Study Guide

CRISC

Created By: Nenad Andrejevic, Teaching Assistant

Module 1: Welcome and Introduction

Lesson 1.1: Welcome and Introduction

Skills Learned From This Lesson: Introduction to course - agenda, instructor introduction, Introduction to certificate CRISC

- Course material:
    - Study guide (you are reading it now)
    - Glossary
    - Flashcards

Lesson 1.2: Who is ISACA?

Skills Learned From This Lesson: History and value of ISACA as organisation, value of c certification, other ISACA certification

- ISACA is an international professional association focused on IT (Information technology) governance. It is known as the Information Systems Audit and Control Association, although ISACA now goes by its acronym only.
    - WEB: https://www.isaca.org
    - CRISC - is the only certification that prepares and enables IT professionals for the unique challenges of IT and enterprise risk management, and positions them to become strategic partners to the enterprise.
        - https://www.isaca.org/Certification/CRISC-Certified-in-Risk-and-Information-Systems-Control/Pages/default.aspx
    - Respectable certificate around the globe.
    - Vendor neutral - not vendor specific.
    - Portable certification - not industry specific.

  - Increase your marketing value :-)

Lesson 1.3: Who Should Take CRISC?

Skills Learned From This Lesson: Benefits of certification for you and for your employer.

- Those who earn CRISC help enterprises to understand business risk, and have the technical knowledge to implement appropriate IS controls.
- CRISC is designed for:
  - IT professionals
  - Risk professionals
  - Control professionals
  - Business analysts
  - Project managers
  - Compliance professionals
- IT risk are business risk
- CRISC certification can help you pass the other IT security certifications such as CISM, CISA, CISSP or PMP.
- Course agenda follow the ISACA Risk life cycle:
  - Domain 0 - Introduction To Is Risk Management Concepts
  - Domain 1 - Identifying IT Risk (27%)
  - Domain 2 - Assessing IT Risk (28%)
  - Domain 3 - Risk Response And Mitigation (23%)
  - Domain 4 - Risk And Control Monitoring And Reporting (22%)
  - Exam question preparation review

Lesson 1.4: The Exam

Skills Learned From This Lesson: What is the certification process, how to register and scheduling the exam. You will learn about the exam format, numbers of questions, passing score. Steps need to be taken after the exam and application submitting process.

- Since December 2017, ISACA changed from paper based exam to computer based exam. There were no more paper based exams.

- !!!! NOTE !!!! - In the video, Kelly explain about registration process and time frames for taking exam. However ISACA change their exam policy, from the June 2019. !!!! NOTE !!!
- Beginning in June 2019, ISACA exams (CISA, CISM, CGEIT, CRISC, CSX-Audit, CSX-Fundamentals, COBIT) are now administered all year round in what is known as Continuous Testing.
- Exam candidates may register for the exam whenever they are ready to sit for the examination. There are no deadlines as to when an individual needs to register by.
- When registering for Continuous Testing, exam candidates are provided with a 365-day exam eligibility period to sit for the examination. Individuals may schedule their examination for a location, date, and time that is most convenient to them (based on location and date availability.
- Exam format
    - 150 Multiple choice questions
    - Four hours allotted for taking exam
    - Scoring from 200-800 points 450 points for passing
    - Only one Credited answer
    - Questions are weighted
    - Questions are designed to test Practical knowledge and experience
- After successfully passing the exam:
    - Meet the following work experience requirements in the fields of IT risk management and IS control.
    - A minimum of at least three (3) years of cumulative work experience performing the tasks of a CRISC professional across at least two (2) of the four (4) CRISC domains is required for certification. Of these two (2) required domains, one (1) must be in either Domain 1 or 2.
    - Adherence to the Code of Professional Ethics
        - https://www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/default.aspx
    - Adherence to the Continuing Professional Education (CPE) Policy
        - Attain and report a minimum of one hundred and twenty (120) CPE hours for a three-year reporting period and attain and report an annual minimum of twenty (20) CPE hours.

Brought to you by:
CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

- https://www.isaca.org/Certification/Additional-Resources/Pages/Annual-CPE-Audit.aspx

Module 2: Preliminary

Lesson 2.1: Video Introduction to Information Security Risks

Skills Learned From This Lesson: Risk, Information security Risk, Definition, Risk factors, Assets, Threat, Vulnerability, Likelihood

- Risk definition by ISACA - The combination of the probability of an event and its impact.
- For many practitioners, traditional definition Risk = Threat x Vulnerability is considered more useful because separate risk from impact (consequences).
- IT Risk - The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.
- Assets - Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation.
- Risk calculation is defined by R(risk) = A(asset) x T(threat) x P(probability)

Lesson 2.2: Risk Governance vs. Risk Management

Skills Learned From This Lesson: Governance, Management, Board of directors, Steering committee,Senior management

- Entities responsible for governance - board of directors, managers, shareholders, creditors, auditors, regulators.
- Corporate governance is the collection of mechanisms, processes and relations by which corporations are controlled and operated. Governance structures and principles identify the distribution of rights and responsibilities among different participants in the corporation (such as the board of directors, managers, shareholders, creditors, auditors, regulators, and other stakeholders) and include the rules and procedures for making decisions in corporate affairs. (https://en.wikipedia.org/wiki/Corporate_governance)
- Culture of the organization - also includes the organization’s vision, values, norms, systems, symbols, language, assumptions, beliefs, and habits (Needle, 2004).
- “ Culture, more than rule books, determine how a company behaves.” - Warren Buffett
- Risk Governance - four main objectives:

Brought to you by:
CYBRARY | FOR BUSINESS
*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

  - Establish and maintain common risk view
  - Integrate risk management into the enterprise
  - Make risk-aware business decisions
  - Ensure that risk management controls are implemented and operating correctly
- Governance should give an answer to these four questions :
  - Are we doing the right things ?
  - Are we doing the right way ?
  - Are we getting them done well ?
  - Are we getting the benefits ?
-
- Governance determine - focus, directions
- Governance delivering value
- Risk Management
- “Companies that think about risk in the context of their business decisions can be better positioned to manage the risks that drive performance.” - GRC survey 2015, EY, 2015
- Context of the organization define risk view.
- Risk management is conducted by functional leadership.
- Focus on :
  - Planning
  - Building
  - Running
  - Monitoring
- Risk management - Foresees challenges to a degree that’s acceptable by senior management (or board directors)
- Main difference - Governance (is more about WHAT) vs Management (HOW)

Lesson 2.3: Risk Definitions -Little bit coroase sound :(

Skills Learned From This Lesson: Asset, Vulnerability, Threat, Probability, Impact, Threat agent, Exploit, Risk, Skill

- Asset - Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation.
- Vulnerability - A weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Threat - Anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm.A potential cause of an unwanted incident (ISO/IEC 13335)
- Probability - The likelihood to the risk will occur.
- Impact - Magnitude of loss resulting from a threat agent exploiting a vulnerability. The damage caused it the risk will occur.
- Threat agent - Methods and things used to exploit a vulnerability. Examples include determination, capability, motive and resources (What carries out to attack).
- Exploit- Full use of a vulnerability for the benefit of an attacker. An instance of compromise.
- Risk definition by ISACA - The combination of the probability of an event and its impact (consequence). Risk are unknown entities - until they are realized (and then becomes an incident)
- Additional Risk Definitions
- Inherent risk - The risk level or exposure without taking into account the actions that management has taken or might take (e.g., implementing controls).
- Residual risk - The remaining risk after management has implemented a risk response.
- Secondary Risk - One risk response may cause a second risk event (e.g. system cannot boot after security patch applied)
- Risk Appetite - Risk appetite is the level of risk that an organization is prepared to accept in pursuit of its objectives, before action is deemed necessary to reduce the risk. It represents a balance between the potential benefits of innovation and the threats that change inevitably brings. Amount and type of risk that an organization is prepared to pursue, retain or take (ISO 31000)
- Risk Tolerance - levels of risk, types of risk, and degree of risk uncertainty that are acceptable.
- Risk profile - A risk profile identifies the acceptable level of risk an organization is prepared and able to accept.
- Risk Threshold - measure of the level of uncertainty or the level of impact at which a stakeholder may have a specific interest. Below that risk threshold, the organization will accept the risk. Above that risk threshold, the organization will not tolerate the risk.
- Risk Capacity - refers to the maximum amount of risk that an organization is able to tolerate.
- Risk Utility - The positive outcome desired from taking risk.

CYBRARY

- Types of Risk
  - Systemic Risk - Systemic risk is the possibility that an event at the company level could trigger severe instability or collapse an entire industry or economy. Systemic risk was a major contributor to the financial crisis of 2008. Companies considered to be a systemic risk are called "too big to fail."
  - Contagious Risk - Event that happen to several business partner in a short time frame (e.g. DYN DoS - led to loss of availability to Clodud providers such as Amazon, Yahoo, Twitter etc)
  - Obscure Risk - Unknown of unknowns, risk that is still unknown, or difficult for identification.

Lesson 2.4: IT Risk Management

Skills Learned From This Lesson: IT Risk, Business Risk, Controls

- Business risk and IT risk should be aligned, they should not be (and they aren't) different entities.
- IT risk is a subset of business risk.
- Information security is all about risk management.
- Different type of risk, require different set of controls
- IT risk attempt to reduce IT risk to an acceptable level, focused on “known unknowns”, however Business Continuity Plan is focused on “unknown unknowns” (black swan), with moderate to high impact.
- Context of IT Risk Management depends on Context of entire organization, or environment. Different organizations require different approaches to IT Risk Management.
- Exam tip: Always start with knowing the context of organization.

Lesson 2.5: IT Security Basics

Skills Learned From This Lesson: Information Security, Confidentiality, Integrity, Availability, CIA Triad, Identity and Access Management (IAM), Non-Repudiation

- Confidentiality - Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information.
  - Threats against confidentiality :

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the ***fastest growing catalog*** *in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

        - Social engineering
        - Media reuse
        - Eavesdropping
- Integrity - is the concept of protecting the reliability and correctness of data. Integrity protection prevents unauthorized alteration of data. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
    - System integrity - refer to integrity of the system (include not limited to operating system, Software, hardware / firmware etc) - free from unauthorized manipulation.
    - Data integrity - refer to integrity of the data (no alteration in the data) - intentionally or not, including but not limited to corruption of data or malicious modification.
- Availability - means authorized subjects are granted timey and uninterrupted access to objects. Availability protection controls support sufficient bandwidth and timeliness of processing as deemed necessary by the organization or situation.
    - To provide timely and reliable access to resources enable:
        - Redundancy
        - Prevent Single point of Failure
        - Comprehensive fault tolerance (Data, Hard Drives, Solid State Drives, Network links, Servers, Power etc.)
- Identity and Access Management (IAM) - Encapsulates people, processes and products to identify and manage the data used in an information system to authenticate users and grant or deny access rights to data and system resources. The goal of IAM is to provide appropriate access to enterprise resources.
    - Main functions are:
        - Account provisioning / deprovisioning
        - Identification
        - Authentification
        - Authorisation
        - Auditing
- Non-Repudiation -is the assurance that someone cannot deny the validity of something.
    - Provide proof of the integrity and origin data or message.

    - Must include authentication that can be asserted to be genuine with high assurance.
    - A sender cannot dispute having sent a message, nor the contents of that message.
    - Digital signatures (combined with other measures) can offer non-repudiation.

