cases.<br>- Classification of Bugs use term DREAD.<br>[D] Damage potential<br>[R] Reproducibility<br>[E] Exploitability<br>[A] Affected user base<br>[D] Discoverability<br>- Threat source use term STRIDE<br>Spoofing, Tampering, Repudiation, Information disclosure, Elevation of privileges |
| Risk in design | - Code reuse.<br>- Flaw -> inherent fault with the code design.<br>- Bug -> Implementation web (poor implementation)<br>- Open vs. closed design |
| Controls evaluation | - Efficacy<br>- Economy of mechanism (not just lower dollar value)<br>- Cost/benefit analysis<br>- Psychological acceptability |

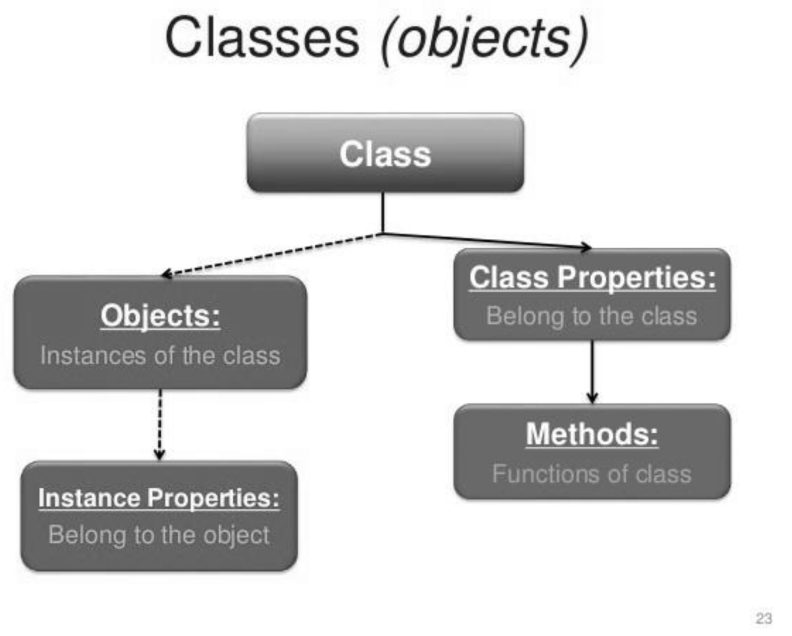
- Secure design considerations
    - CIA
    - AAA
    - Secure design principles
      (Enough security, DoD, SoD, Fail Safe, Open Design,

economy of mechanism, least common mechanism, weakest link, Single point of failure, physiological acceptance)

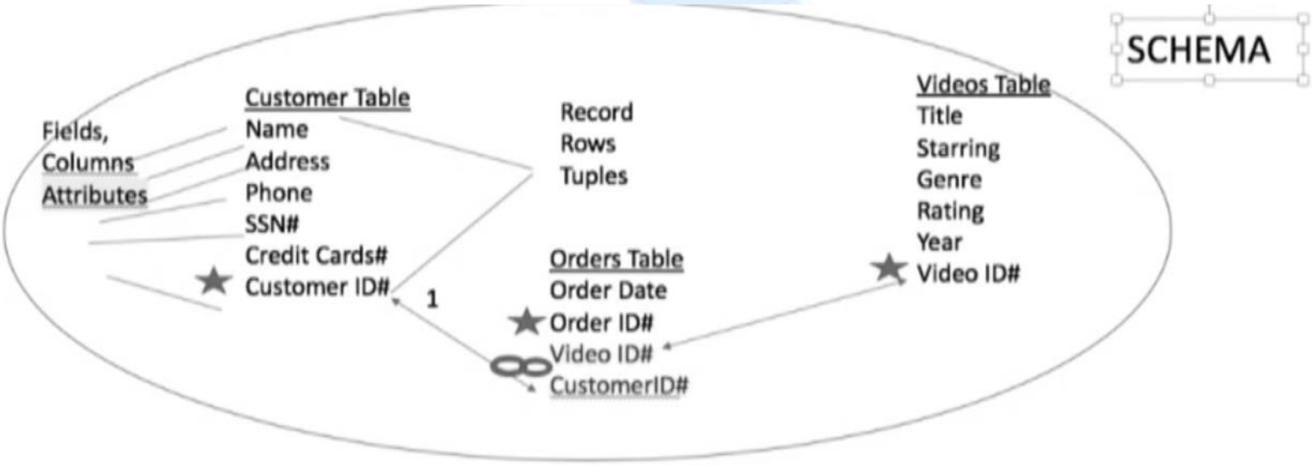
- Quality means fitness for use, security focuses on reducing the impact of probability of vulnerability or threat, both terms can be achieved through the entire development lifecycle.

- Difference between Verifying and validating.
  - Verification confirms the correctness of application as per requirements and specifications.
  - Verification comes before certification, certifying product means it is verified. Certification is technical verification.
  - Validation is the management acceptance of the product.
  - Accreditation comes after validations, management, or ISO decision.

- OOP is modular and reusable, it uses objects, classes, methods, functions. Class is a concept, object the class to life, username, email, and password attributes to object.