CYBRARY

- Classification of data is another way to protect our information. In order to protect data those should be considered :
        - Cost - Value of the data or asset.
        - Classify - The owner of the data/asset provide classification based on predefined standards.
        - Control - depends on the level of the classification, security controls should be implemented equally for the data or asset within the same classification.
    - Business classification (by ISO 27001) :
        - Public (everyone has access)
        - Internal (all employees have access)
        - Restricted (most employees have access)
        - Confidential (only senior management have access)
    - The U.S. government uses three levels of classification to designate how sensitive certain information is:
        - Confidential
        - Secret
        - Top Secret

Lesson 2.6: Risk Management for IT Projects

Skills Learned From This Lesson: IT Projects, PMI, PMBOK, Risk register

- Project management is usually focused to deliver “on time, on budget”. Risk management in project management is essential to keep the project under control.
- The PMBOK’s Project Risk Management knowledge area contains 7 processes:
    - Plan Risk Management

        - This initial step involves the production of a risk management plan, a component of the overall project management plan. It includes things like itemizing the risk categories (market, procurement, resources, etc.), determining the timing and procedures for reassessing risks, and definitions of risk probability and impact.
        - The only output is a Risk Management Plan.
    - Identify Risks
        - This is where the value is created. A good list of potential risks to a project's cost, schedule, or any other critical success factor is the key to great risk management.
        - Inputs
            - Project management plan
            - Project documents
            - Agreements
            - Procurement documentation
            - Enterprise environmental factors
            - Organizational process assets
        - Outputs
            - Risk register
            - Risk report
            - Project documents updates
    - Perform Qualitative Risk Analysis
        - Each risk on the risk register is analyzed and a ranking assigned to the two underlying variables probability of occurrence, and impact. Overall risk priority ranking is found (by multiplication of the two rankings).
        - Inputs
            - Project management plan
            - Project documents
            - Enterprise environmental factors
            - Organizational process assets
        - Output
            - Project documents updates
    - Perform Quantitative Risk Analysis

CYBRARY

        - Using the risk priorities established during the previous Qualitative Risk Analysis step, the impact on the project's schedule and budget are determined.
        - Inputs
            - Project management plan
            - Project documents
            - Enterprise environmental factors
            - Organizational process assets
        - Output
            - Project documents updates
    - Plan Risk Responses
        - In this process you take the most important risks to the project and create an action plan, not just for responding to the risk if it happens, but for monitoring the risk triggers so you have the earliest possible warning.
        - Inputs
            - Project management plan
            - Project documents
            - Enterprise environmental factors
            - Organizational process assets
        - Outputs
            - Change requests
            - Project management plan updates
            - Project documents updates
    - Implement Risk Responses
        - When a risk event is triggered, the response plan springs into action.
        - Inputs
            - Project management plan
            - Project documents
            - Organizational process assets
        - Outputs
            - Change requests
            - Project documents updates
        -
    - Monitor Risks

CYBRARY

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Throughout the project, the risk register is monitored to ensure the analysis remains current. Risk priorities can change as many things can happen throughout a project that change the risk profile (probability, impact) of each risk.
  - Inputs
    - Project management plan
    - Project documents
    - Work performance data
    - Work performance reports
  - Outputs
    - Work performance information
    - Change requests
    - Project management plan updates
    - Project documents updates
    - Organizational process assets updates

- Every process listed above had their inputs as well as outputs. Inputs can be interview, plan, documents, output from other process etc. One of the biggest and most important documents is Risk register. Central repository for information about risk, used to communicate with stakeholders.

Lesson 2.7: ISACA's Framework and Lifecycle
Skills Learned From This Lesson: ISACA, Risk, Framework, IT Governance

- Purpose of the ISACA Risk IT Framework - Management of business risk is an essential component of the responsible administration of any enterprise. Almost every business decision requires the executive or manager to balance risk and reward.
- Benefits and outcome:
  - Accurate view on current and near-future IT-related events.
  - End-to-end guidance on how to manage IT-related risks.
  - Understanding of how to capitalise on the investment made in an IT internal control system already in place Integration with the overall risk and compliance structures within the enterprise.
  - Common language to help manage the relationships Promotion of risk ownership throughout the organisation

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- The Risk IT framework consists of:
    - **Risk Governance (RG)** Ensure that IT risk management practices are embedded in the enterprise, enabling the enterprise to secure optimal risk-adjusted return.
        - RG1 Establish and maintain a common risk view
        - RG2 Integrate with ERM
        - RG3 Make risk-aware business decisions
    - **Risk Evaluation (RE)** Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.
        - RE1 Collect data
        - RE2 Analyse risk
        - RE3 Maintain risk profile
    - **Risk Response (RR)** Ensure that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.
        - RR1 Articulate risk
        - RR2 Manage risk
        - RR3 React to events
- ISACA's Risk Management Life Cycle
    - Cyclical process
    - Process based on the complete cycle of all elements
    - Continuous process with refinement, adaptation and improvement

CYBRARY

Lesson 2.8: Review Questions

Skills Learned From This Lesson: RISK, Exam, Question

-
-

Module 3: Risk Identification

Lesson 3.1: Risk Identification Intro

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

Skills Learned From This Lesson: ISO, ISO/IEC 27005, Frameworks, NIST, SP 800-39, SP 800-30, SP 800-37, Culture, Risk Register, Domain 1.

- Domain 1 - Risk Identification Agenda
- International Organization for Standardization (ISO) They develop and publish international standards. ISO creates documents that provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose.
    - ISO 27005 is the international standard that describes how to conduct an information security risk assessment in accordance with the requirements of ISO 27001.
    - Risk assessments are one of the most important parts of an organisation’s ISO 27001 compliance project. ISO 27001 requires you to demonstrate evidence of information security risk management, risk actions taken and how relevant controls from Annex A have been applied.
- ISO 27005 is applicable to all organisations, regardless of size or sector. It supports the general concepts specified in ISO 27001, and is designed to assist the satisfactory implementation of information security based on a risk management approach.
- Content of the standard ISO/IEC 27005:2018 (latest version published in 2018)
    - The standard doesn't specify, recommend or even name any specific risk management method. It does however imply a continual process consisting of a structured sequence of activities, some of which are iterative:
    - Establish the risk management context (e.g. the scope, compliance obligations, approaches/methods to be used and relevant policies and criteria such as the organization’s risk tolerance or appetite);
    - Quantitatively or qualitatively assess (i.e. identify, analyze and evaluate) relevant information risks, taking into account the information assets, threats, existing controls and vulnerabilities to determine the likelihood of incidents or incident scenarios, and the predicted business consequences if they were to occur, to determine a ‘level of risk’;
    - Treat (i.e. modify [use information security controls], retain [accept], avoid and/or share [with third parties]) the risks appropriately, using those ‘levels of risk’ to prioritize them;
    - Keep stakeholders informed throughout the process; and

CYBRARY

    - Monitor and review risks, risk treatments, obligations and criteria on an ongoing basis, identifying and responding appropriately to significant changes.
- ISACA Risk IT Framework (Covered in Lesson 2.7: ISACA's Framework and Lifecycle)
- The National Institute of Standards and Technology (NIST) is a physical science laboratory, and a non-regulatory agency of the United States Department of Commerce. Its mission is to promote innovation and industrial competitiveness. NIST's activities are organized into laboratory programs that include nanoscale science and technology, engineering, information technology, neutron research, material measurement, and physical measurement.
    - NIST's cybersecurity programs seek to enable greater development and application of practical, innovative security technologies and methodologies that enhance the country's ability to address current and future computer and information security challenges.
- The purpose of **Special Publication 800-39** is to provide guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems. Special Publication 800-39 provides a structured, yet flexible approach for managing information security risk that is intentionally broad-based, with the specific details of assessing, responding to, and monitoring risk on an ongoing basis provided by other supporting NIST security standards and guidelines. The guidance provided in this publication is not intended to replace or subsume other risk-related activities, programs, processes, or approaches that organizations have implemented. Rather, the information security risk management guidance described herein is complementary to and can be used as part of a more comprehensive Enterprise Risk Management (ERM) program.
- The purpose of **Special Publication 800-30** rev 1 is to provide guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39. Risk assessments, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process—providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks.
- **Special Publication 800-37 rev 1 and 2** describes the Risk Management Framework (RMF) and provides guidelines for applying the RMF to information systems and

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

organizations. The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.

- Risk Culture - remember “fish stinks from the head”.

Lesson 3.2: ISO 270005 Framework

Skills Learned From This Lesson: Risk Identification, Risk Estimation, Risk Evaluation, Risk Response.

- Unlike ISO 31000:2018 Risk Management Guidelines, which were written to be easily understood by top executives and board directors, the ISO 27005:2018 is longer, denser and more technically targeted to chief information security officers (CISOs), chief risk officers and auditors. It emphasizes the importance of a systematic approach to developing and maintaining an information security risk management (ISRM) process — and reminds stakeholders that risk management must be continual and subject to regular review to ensure continued effectiveness.
- Although ISO 27005 does not specify any specific risk management methodology, it does imply a continual information risk management process based on six key components:
- 1. **Context establishment:** The risk management context sets the criteria for how risks are identified, who is responsible for risk ownership, how risks impact the confidentiality, integrity and availability of the information, and how risk impact and likelihood are calculated.
- 2. **Risk assessment:** Many organisations choose to follow an asset-based risk assessment process comprising five key stages:

  I. Compiling information assets.
  II. Identifying the threats and vulnerabilities applicable to each asset.
  III. Assigning impact and likelihood values based on risk criteria.
  IV. Evaluating each risk against predetermined levels of acceptability.
  V. Prioritising which risks need to be addressed, and in which order.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- 3. **Risk treatment:** There are four ways to treat a risk:

  I. ‘Avoid’ the risk by eliminating it entirely.
  II. ‘Modify’ the risk by applying security controls.
  III. ‘Share’ the risk with a third party (through insurance or outsourcing).
  IV. ‘Retain’ the risk (if the risk falls within established risk acceptance criteria).

- 4. **Risk acceptance:** Organisations should determine their own criteria for risk acceptance that consider existing policies, goals, objectives and shareholder interests.
- 5. **Risk communication and consultation:** Effective communication is pivotal to the information security risk management process. It ensures that those responsible for implementing risk management understand the basis on which decisions are made, and why certain actions are required. Sharing and exchanging information about risk also facilitates agreement between decision makers and other stakeholders on how to manage risk.
  - Risk communication activity should be performed continually, and organisations should develop risk communication plans for normal operations as well as emergency situations.
- 6. **Risk monitoring and review:** Risks are not static and can change abruptly. Therefore, they should be continually monitored in order to quickly identify changes and maintain a complete overview of the risk picture.
- While the ISO 27005:2018 outlines both the “what” and the “how” of a risk management process, it avoids doing so narrowly or prescriptively. Although it defines a systematic and cyclical process where inputs, actions and outputs are well-defined at each step, the ISO 27005:2018 leaves a lot of room for the organization to customize its own procedures to produce value regardless of its size, sector, regulatory environment or geographic location.
- By developing a structured ISRM process and carefully and continually reviewing it with stakeholders, any organization can ensure that its risk appetite is aligned to its culture, business objectives and strategies, especially in the face of changing market conditions and regulations.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

Lesson 3.3: NIST 800-39 Risk Framing
Skills Learned From This Lesson: risk management, security, risk assessment, roles, responsibilities, organization, mission, information system

- The purpose of Special Publication 800-39 is to provide guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems. Special Publication 800-39 provides a structured, yet flexible approach for managing risk that is intentionally broad-based, with the specific details of assessing, responding to, and monitoring risk on an ongoing basis provided by other supporting NIST security standards and guidelines.
- Managing risk is a complex, multifaceted activity that requires the involvement of the entire organization—from senior leaders/executives providing the strategic vision and top-level goals and objectives for the organization; to mid-level leaders planning, executing, and managing projects; to individuals on the front lines operating the information systems supporting the organization’s missions/business functions.
- Risk management is a comprehensive process that requires organizations to:
  - frame risk (i.e., **establish the context** for risk-based decisions);
  - assess risk;
  - respond to risk once determined; and
  - monitor risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations.
- The first component of risk management addresses how organizations frame risk or establish a risk context—that is, describing the environment in which risk-based decisions are made. The purpose of the risk framing component is to produce a risk management strategy that addresses how organizations intend to assess risk, respond to risk, and monitor risk—making explicit and transparent the risk perceptions that organizations routinely use in making both investment and operational decisions. The risk frame establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations.
- Establishing a realistic and credible risk frame requires that organizations identify:

CYBRARY

- ○ Risk assumptions (e.g., assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time);
- ○ Risk constraints (e.g., constraints on the risk assessment, response, and monitoring alternatives under consideration);
- ○ Risk tolerance (e.g., levels of risk, types of risk, and degree of risk uncertainty that are acceptable); and
- ○ Priorities and trade-offs

-

Lesson 3.4: NIST 800-39 Risk Assessment
Skills Learned From This Lesson: Assessment, Framework, Monitor, Response

- The second component of risk management addresses how organizations assess risk within the context of the organizational risk frame. The purpose of the risk assessment component is to identify:
  - ○ Threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation;
  - ○ Vulnerabilities internal and external to organizations;
  - ○ The harm (i.e., consequences/impact) to organizations that may occur given the potential for threats exploiting vulnerabilities; and
  - ○ The likelihood that harm will occur.
- The end result is a determination of risk (i.e., the degree of harm and likelihood of harm occurring).
- Additional framework described in special publication 800-30 rev 1, cover risk assessment.
-

Lesson 3.5: NIST 800-39 Risk Response
Skills Learned From This Lesson: Skill, Skill, Skill

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- The third component of risk management addresses how organizations respond to risk once that risk is determined based on the results of risk assessments.
- The purpose of the risk response component is to provide a consistent, organization-wide, response to risk in accordance with the organizational risk frame by:
    - Developing alternative courses of action for responding to risk;
    - Evaluating the alternative courses of action;
    - Determining appropriate courses of action consistent with organizational risk tolerance; and
    - Implementing risk responses based on selected courses of action.
- To support the risk response component, organizations describe the types of risk responses that can be implemented (i.e., accepting, avoiding, mitigating, sharing, or transferring risk).

Lesson 3.6: NIST 800-39 Risk Monitoring
Skills Learned From This Lesson: Monitoring, Legislation, Effectiveness, Major change, KRI, KPI

- The fourth component of risk management addresses how organizations monitor risk over time.
- The purpose of the risk monitoring component is to:
    - Verify that planned risk response measures are implemented and information security requirements derived from/traceable to organizational missions/business functions, federal legislation, directives, regulations, policies, and standards, and guidelines, are satisfied;
    - Determine the ongoing effectiveness of risk response measures following implementation; and
    - Identify risk-impacting changes to organizational information systems and the environments in which the systems operate.
- To support the risk monitoring component, organizations describe how compliance is verified and how the ongoing effectiveness of risk responses is determined (e.g., the types of tools, techniques, and methodologies used to determine the sufficiency/correctness of risk responses and if risk mitigation measures are

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

implemented correctly, operating as intended, and producing the desired effect with regard to reducing risk). In addition, organizations describe how changes that may impact the ongoing effectiveness of risk responses are monitored.

- KRI - Key Risk Indicators (KRIs), as the name suggests, measure risk. KRIs are used by organisations to determine how much risk they are exposed to or how risky a particular venture or activity is.
- KPI- Key Performance Indicators (KPIs) are the gauges and measurements an organisation uses to understand how well individuals, business units, projects and companies are performing against their strategic goals.
- While KPIs help organisations understand how well they are doing in relation to their strategic plans, KRIs help them understand the risks involved and the likelihood of not delivering good outcomes in the future. This means KRIs can be the flipside or KPIs.
- KPIs and KRIs are not the same. KRIs help to quantify risks, while KPIs help to measure business performance.

Lesson 3.7: NIST 800-30 Intro !!! NOTE !!! First 35 seconds are without sound or picture !!! Note!!!
Skills Learned From This Lesson: NIST 800-39, Revision 1, Assessment, Framework, Threats, Vulnerabilities, Impact.
The purpose of Special Publication 800-30 is to provide guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39. Risk assessments, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process—providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks.

- The purpose of risk assessment is to inform decision makers, stakeholders and support risk responses by identifying:
- Threats to organization

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

  - A threat is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.
- Vulnerabilities
  - A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.
- Impact
  - The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
- Risk assessments can be conducted at all three tiers in the risk management hierarchy—including Tier 1 (organization level), Tier 2 (mission/business process level), and Tier 3 (information system level).

Lesson 3.8: NIST 800-30 Risk Assessment Methodology
Skills Learned From This Lesson: Frame Risk, Quantitative, Qualitative, Semi-qualitative,

- NIST 800-39 guide us through fundamental concepts associated with managing information security risk across an organization. Comprehensive process requires organizations to:
  - frame risk
  - assess risk
  - respond to risk once determined
  - monitor risk
- NIST 800-30 provide guidance on Assessment Risk and methodology used for it.
- A risk assessment methodology typically includes:
  - A risk assessment process
  - An explicit risk model
  - An assessment approach specifying the range of values those risk factors can assume during the risk assessment and how combinations of risk factors are

CYBRARY

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

identified/analyzed so that values of those factors can be functionally combined to evaluate risk. Assessment types are:

- Quantitative
  - Quantitative assessments typically employ a set of methods, principles, or rules for assessing risk based on the use of numbers—where the meanings and proportionality of values are maintained inside and outside the context of the assessment.
- Qualitative
  - Qualitative assessments typically employ a set of methods, principles, or rules for assessing risk based on nonnumerical categories or levels (e.g., very low, low, moderate, high, very high). This type of assessment supports communicating risk results to decision makers.
- Semi-qualitative,
  - semi-quantitative assessments typically employ a set of methods, principles, or rules for assessing risk that uses bins, scales, or representative numbers whose values and meanings are not maintained in other contexts. This type of assessment can provide the benefits of quantitative and qualitative assessments.

○ An analysis approach

- Threat-oriented
  - A threat-oriented approach starts with the identification of threat sources and threat events, and focuses on the development of threat scenarios.
- asset/impact-oriented
  - An asset/impact-oriented approach starts with the identification of impacts or consequences of concern and critical assets, possibly using the results of a mission or business impact analyses and identifying threat events that could lead to and/or threat sources that could seek those impacts or consequences.
- vulnerability-oriented, describing how combinations of risk factors are identified/analyzed to ensure adequate coverage of the problem space at a consistent level of detail.

CYBRARY

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Risk assessment component of risk management—provide a step-by-step process for organizations on:
  - How to prepare for risk assessments
  - How to conduct risk assessments
  - How to communicate risk assessment results to key organizational personnel
  - How to maintain the risk assessments over time.

Lesson 3.9: NIST 800-37 Revision 1 and Revision 2
Skills Learned From This Lesson: NIST 800-37, Risk Management Framework (RMF), revision 1, Federal Information Systems,

- This publication describes the Risk Management Framework (RMF) and provides guidelines for applying the RMF to information systems and organizations.
- The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.
- First question when you start with Risk Management should be “What I should be protecting ?” and tools can help us in this process is FIPS 199. Determine what kind of assets, what kind of information is on those systems - help us to select the appropriate controls to protect the assets.
  - Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document).
  - Tool for selecting controls should be always FIPS 200, depend on categorisation of the assets we can use control, from FIPS 200.
  - Security controls for the information system should be documented in the security plan.
- Implementation of the security controls specified in the security plan is our next step. Security control implementation is consistent with the organization’s enterprise architecture and information security architecture.

Assess security controls - Develop, review, and approve a plan to assess the security controls.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- The security assessment plan provides the objectives for the security control assessment, a detailed roadmap of how to conduct such an assessment, and assessment procedures. The assessment plan reflects the type of assessment the organization is conducting.

Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.

- Security control assessments determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system.

Authorisation step require preparation plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.

- The plan of action and milestones, prepared for the authorizing official by the information system owner or common control provider, is one of three key documents in the security authorization package and describes the specific tasks that are planned:
  - To correct any weaknesses or deficiencies in the security controls noted during the assessment;
  - To address the residual vulnerabilities in the information system.
- The security authorization package contains:
  - The security plan;
  - The security assessment report
  - The plan of action and milestones.
- The information in these key documents is used by authorizing officials to make risk-based authorization decisions.
- Last step in Security life cycle is monitoring. Information systems are in a constant state of change with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the systems reside and operate. A disciplined and structured approach to managing, controlling, and documenting changes to an

CYBRARY

information system or its environment of operation is an essential element of an effective security control monitoring program.

NIST 800-37 Revision 2 (December 2018) - Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy

There are seven steps in the RMF; a preparatory step to ensure that organizations are ready to execute the process and six main steps. All seven steps are essential for the successful execution of the RMF. The steps are:

- Prepare to execute the RMF from an organization- and a system-level perspective by establishing a context and priorities for managing security and privacy risk.
- Categorize the system and the information processed, stored, and transmitted by the system based on an analysis of the impact of loss.
- Select an initial set of controls for the system and tailor the controls as needed to reduce risk to an acceptable level based on an assessment of risk.
- Implement the controls and describe how the controls are employed within the system and its environment of operation.
- Assess the controls to determine if the controls are implemented correctly, operating as intended, and producing the desired outcomes with respect to satisfying the security and privacy requirements.
- Authorize the system or common controls based on a determination that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable.
- Monitor the system and the associated controls on an ongoing basis to include assessing control effectiveness, documenting changes to the system and environment of operation, conducting risk assessments and impact analyses, and reporting the security and privacy posture of the system.

Lesson 3.10: Alignment with the Business
Skills Learned From This Lesson: Buy-in, RACI, Goals, Objectives

- The purpose of Information security is to support the business, to bring value for the business.
- IT Risk measured by impact of the risk on business operations.
- Buy-in of senior management :
    - Risk management
    - Provide budget, authority and access needed
    - Support from senior management should be visible and active
- Alignment with Business Goals and Objectives (it's no matter fact are you going just for certification or to work in an organization-you should understand context of organization)
- Communicate with senior management about:
    - Vision and strategy
    - Lines of business, new technology, future growth, changes in priorities
- Ensure risk is aligned with and integrated into strategy, vision and direction.
- The Risk practitioner should seek to :
    - Understand the business
    - Listen to the strategy
    - Proactively seek out ways to secure new technologies and business process
    - Build relationships and communication infrastructure to weave risk management into each business process and new projects
    - Be aware of and mitigate the risk of change
    - Work to create a culture that encourages participation of risk management into business process
    - Understand past events
    -
- In order to effectively support the organization is to have a set of clearly defined set of roles and responsibility.
- A RACI chart is a simple matrix used to assign roles and responsibilities for each task, milestone, or decision on a project.
- RACI stands for Responsible, Accountable, Consulted, Informed. Each letter in the acronym represents a level of task responsibility.
    - Responsible: This team member does the work to complete the task.
    - Accountable: This person delegates work and is the last one to review the task or deliverable before it's deemed complete.

CYBRARY

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Consulted: Every deliverable is strengthened by review and consultation from more than one team member. Consulted parties are typically the people who provide input based on either how it will impact their future project work or their domain of expertise on the deliverable itself.
- Informed: These team members simply need to be kept in the loop on project progress, rather than roped into the details of every deliverable.

Three Lines of Defense - 3LoD

In order to design an efficient risk management system, the processes used to control the company risks should be interconnected in a holistic system.

- Notes

1. The first layer of defense- Management Control / Ownership:

The first layer of defense is implemented by the unit, component or business function that performs daily operation activities, especially those that are the front lines of the organization. In this case they are expected to:

- Note
- Ensure the conductive control environment in their business unit.
- Implement risk management policies on their roles and responsibilities, especially in activities that lead to corporate growth. They are expected to be fully aware of the risk factors that should be considered in every decision and action.
- Be able to execute effective internal control in their business units, as well as the monitoring process and maintaining transparency in the internal control itself.