- Databases foundation and key terms: -
  - Hierarchical Databases (Like LDAP, DNS)
  - Distributed Database (Like DNS ".com, .net, .gov")
  - Entity integrity -> field is unique and cannot be empty (Primary key)
  - Primary key -> uniquely identifies each record as unique.
  - Normalization -> Each attribute in a database must describe only the primary key. Provides a means for removing duplicates.
  - Databases consist of tables that include attributes associated with value; this value is called records.
  - Tuples refer to information in table rows.
  - Relational databases use primary keys from different tables, when it appears in secondary table, it is referred as a foreign key.
  - Cardinality means number of rows in a relation.
  - Degree, number of column in a relation



  - Aggregation, information is aggregated together can provide classified information.
  - Inference,
  - Polyinstantiation, two description for the same event in database for info we need to protect instead of tagging it top secret.

## - Additional Notes – Aggregated

- Criticality vs sensitivity is important, criticality is mostly about data owned by organizations, while sensitivity I smore related to privacy.
- Terms related to cloud includes Data dispersion which means replicating data to multiple availability zones, while data fragmentation involves splitting a data set into smaller fragments and distributing them across many machines.
- Data obfuscation and masking "hide," anonymization "medical statistics," and tokenization is used in Banking and financial services.
- DRM "data rights management," applies ACL on file level, IRM will travel with the file "persistent," support dynamic policy where owner can change/recall/expire content after distribution.
- Archives are data considered to be out of use but preserved if it is required later.
- Backups are copies of current data, intended for fault tolerance.
- Media disposal
  1. Degaussing work with magnetic media, it leaves drive usable "After perform low-level formatting," data still however able to retrieve with special technology.
  2. Deleting or format is not secure, deleting is just removing the pointer, the most effective way if you want to re-use the media, zeroization is the answer.
- IOCE and SWGDE -> Provide forensics guidelines.
- Digital evidence must be "authentic, accurate, complete, convincing, admissible."
- Steps of forensics
  1. Identification
  2. Preservation
  3. Collection (Store with volatile)

4. Examination
5. Analysis
6. Presentation
7. Decision

- Evidence life cycle
  1. Collection and identification
  2. Analysis
  3. Storage, preservation, transportation
  4. Present in court.
  5. Return to victim.
- Evidence types
  1. Direct evidence
  2. Tangible evidence
  3. Best evidence
  4. Secondary evidence
  5. Corroborative evidence
  6. Circumstantial evidence
  7. Hearsay evidence
  8. Demonstrative evidence
- Types of backups
  1. Full backup -> archive bit is reset.
  2. Incremental backup -> backup all files modified since last backup and reset arch. Bit
  3. Differential backup -> backup all files modified since last full backup, do not reset arch.bit.
  4. Copy backup -> backup full, do not reset arch.bit, use before upgrades.
- IDS detection uses either pattern matching (signature) or profile matching (anomalies, heuristics, behavioral).
- A line conditioner ensures steady and stable voltage by filtering incoming power and eliminating fluctuation and interference.

- Incidental computer crime -> the computer store tools and seized as part of evidence.
- Computer targeted crime -> attack aims to harm computer or its owner.
- Computer assisted crime -> when computer is the tool in attack.
- Computer prevalence crime occurs because computer is widely used ex. Software piracy.
- GLBA is applicable to finance institutes.
- Civil law has no prison option, only fines.
- SPA in the US is an association that deals with prevention of software piracy.
- Disclosure of sensitive info related to drug or alcohol abuser permitted to
  1. Disclosure allowed by the court order.
  2. Patient gives his written consent for the disclosure.
  3. To medical personal in an emergency
  4. To qualified personnel for purpose of research and audit.
- When a person took too many permissions than usual, it called authorization creep.
- For medical, privacy notice to be provided at the first time, on post, and upon request.
- The security analyst has a strategic role in creating security processes; he participates in system development to maximize the benefit by incorporating security in the design.
- Exigent circumstances are used when evidence might be destroyed. It allows officials to seize evidence without a warrant.
- In data center design, the internal walls must have a 1-hour fire rating, adjacent walls should have a two-hour minimum

fire rating, the door must prohibit forcible entries, and raised floors should be electrically grounded.

- Safe harbor privacy law is mandated in Europe; GDPR, however, is applied around the globe.
- Due care implies that a company assumes responsibility for the actions taking place within it by taking reasonable measures to prevent security breaches and protect data. Due diligence is lower than due care performed before the due-care standard is set.
- System and data owners are accountable for the CIA.
- Finance public trade companies in the US are subject to SOX, BASEL, GLBA
- The Patriot Act is used by the US to reduce restrictions of search email, medical, and financial where the U.S. government is investigating agents of governments.
- A no expectation of privacy statement in policy indicates that data transferred in company network is not guaranteed to remain confidential.
- BS7799 is the base of ISO 17799, which describes enterprise security.
- COSO is a security framework that acts as a model for corporate governance and focuses more on strategic goals, while Cobit focuses on operational goals.
- Administrative law is also known as regulatory; an example of it is PCI-DSS
- Civil law is based on written laws; it is used in Europe.
- Common law is made up of criminal, administrative, and civil law, used in the US, UK, ANZAC
- Under mixed law, when two legal systems are used in a country, one law may apply in one situation.

- U.S. Federal sentencing guidelines take care of white-collar crimes inside organizations.
- The Delphi technique is a quantitative risk analysis in which each member provides anonymous opinions to ensure that members are not pressured into agreeing with other parties.
- The Internet Advisory Board (IAB) helps to develop ethics-related statements concerning the use of the Internet.
- W3C developed P3P.
- OBM circular developed to meet information resource management requirements.

Thank you.

https://cyvitrix.com

Check out our Courses!

Here