2. Second-tier defense - Risk Management

The second layer of defense is executed by risk management and compliance functions, especially in structured risk management and compliance units e.g. department or risk management and compliance units. In this case, they are expected to:

- Note
- Be responsible for risk management development, monitoring process and the implementation of the company's overall risk management.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Monitor and ensure that all business functions being implemented in accordance with risk management policies and standard operating procedures that have been established by the company.
- Monitor and report to the department with the highest accountability on complete company's exposure to risks.

3. Third-tier defense Assurance / Internal Audit
The third layer of defense is implemented by both auditors and internal auditors the external auditor. Role of the internal auditor is much more intense in this 3LD models because they are part of the company that is independent by design. In this case, the internal auditors are expected to:

- Note
- Review and evaluation of the design and implementation of risk management holistically.
- Ensure the effectiveness of the first layer of defense and the second-tier.

Lesson 3.11: Risk Culture
Skills Learned From This Lesson: Risk Culture, Risk Communication, Skill, Skill, Skill

- Risk culture is a system of values and behaviors present in an organization that shape risk decisions of management and employees. One element of risk culture is a common understanding of an organization and its business purpose. Employees must also understand that risk and compliance rules apply to everyone as they work towards business goals.

- Risk Communication - Risk communication is the interactive exchange of information about risks among risk assessors, managers, news media, interested groups, and the general public.
- The main purpose of communicating risks is to inform people about the potential hazards related to a particular condition or activity. These hazards may be directly linked to a

Brought to you by:
CYBRARY | FOR BUSINESS
*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

person, community or property. It involves a two-way exchange of information between the parties likely to be affected

- Communicating risks enables managers and the team members to determine the probability of a risk materializing and its possible impacts. It allows analysts to understand the difference between risks and hazards found in a particular area.
- Sarah Tennyson: “Enterprise-wide risk management requires a shift in the behaviour and mindset of employees across an organization. To realize the full benefits of improved systems, tools, and analytical skills, people need to learn new ways of perceiving situations, interpreting data, making decisions, influencing, and negotiating”

CYBRARY

Lesson 3.12: Roles and Responsibilities
Skills Learned From This Lesson: Risk Prioritization, Risk Practitioner, Risk Roles, Responsibility, Chief Risk Officer (CRO)

- Risk Prioritization - A Risk Analysis may identify a number of risks that appear to be of similar ranking or severity. When too many risks are clustered at or about the same level, a method is needed to prioritize risk responses and where to apply limited resources. In order to prioritize risk following parameters should be considered:
  - Cost of the response to reduce risk with tolerance levels
  - Capability to implement response (usually refer to limited resources)
  - Effectiveness and efficiency of the response
- Risk Roles and Responsibility - Recognizing that organizations have varying missions, business functions, and organizational structures, there may be differences in naming conventions for risk management roles and how risk management responsibilities are allocated among organizational personnel. However, the basic functions remain the same:
  - CIO - is a job title commonly given to the most senior executive in an enterprise who works with information technology and computer systems, in order to support enterprise goals. Primary focus is **value delivery**.
  - Business management - The individuals with the business with roles related to managing a program. Typically **accountable** for analyzing risks, maintaining risk profile and risk-aware decisions.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

  - Chief Risk Officer (CRO) - is the executive-level manager **responsible** for maintaining risk, analyzing risk, maintaining risk profile and risk aware decisions.
  - CRO responsibilities include:
    - Managing the risk assessment process
    - Implementation of corrective actions
    - Communicate risk management issues
    - Supporting the risk management functions
- Risk Practitioner - responsibility:
  - Develop, maintain, manage and execute a comprehensive process for identifying, assessing, mitigating, monitoring and reporting on risk that may impact on organizational performance.
  - Define Key Risk Identificator (KRI)
  - Report trends on risk profile to management to aid in decision making
  - Identify Key Performance Indicator (KPI)
  - Analyze performance indicator to determine the effectiveness of the control environment
  - Report performance on control environment to management to aid in decision making

Lesson 3.13: The Risk Register
Skills Learned From This Lesson: Risk register, Risk Awareness ProgramSkill

- A risk register is a listing of all risk identified for the enterprise.
- The risk register records:
  - All known risk
  - Priorities of risk
  - Likelihood of risk
  - Potential risk impact
  - Status of the risk mitigation plans
  - Contingency plans
  - Ownership of risk
- The purpose of a risk register is to consolidate risk data into one place and permit the tracking of risk.

CYBRARY

- The risk register allows management to refer to a single document to do the following:
  - Gain insight into the outstanding risk issues.
  - Learn about the status of risk mitigation efforts.
  - Become aware of the emergence of newly identified and documented risk
- The risk register contains all risk detected by various departments or activities of the organization, including the following:
  - Risk identified in audits
  - Vulnerability assessments
  - Penetration tests
  - Incident reports
  - Process reviews
  - Management input
  - Risk scenario creation
  - Security assessments

- Risk awareness is about acknowledging that risk is an integral part of the business. This does not imply that all risks are to be avoided or eliminated, but rather that they are well understood and known, IT risk issues are identifiable, and the enterprise recognises and uses the means to manage them.
- The Risk Awareness Program:
  - Creates understanding of risk, risk factors and types of risk
  - Should be tailored to the needs of the groups within an organization
  - Should not disclose vulnerabilities or ongoing investigations
- Can server to mitigate risk through education on policy and procedure

CYBRARY

Lesson 3.14: Risk Scenarios
Skills Learned From This Lesson: Skill, Skill, Skill

- A risk scenario is a description of a possible event whose occurrence will have an uncertain impact on the achievement of the enterprise’s objectives.
- Risk scenario development provides a way of conceptualizing risk useful in the process of risk identification.

- Risk scenarios are also used to document risk in relation to business objectives or operations impacted by events, making them useful as the basis for quantitative risk assessment.
- Risk scenario is a technique used to make risk more concrete and tangible and allow for proper :
    - Bring realism
    - Provide insight
    - Awareness
    - Facilitate organizational engagement
    - Provide a tool to facilitate communication
    - Enhance risk management effort
    - Provide realistic view of risk
- Risk scenario is characterized by:
    - Threat actor that can be:
        - Internal to the organization (employee, contractor)
        - External to the organization (competitor, business partner, regulator, act of god)
    - Threat type:
        - Malicious,
        - Accidental,
        - Failure,
        - Natural,
    - Event
        - Disclosure,
        - Modification
        - Theft
        - Destruction
        - Bad design
        - Ineffective execution
        - Inappropriate use
    - Asset or Resource
        - People and organization
        - Process
        - Infrastructure or facilities

CYBRARY

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

        - IT infrastructure
        - Information
        - Application
    - Time
        - Duration
        - Timing of occurrence (critical or not)
        - Timing to detect
        - Timing to react
- Risk Scenario - Event
    - Events - can be categorised along the vector which they affect:
        - Loss Events
            - Events generating the negative impact.
        - Vulnerability Events
            - Events contributing to the magnitude or frequency of loss events occuring.
        - Threat Events
            - Circumstances or events that can trigger loss events
- Risk scenarios may be derived via two different mechanisms:
    - **Top-down approach**: From the overall business objectives, an analysis of the most relevant and probable IT risk scenarios impacting the business objectives is performed. If the impact criteria are well aligned with the real value drivers of the enterprise, relevant risk scenarios will be developed.
    - **Bottom-up approach**: A list of generic scenarios is used to define a set of more concrete and customized scenarios, which are then applied to the individual enterprise situation.
- Risk scenario development is based on:
    - Describing a potential risk event
    - Documenting the factors and areas that may be affected by the risk event
    - Each scenario should be related to a business objective or impact.
    - Effective scenarios must focus on real and relevant potential risk events.

Lesson 3.15: Hardware and Software Risks

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

CYBRARY

Skills Learned From This Lesson: Hardware risk, Software risk, SDLC,

- Hardware risk associated with:
  - Outdated hardware
  - Poorly maintained hardware
  - Misconfiguration hardware
  - Poor architecture
  - Lack of documentation
  - Lost, misplaced or stolen hardware
  - Hardware that is not discarded in a secure manner
  - Sniffing or capturing traffic
  - Physical access
  - Hardware failure
  - Unauthorized hardware
  - Notes
- Software Risk
  - Software Development Life Cycle (SDLC), also referred to as the application development life-cycle, is a process for planning, creating, testing, and deploying an information system.
- Phases in SDLC
- Software associated risks:
  - Poor or no data validation
  - Exposure of sensitive data
  - Improper modification of data
  - Logic flaws
  - Software bugs
  - Lack of logs
  - Lack of version control
  - Loss of source code
  - Weak or lack of access control
  - Lack of operability with other software
  - Back doors
  - Poor coding practices ...

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

Lesson 3.16: Network Risks
Skills Learned From This Lesson: Network, Monitor, Components, Architecture Skill, Skill, Skill

- Risk associated with network:
  - Network configuration and management
  - Network equipment protection
  - Layered defence
  - Redundancy
  - Bandwidth
  - Usage of encryption for transmission of sensitive data
  - Encryption key management
  - Documentation of network architecture …
- Risk associated with Network Components
  - Firewall
  - Router
  - Proxy
  - DNS
  - Switch
- Risk associated with Network Architecture
  - Local Area Network (LAN)
  - Wide Area Network (WAN)
  - Virtual Area Network (VPN)
  - Demilitarized zone (DMZ)
  - Extranet
  - User Interface
- Risk associated with utilities
  - Environmental utilities
    - Power interruptions
      - Losses
      - Generators
      - Batteries
    - HVAC
    - Water

CYBRARY

        - Secure operational
- Risk associated with Software utilities
    - Use of outdated drivers
    - Unavailability of drivers
    - Use of insecure components
    - Unpatched vulnerabilities

In the world of informational security threats come from all different directions !!

Lesson 3.17: Emerging Risks
Skills Learned From This Lesson: Emerging risks, IT assessment, Threats, Vulnerabilities

- New Threats and Vulnerabilities
    - Risk environment constantly changes
    - Work with owners do determine responses.
    - Ensure that new threats and vulnerabilities are evaluating during IT risk assessment.
        - Employees
        - Contractors
        - Business partners
        - CyberCriminals
        - Nation state-sponsored attackers
        - Competition sponsored attackers
        - Hacktivist
        - Other ..still unknown

Lesson 3.18: 3rd Party Risks
Skills Learned From This Lesson: Outsourcing, Service Level Agreement (SLA)

- Third-Party Management - Third-party management is the process whereby companies monitor and manage interactions with all external parties with which it has a relationship.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Third-Party comes in all colors, shapes and flavours, starting from hardware, software, Internet Provider Services, Cloud services, etc …The importance of having a complete list of all third parties of an enterprise cannot be overstated. Keeping that in mind an enterprise must identify potential threats and vulnerabilities introduced through relationships with all third parties. This has become especially important given the continued growth of outsourcing and offshoring, along with the increased scrutiny being placed on third parties by regulators.

Module 4: Risk Assessment
Lesson 4.1: Risk Assessment Intro
Skills Learned From This Lesson: Risk Assessment, Risk Identification, Risk scenario

- Domain 2 - Risk Identification Agenda -Exam Relevance
  - IT Risk Assessment 28% - (approximately 2 questions)
- Analyze and evaluate IT risk to determine the likelihood and impact on business objectives to enable risk-based decision making.
  - 2.1 Analyze risk scenarios based on organizational criteria (e.g., organizational structure, policies, standards, technology, architecture, controls) to determine the likelihood and impact of an identified risk.
  - 2.2 Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation.
  - 2.3 Review the results of risk and control analysis to assess any gaps between current and desired states of the IT risk environment.
  - 2.4 Ensure that risk ownership is assigned at the appropriate level to establish clear lines of accountability.
  - 2.5 Communicate the results of risk assessments to senior management and appropriate stakeholders to enable risk-based decision making.
  - 2.6 Update the risk register with the results of the risk assessment.
- Learning Objectives:
  - Identify and apply risk assessment techniques
  - Analyze risk scenarios
  - Identify current state of controls
  - Assess gaps between current and desired states of the IT risk environment

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Communicate IT risk assessments result to relevant stakeholders
- Risk Identification
    - The process of determining and documenting the risk that an enterprise faces
    - Documentation of assets and their value
- Risk Assessment
    - A process used to identify and evaluate risk and its potential effects
    - Assessing critical functions and defining controls in place

Lesson 4.2: Tools and Techniques Part 1

Skills Learned From This Lesson: Tools, Techniques, Bowtie, Decision tree, Skill, skill skill

- Technique used in Risk assessment :
    - Bow tie Analysis
    - Decision Tree Analysis
    - Cause and Effect Analysis
    - Business Impact Analysis (BIA)
    - Strength Weakness Opportunity Threats (SWOT) Analysis
    - Boston Consulting Group Matrix (BCG)
- BOWTIE Analysis - A 'bowtie' is a diagram that visualizes the risk you are dealing with in just one, easy to understand the picture. Bowtie Analysis taking into account:
    - Causes
    - Control Measures (Prevention / Proactive)
    - Risk / Hazard
    - Recovery Measures (Mitigation / Reactive)
    - Consequences
- Decision Tree Analysis For Expected Monetary Value (EMV) -A decision tree is a flowchart-like structure in which each internal node represents a "test" on an attribute (e.g. whether a coin flip comes up heads or tails), each branch represents the outcome of the test, and each leaf node represents a class label (decision taken after computing all attributes). The paths from root to leaf represent classification rules.
- A decision tree consists of three types of nodes:
- Decision nodes – typically represented by squares
- Chance nodes – typically represented by circles

CYBRARY

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- End nodes – typically represented by triangles

Lesson 4.3: Tools and Techniques Part 2
Skills Learned From This Lesson: Cause and effect, Fishbone, Ishakawa,

- Cause and effect (fishbone or Ishikawa)
    - Ishikawa diagrams (also called fishbone diagrams, herringbone diagrams, cause-and-effect diagrams, or Fishikawa) are causal diagrams created by Kaoru Ishikawa that show the causes of a specific event.
    - The defect is shown as the fish's head, facing to the right, with the causes extending to the left as fishbones; the ribs branch off the backbone for major causes, with sub-branches for root-causes, to as many levels as required

- Advantages
    - Highly visual brainstorming tool which can spark further examples of root causes
    - Quickly identify if the root cause is found multiple times in the same or different causal tree
    - Allows one to see all causes simultaneously
    - Good visualization for presenting issues to stakeholders
- Disadvantages
    - Complex defects might yield a lot of causes which might become visually cluttering
    - Interrelationships between causes are not easily identifiable

- SWOT Analysis - SWOT analysis (or SWOT matrix) is a strategic planning technique used to help a person or organization identify strengths, weaknesses, opportunities, and threats related to business competition or project planning.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Strengths and weakness are frequently internally-related, while opportunities and threats commonly focus on the external environment. The name is an acronym for the four parameters the technique examines:
    - Strengths: characteristics of the business or project that give it an advantage over others.
    - Weaknesses: characteristics of the business that place the business or project at a disadvantage relative to others.
    - Opportunities: elements in the environment that the business or project could exploit to its advantage.
    - Threats: elements in the environment that could cause trouble for the business or project.
- BCG Matrix - Boston Consulting Group - created to evaluate the strategic position of the business brand portfolio and its potential. (https://www.bcg.com)
- The growth share matrix was built on the logic that market leadership results in sustainable superior returns. Ultimately, the market leader obtains a self-reinforcing cost advantage that competitors find difficult to replicate. These high growth rates then signal which markets have the most growth potential.
    - Each of the four quadrants represents a specific combination of relative market share, and growth:
        - Low Growth, High Share. Companies should milk these “cash cows” for cash to reinvest.
        - High Growth, High Share. Companies should significantly invest in these “stars” as they have high future potential.
        - High Growth, Low Share. Companies should invest in or discard these “question marks,” depending on their chances of becoming stars.
        - Low Share, Low Growth. Companies should liquidate, divest, or reposition these “pets”

CYBRARY

Lesson 4.4: Business Impact Analysis
Skills Learned From This Lesson: Skill, skill skill

- Business impact analysis (BIA) is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency. Having that in mind you should:
    - Identifies and prioritizes all business
    - Determine and identify mission / business process and recovery criticality based on :
        - Impact of a system disruption to those critical systems
        - Determine outage impact and estimated downtime
    - Risk identification:
        - Internal vs 3rd Party
        - Probability and impact
    - Identity resource requirement to resume critical process soon as possible
    - Identify recovery priorities for system resources
- Business Impact Assessment Priorities :
    - Create In-depth list of business process and their impact on the organization, make sure that business process are always interconnected.
    - Often delegated to individual departments for accuracy and buy-in
    - Criticality is driven by the amount of lost the organization will suffer if the resource is unavailable.
    - MTD / MTO - Maximum Tolerable Downtime / Outage Maximum time that an enterprise can support processing in alternate mode.
    - RTO - The amount of time allowed for the recovery of a business function or resource after a disaster occurs.
    - RPO - Recovery Point Objective - Tolerance for data loss
    -
- Business impact analysis document (template) should have:
    - Business Unit Name
    - Head Count - Number of full time staff in the business unit :
    - Parent Process - Brief description of the principal activities the unit performs, e.g. sales, contractor, interface
    - Priority Rank - Subjective ranking of parent process according to criticality to the business unit

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Recovery Time Objective - Timeline needed to recover the parent process work should be restored following a disruption.
- Recovery Point Objective - Point in time to which parent process work should be restored following a disruption
- Parent Process Depends On - Names of organization and/or processes the parent process needs for formal operations
- Parent Process required by - Names of organizations and / or process that need the sub-process for normal operations

Lesson 4.5: Controls Assessment
Skills Learned From This Lesson: Skill, skill skill

- After Business impact analysis, assessment controls already in place, should give us an overall picture about controls, and purpose of controls. Below we have usual ways to assess the controls:
    - Audits (internal or external)
    - Control tests - used to test one of more specific types of risk
    - Incident reports (follow up and lesson learn)
    - IT operation feedback
    - Logs: Valuable but underutilized
    - Media reports
- Risk Control Analysis
    - Threat and misuse case modeling
        - Misuse case modeling looks at all the possible errors, mistakes or ways a system can be misused
        - Threat modeling examines the ways a system can be attacked and used for the purpose for which the system was never intended
    - Root Cause analysis - Establish the origins of events (root cause) to learn from consequences
        - Pre-mortem: a facilitated workshop where the group is told to pretend that the project has failed and then they are to discuss why it has failed.

CYBRARY

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

Lesson 4.6: Stride Threat Modeling
Skills Learned From This Lesson: STRIDE, Threat, Software Development

- Threat Modeling - Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Escalation of Privilege.
- Used in software development - Risk assessment
- Tools for software threat modeling:
  - Microsoft Threat model tool (more on Microsoft web https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool)
  - OWASP Dragon (https://threatdragon.org)

Lesson 4.7: Gap Analysis
Skills Learned From This Lesson: Gap, Analysis, CMMI, CMU, maturity level

- In management literature, gap analysis involves the comparison of actual performance with potential or desired performance. Gap analysis identifies gaps between the optimized allocation and integration of the inputs (resources), and the current allocation-level.Gap analysis involves determining, documenting and improving the difference between business requirements and current capabilities.
- First step in Gap analysis should be determining business objectives and goals. Depending on objectives and goals, gap analysis should compare current state of risk, controls and try to improve current state.
- CMMI - Capability Maturity Model Integration (CMMI) is a process level improvement training and appraisal program. Administered by the CMMI Institute, a subsidiary of ISACA, it was developed at Carnegie Mellon University (CMU). It is required by many United States Department of Defense (DoD) and U.S. Government contracts, especially in software development. CMU claims CMMI can be used to guide process improvement across a project, division, or an entire organization. Version 2.0 was published in 2018. Web site of CMMI https://cmmiinstitute.com/
- CMMI defines the following maturity levels for processes:
  - Initial,

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Managed,
- Defined,
- Quantitatively Managed, and
- Optimizing

- Gap Analysis should track Key Indicators such as:
    - KPIs - Key Performance Indicators - A performance indicator or key performance indicator (KPI) is a type of performance measurement. KPIs evaluate the success of an organization or of a particular activity (such as projects, programs, products and other initiatives) in which it engages.
    - KRIs - Key Risk Indicators - A key risk indicator (KRI) is a measure used in management to indicate how risky an activity is. Key risk indicators are metrics used by organizations to provide an early signal of increasing risk exposures in various areas of the enterprise.
    - KGIs - Key Goal Indicators - a measure that tells management, after the fact, whether an IT process has achieved its business requirements and is usually expressed in terms of information criteria.

Lesson 4.8: Risk Analysis Methodologies
Skills Learned From This Lesson: Assessment, Quantitative, Qualitative

- Risk Assessment types are:
    - Quantitative
        - Quantitative assessments typically employ a set of methods, principles, or rules for assessing risk based on the use of numbers—where the meanings and proportionality of values are maintained inside and outside the context of the assessment.
            - More experience required than with Qualitative Assessment
            - Involves calculation to determine a dollar value associated with each risk event.
            - Business decisions are made on this type of analysis
            - Goal is to the dollar value of a risk and use that amount to determine what the best controls is for particular asset

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

        - Necessary for a cost benefit analysis.
    - Formulas and Terms:
        - (AV) -Asset Value - Dollar figure that represent what the asset is worth to the organization.
        - (EF) Exposure factor is the subjective, potential percentage of loss to a specific asset if a specific threat is realized.
        - (SLE) - Single-loss expectancy (SLE) is the monetary value expected from the occurrence of a risk on an asset. Computed using SLE = asset value x exposure factor.
        - (ARO) - Annual Rate of Occurrence - How often the threat is expected to materialize
        - (ALE) - The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE). It is mathematically expressed as: ARO = ALE * SLE
        - (TCO) - Total Cost of Ownership is total cost of implementing a safeguard. Often in addition to initial cost , there are ongoing maintenance as well.
        - (ROI) - Return of Investment - Amount of money saved by implementation of safeguard. Sometimes referred as the value of the safeguard / control.

CYBRARY

- Qualitative
    - Qualitative assessments typically employ a set of methods, principles, or rules for assessing risk based on nonnumerical categories or levels (e.g., very low, low, moderate, high, very high). This type of assessment supports communicating risk results to decision makers.
    -
- Semi-qualitative,

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

        - semi-quantitative assessments typically employ a set of methods, principles, or rules for assessing risk that uses bins, scales, or representative numbers whose values and meanings are not maintained in other contexts. This type of assessment can provide the benefits of quantitative and qualitative assessments.

Lesson 4.9: Risk Assessment Report
Skills Learned From This Lesson: Report, IT Risk, Skill, skill skill

- The report which contains the results of performing a risk assessment or the formal output from the process of assessing risk.
- Result of risk assessment should indicate gaps between current risk state and desired state
- Risk assessment report should provide management documentation of risk along with recommendations for addressing any outstanding risk issues
    - Justifiable and linked with the results of the risk assessment
    - Document process used and results of the risk assessment
    - State risk level and priorities
- Each risk must be at a level in the organization where they can make necessary decisions and can be accountable
- Ownership with an individual is needed for accountability
- IT RISK Assessment Report include:
    - Objectives of the risk assessment process
    - Scope and description of the area subject to assessment
    - External context and factors affecting risk assessment
    - Risk assessment criteria
    - Risk assessment methodology used
    - Resources and references used
    - Identification of risk, threats and vulnerabilities
    - Assumptions used in the risk assessment
    - Potential of unknown factors affecting assessment
    - Result of risk assessment
    - Recommendations and conclusions

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Communicating the IT Risk Assessment Results
  - Results should be compiled into a report to senior management (try to avoid technical terms and use only management terms if it's possible)
  - Report should list all risk (risk register) along with severity and owner
  - Provide *recommendation* on what action to take

Module 5: Risk Mitigation

Lesson 5.1: Risk Mitigation Reduction

Skills Learned From This Lesson: Risk response, Risk Mitigation

- Domain 3—Risk Response and Mitigation

Determine risk response options and evaluate their efficiency and effectiveness to manage risk in alignment with business objectives.
3.1 Consult with risk owners to select and align recommended risk responses with business objectives and enable informed risk decisions.
3.2 Consult with, or assist, risk owners on the development of risk action plans to ensure that plans include key elements (e.g., response, cost, target date).
3.3 Consult on the design and implementation or adjustment of mitigating controls to ensure that the risk is managed to an acceptable level.
3.4 Ensure that control ownership is assigned to establish clear lines of accountability.
3.5 Assist control owners in developing control procedures and documentation to enable efficient and effective control execution.
3.6 Update the risk register to reflect changes in risk and management's risk response.
3.7 Validate that risk responses have been executed according to the risk action plans.

- Aligning Risk Response with Business Objectives
  - Management is always responsible for evaluating and responding to the risk recommendations included in the risk report provided following risk assessment.
  - Management must always be aware of the drivers for risk management, such as compliance with regulations and the need to support and align the risk response with business priorities and objectives.

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- **Risk Response Options**
    - ***Risk mitigation*** - with appropriate control measures or mechanism
    - ***Risk avoidance*** - terminate the activity that give rise to it.
    - ***Risk transfer*** - to another party (usually an insurance company)
    - ***Risk acceptance*** - accept the risk.
- ***Risk mitigation*** means action is taken to reduce the frequency and/or impact of a risk.
    - May require the use of several controls until it reaches level of risk acceptance or risk tolerance
    - Examples of risk mitigation
        - Strengthening overall risk management practices, such as implementing sufficiently mature risk management processes
        - Deploy new technical, management or operational controls that reduce either the likelihood or impact of an adverse event
        - Installing a new access control system
        - Implementing policies or operational procedures
        - Using compensating controls
- ***Risk Avoidance*** means exiting the activities or conditions that give rise to risk
    - Applies when no other risk response is adequate
    - Examples of risk avoidance :
        - Relocating a data center away from a region with significant natural hazards.
        - Declining to engage in a very large project when the business case shows a notable risk of failure
        - Declining not to use a certain technology or software package because it would prevent future expansion.

CYBRARY

Lesson 5.2: Risk Mitigation Transference and Acceptance

Skills Learned From This Lesson: Risk Acceptance,Risk Transfer, Risk Sharing

- ***Risk Acceptance***

- A conscious decision made by senior management to recognize the existence of risk and knowingly decide to allow (assume) the risk to remain without (further) mitigation
    - Management response for impact of the risk event
- Defined as the amount of risk that senior management has determined is within acceptable or permissible bounds
    - Not the same as risk ignorance / rejection, which is the failure to identify or acknowledge risk
- *Risk tolerance*- An exception when senior management decides to exceed risk acceptance levels

- ***Risk Transfer / Sharing*** **-** is a decision to reduce loss through sharing the risk of loss with another organization (Purchasing insurance)
    - Partnership with another organization are an example
    - Decision should be reviewed on a regular basis

Lesson 5.3: Information Security Concepts

Skills Learned From This Lesson:Information security program, Information security practices

- As defined by ISACA the goal of this domain is to:" Develop and maintain an information security program that identifies, manages and protect the organization's assets while aligning to information security strategy and business goals, thereby supporting and effective security posture."
- Information Security Program - encompasses all the activity and resources that collectively provide information security services to an organization. NotesNotesNotes
    - Is best coordinated by COO, as this individual should properly see the need for balance between information security and business operations.
- Key Information Security Program Elements :
    - Technology - is often seen by enterprise management as a way to resolve security threats and risk.
    - People -Represents a human collective and must take into account values, behaviors and biases.
    - Process - Include formal and informal mechanisms to get things done.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Essential Information Security Practices
  - Management Commitment
  - Risk Management
  - Asset inventory and management
  - Change Management
  - Incident Response and Management
  - Configuration Management
  - Training and Awareness
  - Continuous Audit
  - Metrics and Measurement
  - Vulnerability Assessment
  - Penetration Testing
  - Application Security Testing
  - Device Management
  - Log Monitoring, Analysis and Management
  - Secure Development

Lesson 5.4: Security Program Requirements

Skills Learned From This Lesson: Security program, Risk Management, Conceptual

- Must be enterprise wide, there should not be separate programs for IT, Finance etc .. Enterprise security architecture at conceptual, logical, functional and physical level - holistic.
- Must manage risk to an acceptable level. Board of directors, senior management should define risk appetite, and we should manage risk to an acceptable level.
- Must be defined in business language (terms) to help non-technical stakeholders understand and endorse program goals.
- Must provide security related feedback to business owners and stakeholders.

CYBRARY

Lesson 5.5: Essential Elements of an Information Security Program

Skills Learned From This Lesson: Metrics, Security Program, IS Objectives

- Well planned Information Security strategy, aligned with business goals
- Objective of the Information Security program is to implement the strategy in the most cost-effective manner possible, while maximizing support of business functions and minimizing operational disruptions.
- It is essential to determine the forces that drive the business need for information security program. Primary drivers could be :
  - Increasing requirements for regulatory compliance
  - Higher frequency and cost related to security incidents
  - Business process or objectives that may be increased organizational risk…
- Information security Program should :
  - Provide strategic alignment with business objectives
  - Use Risk management as the foundation for security related decisions
  - Deliver Value to stakeholders (direct or indirect)
  - Manger resources effectively and efficiently
  - Provide integration with other assurance functions (operational security, physical security, facility security ….)
  - Use performance measurement to provide a means of measuring progress and monitoring.
  - Metrics must be developed at multiple levels, including strategic, management and operational levels.
  - Metrics should be defined and agreed on by management.

Lesson 5.6: Introduction to Information Security Frameworks - ISO 27002

Skills Learned From This Lesson: ISO 2700x, COBIT 5/ 2019

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- The information security management framework is a conceptual representation of and information security management structure. It should define technical, operational, administrative and managerial components of program.
    - More Notes
- The ISO/IEC 27000 family of information security standards
- The ISO 27000 family of information security management standards is a series of mutually supporting information security standards that can be combined to provide a globally recognised framework for best-practice information security management.
- The security standard ISO/IEC 27001:2015 Information Security Management System (ISMS) and the accompanying code of practice 27002:2015 provide widely accepted framework and approach to information security management. ISO/IEC 27001 standard can be mapped to COBIT, but are less business oriented, less comprehensive and do not provide complete tool sets.
- COBIT 2019 - provides comprehensive framework with focus on helping enterprises create optimal value from IT by maintaining a balance between realising benefits and optimizing risk levels and resource use.
- While COBIT 5 provide 5 key principles for governance and management of enterprise IT, COBIT 2019 provide 6 key principles.
- Cobit 2019 - Key Principles :
    - Provide Stakeholder Value
    - Holistic Approach
    - Dynamics Governance System
    - Governance Distinct from Management
    - Tailored to Enterprise Needs
    - End to End Governance System
- COBIT 2019 - improves on prior version of COBIT in following areas:
    - Flexibility and openness
    - Currency and relevance
    - Prescriptive application
    - Performance management of IT

Lesson 5.7: Information Security Frameworks

Skills Learned From This Lesson: Frameworks,

CYBRARY

- Components of Information Security Framework
    - Operational components
        - Operational components of security program are the ongoing management and administrative activities that must be performed to provide the required level of security assurance. They are generally conducted on daily to weekly timeline.
    - Management components
        - They will include strategic implementation activities such as standards development or modification, policy reviews and oversight of initiatives or program executions. Those activities generally take place less frequently than operational components.
    - Administrative components
        - Information security management must address the same business administration activities as other business units, such as budgeting planning, total cost of ownership (TCO) analysis, return on investment (ROI).
    - Educational Components - Information security management activities must include employee education and awareness regarding security risk. Awareness training is often integrated with employee initial training. However it's recommended to re-educate employees at least once per year.

CYBRARY

Lesson 5.8: Information Security Architecture !!! NOTE !!! First 30 sec of this video is without any signal !!! NOTE !!!
Skills Learned From This Lesson: Architecture, Type of Architecture

- Purpose of Architecture - Infrastructure comprises the computing platforms, Hardware, Software, FirmWare, Networks and it supports a wide range of applications, to meet business objectives. Once infrastructure is designed and deployed, the infrastructure should be secure.
- Types of Architecture:
    - Business- defines the business strategy, governance, organization and key business processes.

- Data - describes the relationship between integrated components ensuring that data assets are stored, ordered, managed and used in systems.
- Application - provides blueprint for individual application to be deployed, their interactions and relationships.
- Technology - describes the architectural design principles, components, relationships and supporting infrastructure.

Lesson 5.9: Security Operations Events Monitoring

Skills Learned From This Lesson: Operations, Components, Monitoring

- Operational components of security program are the ongoing management and administrative activities that must be performed to provide the required level of security assurance. They are generally conducted on daily to weekly timeline.
- Security operation components include:
    - Event Monitor
    - Vulnerability Management
    - Secure engineering and development
    - Network Protection
    - Endpoint protection and management
    - Identity and access management
    - Security incident management and BCP
    - Security Awareness training
    - Managed security service providers
    - Data Security
    - Cloud resources Management
-
- Event Monitoring - event monitoring is practice of eaming events that are occuring on information systems, including applications, operating systems, database management systems, end user devices, or any type and kind of network device, are being aware of what is going on throughout the entire operating environment.
    - Monitoring is a continuous process, which ensures that all events are recorded and can be investigated later if necessary.

CYBRARY

  - Log review is detailed and systematics form of monitoring which are logged information is analyzed for some specific pattern, abnormal, unauthorised ..activities.
  - Logs can be collected from different sources relevant to security. Manually review and monitoring logs is time consuming action, so administrators often use automatic tools for collecting and monitor logs.
  - SIEM - Security Information and Event Monitor is one of the tools used to automate monitoring of systems. SIEM can collect different types of logs and store in one location for future review.
- Vulnerability Management -refers to identifying vulnerabilities, evaluating them, and taking steps to mitigate risk, associated with them. Major elements of vulnerability management are routine vulnerability scans and periodic vulnerability assessments.

Lesson 5.10: Secure Engineering and Threat Modeling

Skills Learned From This Lesson: Secure Engineering, Development, STRIDE

- Security should be a concentracion at every state of a system development , including the SDLC (Software Development Life Cycle). The SDLC is not a methodology per se, but rather a description of the phases in the life cycle of a software application. The SDLC adheres to important phases that are essential for developers—such as planning, analysis, design, and implementation.
- The Security Development Lifecycle (SDL) is a security assurance process that is focused on software development. Every organization is different in many ways, however, every organization should take care about:
  - Requirements - Security and privacy requirements analysis should be performed on project level and include minimal security requirements, just before any code has been performed.
  - Preliminary analysis:
    - Conduct the preliminary analysis
    - Propose alternative solutions
    - Cost benefit analysis
  - Systems analysis, requirements definition - Define project goals into defined functions and operations of the intended application.

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

        - Collection of facts
        - Scrutiny of the existing system
        - Analysis of the proposed system
    - Systems design - desired features and operations are described in detail.
    - Development - Real coding beginning here.
    - Integration and testing - All pieces of software, bringing together on test environment for test and checked for bugs.
    - Acceptance, installation, deployment - final step for the development, deployed into production.
    - Maintenance- During the maintenance system is assessed to ensure it does not become obsolete.
    - Evaluation - post-implementation review.
    - Disposal - In this phase, plans are developed for discontinuing the use of system information, hardware, and software and making the transition to a new system.
- Some of the sSDLC:
    - Microsoft Security Development Lifecycle - https://www.microsoft.com/en-us/securityengineering/sdl
    - NIST 800-160 Volume 1 https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final
    - OWASP SAMM - https://www.owasp.org/index.php/OWASP_SAMM_Project
- Secure engineering and Development - STRIDE
- STRIDE is a model of threats developed by Praerit Garg and Loren Kohnfelder at Microsoft for identifying computer security threats. It provides a mnemonic for security threats in six categories:

CYBRARY

Threats	Mitigation
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-repudiability

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

Information disclosure (privacy breach or data leak)	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization

Lesson 5.11: Protecting the Network - Segmentation
Skills Learned From This Lesson: Segmentation, Intranet, Extranet, DMZ,

- Networks are not typically configured as one large collection of systems. Usually systems are collected (segmented) into smaller organization units. These smaller group of systems, smaller networks (subnets) can be used to:
    - Boosting performance
    - Reducing communication problems
    - Providing security
- Intranet is a private network, designed to host the same services as Internet (web portal, email services, IM ..etc) and is not accessible from anyone from the internet.
- Extranet (often named as DMZ or perimeter network) is a cross between Internet and intranet.
- Firewall - network device used to filter traffic. There is a various places to implement this device, usually it is implemented between internal and external network. Firewalls are effective against unrequested traffic and connection from outside of network.
- There are different types of firewalls, depends on the service they provide :
    - Static packet-filtering firewalls
    - Application level Gateway firewalls
    - Circuit-level gateway firewalls
    - Stateful inspection Firewalls
    - Next-gen Firewalls
    - Deep packet inspection firewalls.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- AirGap is another way to segment networks from the outside world. Network security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks.

Lesson 5.12: Protecting the Network - Wireless Security
Skills Learned From This Lesson: WEP, WPA, WPA2,WPA3

- Wireless networking is a popular method for connecting home systems as well as corporate systems. Main reasons are easy / fast deployment, and relatively low cost of implementations.
- WEP - Wired Equivalent Privacy is defined by IEEE 802.11 standard. Designed to provide the same level of security and encryption on wireless networks as is found on wired / cabled networks. WEP uses a predefined shared secret key. Secret key is static and shared among all wireless access points and device interfaces. Soon as its released, WEP was cracked. Today WEP can be cracked in less than a minute.
- WPA - Wi-FI Protected Access was designed as a replacement for WEP. Wi-Fi Protected Access is based on LEAP and TKIP and often use secret passphrase for authentication
    - LEAP - Lightweight Extensible Authentication Protocol- Cisco proprietary alternative to TKIP for WPA.
    - TKIP - Temporal Key Integrity Protocol, designed as a replacement for WPA, without replacement of legacy wireless hardware.
- WPA 2 - It is a new encryption scheme known as CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) based on AES encryption.
- AES - The Advanced Encryption Standard (AES), also known by its original name Rijndael, established by the U.S. National Institute of Standards and Technology (NIST) in 2001.
- WPA 3 - In January 2018, the Wi-Fi Alliance announced WPA3 as a replacement to WPA2, the new standard uses an equivalent 192-bit cryptographic strength in WPA3 - Enterprise mode and still mandates the use of CCMP-128 (AES-128 in CCM mode) as the minimum encryption algorithm in WPA3-Personal mode.
- Authentication - WPA, WPA2 and WPA 3 standards support enterprise authentication known as 802.1X / EAP.

- EAP - Extensible Authentication Protocol   is not mechanism of authentication it is rather framework for authentication. EAP enable different methods to be used with existing wireless or point-to-point connection technologies.

Lesson 5.13: Protecting the Network - Services
Skills Learned From This Lesson: DNS, Pharming, DHCP, LDAP

- DNS - The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. Main purpose of DNS is to translate domain name to an IP address. It is essential to have in TCP/IP networks Name System to provide IP's.
  - Widely used attack to DNS is pharming. Pharming is combination of Phishing and Farming, similar to phishing, where a website's traffic is manipulated and confidential information is stolen. In case where DNS cache is poisoning it is possible to route virus-free or malware-free computer to malicious server.
- The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on UDP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.
  - Misuse of DHCP can be:
    - Unauthorized DHCP servers providing false information to clients
    - Unauthorized clients gaining access to resources
    - Resource exhaustion attacks from malicious DHCP clients
- LDAP - The Lightweight Directory Access Protocol is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.
- Web services - are usually exposed to external network. Exposure of services outside of internal network bring to us some degree of risk. Regular testing of web services, vulnerability or pen-test of web services shrink attack surface, and hardening our overall security.
- Mail services - regular vulnerability scanning and pentesting raise our security bar.

CYBRARY

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

Lesson 5.14: Protecting the Network - Through Detection and Network Access Control
Skills Learned From This Lesson: NAC (Network Access Control), SHV (System Health Validator)

- Network Access Control (NAC) is a solution that uses a set of protocols to define and implement a policy that describes how to secure access to network nodes by devices when they initially attempt to access the network.
- Goals of NAC:
    - Prevent / reduce zero -day attack
    - Enforce security policies throughout the network
    - Use identifiers to perform access control
- NAC works in two ways, either preadmison philosophy, postadmison philosophy or both.
    - Preadmison philosophy - end-stations are inspected prior to being allowed on the network
    - Postadmision philosophy - NAC makes enforcement decisions based on user actions, after those users have been provided with access to the network.

Lesson 5.15: Data and Endpoint Security
Skills Learned From This Lesson: Endpoint, Data Security,

- Endpoint security is a security concept every individual device must maintain local security (End device is responsible for its own security)
    - Traditional security has depended on network border entries, however this is not best practice anymore. Threats exist inside of network as well as outside of internal network.
    - Every endpoint device should have an appropriate combination of security controls such as antivirus/malware software, local firewall, IDS/IPS ...
- Best practice (some of) for hardening security on endpoint device include :
    - Remove unnecessary services
    - Patch OS and software used on endpoint device
    - Review default settings (configuration settings, passwords..)
    - Rename guest and admin account
    - Install Antimalware and monitoring software …

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- **Data Security** - In order to protect data we always appreciate CIA triads and appropriate controls for protecting.
    - **Confidentiality**
        - Data at rest - Encryption - controls we should implement to protect data at rest. Data stored on hard drive, SSD .. use encryption.
        - Data in motion - To protect data in motion we should use TLS (transport Layer Protocol) cryptographic protocol design to provide communication security over communication channels.
        - Data in use - probably the hardest part for securing data. Recommendation for securing data in use is homomorphic encryption.
    - Homomorphic encryption - Homomorphic encryption is a form of encryption that allows computation on ciphertexts, generating an encrypted result which, when decrypted, matches the result of the operations as if they had been performed on the plaintext.
    - **Integrity -** control used to provide integrity are
        - Hash / Message digest -A hash function is any function that can be used to map data of arbitrary size to fixed-size values.The values returned by a hash function are called hash values, hash codes, digests, or simply hashes. Most popular algorithms are MD5, SHA and CRC32.
    - **Availability -** Our data should be available most of the time. To achieve this we use redundancy on all levels in our network and servers.

CYBRARY

Lesson 5.16: Selecting a Mitigation Strategy
Skills Learned From This Lesson: Controls Design*,* Cost Benefit Analysis

- Controls Design and Implementation - Controls are any technology, process, practice, policy, standards that serve to regulate any activity to manage risk. Controls can be:
    - Proactive - Proactive controls acting in advance of a future situation, rather than just reacting.
    - Reactive - implement controls when some unexpected / unwanted events occur.
- Vulnerabilities associated with New Controls - New controls always present new risk and new vulnerabilities. Implementation of new controls should consider :
    - Effectiveness of recommended options
    - Compatibility with existing controls

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Legislation and regulation
- Organizational policy and standards
- Operational structure and culture

- Cost Benefit Analysis - If the cost of the implementation controls exceed the benefit of mitigating the risk, organizations should consider to accept the risk rather then implement control. Cost Benefit Analysis helps organizations to get a monetary view of risk and then determine implementation of the controls.
- Return on Investment - ROI is often used as a method to justifying an investments, however, it can be difficult to determine the cost of the controls because it is hard to predict the likelihood of an impact.

Lesson 5.17: Types of Mitigating Controls

Skills Learned From This Lesson: Controls categories

- Control methods
- Control Categories
    - Preventive -Inhibit attempts to violate security policy and include such controls as access control enforcement, encryption and authentication.
    - Detective - warn of violations or attempting violation if security policy.
    - Corrective- remediate vulnerabilities.
    - Compensatory - compensate or increased risk by adding control steps that mitigate risk.
    - Deterrent - provide warnings that can deter potential compromise.
- Managing risk throughout the system /software development life cycle -(covered in deep in lesson 5.10: Secure Engineering and Threat Modeling)

Lesson 5.18: Identity and Access Management

Skills Learned From This Lesson: Identity management, Access Management, IAM

- Identity and Access Management is all about granting and revoking privileges to access to data or systems. Focus of Identity and Access Management is identification,

Brought to you by:
CYBRARY | FOR BUSINESS
Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.

authentification, authorization and accountability. It is more than just which user have access which files or services.

- Identification is a process of subject claiming an identity
- Authorization verifies the identity of the subject by comparing one or two factor against a database of valid identities such as user accounts.
- Identity proofing - In the organizations, new employees prove their identity with appropriate documentation. (something you have- driver licences, passport, SSN, etc ..) Registration is more or less similar to any organization.
- Account provisioning - in the organization, account provisioning should be done via Active Directory automatically (will be ideal).
- Accountability - Auditing, monitoring and logging provide accountability by ensuring that subject can be held accountable for their actions.
- Authentication Factors - there are three methods of authentication known as types of factors:
    - Type1 - Something you know (usually - passwords, PIN, passphrase)
    - Type2- Something you have (Physical device - usually smartcard, hardware token, memory card …)
    - Type3- Something you are (physical characteristics of person identified with different types of biometrics)
- Process of provisioning users should include de-provisioning also. Following the same principle of provisioning, deprovisioning should be also automated task.

CYBRARY

Lesson 5.19: Third Party Governance

Skills Learned From This Lesson: Governance, Third party, Process

- You can transfer RISK, but you cannot transfer LIABILITY.
- Important aspect of security and risk governance is rules and process, when we are dealing with third party.
    - Third party providers are typically:
    - ISP providers
    - Outsourced operation
    - Trading partners
    - Merged or acquired organization

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Some services (from providers) are under the direct control of IT/ Security teams, some of them are under the direct control of other departments. Risk practitioner should be informed and understand business requirements.
- Managing risk to an acceptable level can pose challenges and may require various controls

Lesson 5.20: Policies, Procedures, Standards, and Guidelines
Skills Learned From This Lesson: Policies, Procedures, Standards and Guidelines

- Policies - high level statements, of an organization's beliefs, goals, and objectives and general means and a general means for their attainment for a specific subject area. Three main types of policies exist:
    - The Corporate Security Policy can be thought of as a blueprint for the whole organization’s security program.It is strategic plan for implementing security in the organization.
    - A System Specific policy is concerned with a specific or individual computer system.It is meant to present the approved software, hardware, and hardening methods for that specific system.
    - An Issue-specific policy is concerned with a certain functional aspect that may require more attention.
- Procedures - outline the specifics of how policies, standards and guidelines will actually be implemented in the operating environment.
- Standards - mandatory activities, actions, rules or regulations designed to provide policies with a support structure and specific direction.
- Guidelines - more general statements that provide a framework within which to implement procedures. Guidelines are recommendations (“Best Practice”).
- Baselines - minimum acceptable security configuration for a system or process.

Lesson 5.21: Certification and Accreditation
Skills Learned From This Lesson: TCSEC, ITSEC, CC

- Certification - technical evaluation of the product’s security mechanisms in a particular environment. Once having passed the certification process, the system is verified.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Accreditation - a formal declaration by an Authorisation Official AO (title that has replaced Designated Accrediting Authority - DAA) that information systems are approved to operate at an acceptable level of risk based on the implementation of an approved set of technical, managerial, and procedural safeguards. Once accredited, the system is now validated.
    - More Notes
- Traditional Evaluation Criteria
    - TCSEC - Trusted Computer System Evaluation Criteria is a standard that sets basic requirements for assessing the effectiveness of computer security controls. The TSEC was used to evaluate classify, and select computer systems for processing, storage and retrieval of sensitive or classified information. Frequently referred to as the “Orange Book” issued from DoD in USA. TCSEC define four division D,C,B,and A, where A is the highest security. TCSEC replaced by Common Criteria international standard in 2005.
    - TCSEC evaluates Confidentiality
- ITSEC - Information Technology Security Evaluation Criteria, is a structured set of criteria for evaluating computer security within products and systems. In 1990 a number of Europian countries agreed to recognize the validity of ITSEC evaluations.
    - Evaluates Confidentiality, Integrity and Availability
- Common Criteria (CC) - Common Criteria for Information Technology Security Evaluation (referred to as Common Criteria or CC) is an international standard (ISO/IEC 15408) for computer security certification. ISO/IEC 15408-1:2009 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.
- Protection Profile (PP) – a document, typically created by a user or user community, which identifies security requirements for a class of security devices (for example, smart cards used to provide digital signatures, or network firewalls) relevant to that user for a particular purpose.
- Target of Evaluation (TOE) – the product or system that is the subject of the evaluation. The evaluation serves to validate claims made about the target.
- Security Target (ST) – the document that identifies the security properties of the target of evaluation. The ST may claim conformance with one or more PPs. The TOE is evaluated

Brought to you by:

CYBRARY | FOR BUSINESS

Develop your team with the ***fastest growing catalog*** *in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

against the SFRs (Security Functional Requirements) established in its ST, no more and no less.

- Security Functional Requirements (SFRs) – specify individual security functions which may be provided by a product. The Common Criteria presents a standard catalogue of such functions.
- Evaluation Assurance Level (EAL) – the numerical rating describing the depth and rigor of an evaluation. Each EAL corresponds to a package of security assurance requirements.Common Criteria lists seven levels, with EAL 1 being the most basic and EAL 7 being the most stringent.
- Common Criteria Evaluation Assurance Levels:
    - EAL 1- Functionally tested
    - EAL 2- Structurally tested
    - EAL 3- Methodically tested and checked
    - EAL 4- Methodically designed, tested, and reviewed
    - EAL 5- Semi formally designed and tested
    - EAL 6- Semi formally verified designed and tested
    - EAL 7- Formally verified designed and tested
- Metrics - a measurement of process or entity based on its performance in relation to desired objectives.
- Monitoring is continuous or regular evaluation of system or control to determine its operation or effectiveness. Can be quantitative or qualitative.

CYBRARY

The November 1981 issue of Management Review contained a paper by George T. Doran called There's a S.M.A.R.T. way to write management's goals and objectives. It discussed the importance of objectives and the difficulty of setting them.

Ideally speaking, each corporate, department, and section objective should be:

- Specific – target a specific area for improvement.
- Measurable – quantify or at least suggest an indicator of progress.
- Assignable – specify who will do it.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Realistic – state what results can realistically be achieved, given the available resources.
- Time-related – specify when the result(s) can be achieved.

Module 6: Risk Monitoring and Control Mitigation

Lesson 6.1: Risk, Control Monitoring, and Reporting
Skills Learned From This Lesson: Monitoring Control, Control Assessments

A risk response is designated and implemented based on a risk assessment that was conducted at a single point in time. Changing the nature of risk and associated controls, ongoing monitoring is an essential step of the Risk Management Life Cycle. Some of the reasons for monitoring are:

- Controls can become less effective
- The operational environment may change, and
- New threats, technologies and vulnerabilities may emerge
- Monitoring Controls
    - The purpose of control monitoring is to verify whether the control is effectively addressing the risk.
    - The purpose of risk monitoring is to collect, validate and evaluate goals and metrics, to monitor that process are performing as expected, and to provide reporting.
    - Monitoring may be done though self-assessment or independent assurance reviews.
    - The risk practitioner should encourage management and process owners to positive ownership of control improvement.
- The steps for monitoring controls are:
    - Identify and confirm risk control owners and stakeholders
    - Engage with stakeholders and communicate the risk and information security requirements and objectives for monitoring and reporting
    - Align and continually maintain the information security
    - Establish the information security monitoring process and procedure.

CYBRARY

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

- Agree on life cycle management and change control process for information security monitoring and reporting
    - Request, prioritize and allocate resources for monitoring information security.
- Result of Control Assessments
    - Timeliness of the reporting
        - Are data received in time to take corrective action?
    - Skill of the data analyst
        - Does the analyst have skills to properly evaluate control?
    - Quality of monitoring data available
        - Are the monitoring data accurate and complete?
    - Quantity of data to be analyzed
        - Can the risk practitioner find the important data in the midst of all the other log data available ?

Lesson 6.2: Key Risk Indicators (KRIs)

Skills Learned From This Lesson: KRI, Criteria for KRI

- Risk indicators are metrics capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite
- Benefits to the enterprise:
    - Provide an early warning (forward-looking) signal that a high risk is emerging to enable management to take proactive action (before the risk actually becomes a loss).
    - Provide a backward-looking view on risk events that have occurred, enabling risk responses and management to be improved.
    - Enable the documentation and analysis of trends.
    - Provide an indication of the enterprise's risk appetite and tolerance through metric setting (i.e., KRI thresholds)
    - Increase the likelihood of achieving the enterprise's strategic objectives.
    - Assist in continually optimising the risk governance and management environment.
- Criteria to select KRIs include:
    - Impact—Indicators for risks with high business impact are more likely to be KRIs.

CYBRARY (watermark)

    - Effort to implement, measure and report—For different indicators that are equivalent in sensitivity, the one that is easier to measure is 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 for risk and capable of accurately indicating variances in the risk.
- Examples of KRI's:
    - Quantity of unauthorized equipment or software detected in scan.
    - Number of instances of SLAs exceeding threshold.
    - High average downtime due to operational incidents.
    - Average time to deploy new security patches to servers.
    - Excessive average time to research and remediate operations incidents
    - Number of desktops/laptops that do not have current antivirus signatures or have not run a full scan within scheduled periods.
- KRI support:
    - Risk appetite
    - Risk identification
    - Risk mitigation
    - Risk culture
    - Risk measurement and reporting
    - Regulatory compliance

CYBRARY

Lesson 6.2: Tools for Risk Monitoring

Skills Learned From This Lesson: Tools, SIEM, LOGS

- Data Collections and Extraction Tools and Technique
    - Audit report
        - Internal
        - External
    - Incident reports
    - User feedback
    - Observation
    - Interviews with management

  - Security report
  - Logs
- Data Collection - LOG
  - Analysing of log data should answer on :
    - Are the controls operating correctly ?
    - Are the risk strategy and controls aligned with business strategy and priorities ?
    - Are the controls flexible enough to meet changing threats ?
    - Is the risk management effort aiding in reaching corporate objectives?
    - Is the awareness of risk and compliance embedded into user behaviors ?
  - Logs may contain sensitive information and may be needed for forensic purposes
  - Logs should not contain too much information
- Security Information and Event Management (SIEM), software products and services combine security information management (SIM) and security event management (SEM). They provide real-time analysis of security alerts generated by applications and network hardware.
- External Sources of Information:
  - Media report
  - CERT - Computer Emergency Response Team
  - Security company reports
  - Regulatory bodies
  - Peer organizations

CYBRARY

CRISC Certification Job Practice – Effective 2015

The job practice domains and task and knowledge statements are as follows:
Domain 1—IT Risk Identification (27%)
Domain 2—IT Risk Assessment (28%)
Domain 3—Risk Response and Mitigation (23%)
Domain 4—Risk and Control Monitoring and Reporting (22%)

Domain 1—IT Risk Identification
Identify the universe of IT risk to contribute to the execution of the IT risk management strategy in support of business objectives and in alignment with the enterprise risk management (ERM) strategy.
1.1 Collect and review information, including existing documentation, regarding the organization's internal and external business and IT environments to identify potential or realized impacts of IT risk to the organization's business objectives and operations.
1.2 Identify potential threats and vulnerabilities to the organization's people, processes and technology to enable IT risk analysis.
1.3 Develop a comprehensive set of IT risk scenarios based on available information to determine the potential impact to business objectives and operations.
1.4 Identify key stakeholders for IT risk scenarios to help establish accountability.
1.5 Establish an IT risk register to help ensure that identified IT risk scenarios are accounted for and incorporated into the enterprise-wide risk profile.
1.6 Identify risk appetite and tolerance defined by senior leadership and key stakeholders to ensure alignment with business objectives.
1.7 Collaborate in the development of a risk awareness program, and conduct training to ensure that stakeholders understand risk and to promote a risk-aware culture.

Domain 2—IT Risk Assessment
Analyze and evaluate IT risk to determine the likelihood and impact on business objectives to enable risk-based decision making.
2.1 Analyze risk scenarios based on organizational criteria (e.g., organizational structure, policies, standards, technology, architecture, controls) to determine the likelihood and impact of an identified risk.
2.2 Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation.
2.3 Review the results of risk and control analysis to assess any gaps between current and desired states of the IT risk environment.
2.4 Ensure that risk ownership is assigned at the appropriate level to establish clear lines of accountability.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

2.5 Communicate the results of risk assessments to senior management and appropriate stakeholders to enable risk-based decision making.
2.6 Update the risk register with the results of the risk assessment.

Domain 3—Risk Response and Mitigation

Determine risk response options and evaluate their efficiency and effectiveness to manage risk in alignment with business objectives.
3.1 Consult with risk owners to select and align recommended risk responses with business objectives and enable informed risk decisions.
3.2 Consult with, or assist, risk owners on the development of risk action plans to ensure that plans include key elements (e.g., response, cost, target date).
3.3 Consult on the design and implementation or adjustment of mitigating controls to ensure that the risk is managed to an acceptable level.
3.4 Ensure that control ownership is assigned to establish clear lines of accountability.
3.5 Assist control owners in developing control procedures and documentation to enable efficient and effective control execution.
3.6 Update the risk register to reflect changes in risk and management's risk response.
3.7 Validate that risk responses have been executed according to the risk action plans.

Domain 4—Risk and Control Monitoring and Reporting

Continuously monitor and report on IT risk and controls to relevant stakeholders to ensure the continued efficiency and effectiveness of the IT risk management strategy and its alignment to business objectives.
4.1 Define and establish key risk indicators (KRIs) and thresholds based on available data, to enable monitoring of changes in risk.
4.2 Monitor and analyze key risk indicators (KRIs) to identify changes or trends in the IT risk profile.
4.3 Report on changes or trends related to the IT risk profile to assist management and relevant stakeholders in decision making.
4.4 Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of control performance.

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

4.5 Monitor and analyze key performance indicators (KPIs) to identify changes or trends related to the control environment and determine the efficiency and effectiveness of controls.
4.6 Review the results of control assessments to determine the effectiveness of the control environment.
4.7 Report on the performance of, changes to, or trends in the overall risk profile and control environment to relevant stakeholders to enable decision making.

CYBRARY

CRISC Knowledge Statements

1. laws, regulations, standards and compliance requirements
2. industry trends and emerging technologies
3. enterprise systems architecture (e.g., platforms, networks, applications, databases and operating systems)
4. business goals and objectives
5. contractual requirements with customers and third-party service providers
6. threats and vulnerabilities related to:

    6.1. business processes and initiatives
    6.2. third-party management
    6.3. data management
    6.4. hardware, software and appliances
    6.5. the system development life cycle (SDLC)
    6.6. project and program management
    6.7. business continuity and disaster recovery management (DRM)
    6.8. management of IT operations
    6.9. emerging technologies

1. methods to identify risk
2. risk scenario development tools and techniques
3. risk identification and classification standards, and frameworks
4. risk events/incident concepts (e.g., contributing conditions, lessons learned, loss result)
5. elements of a risk register

Brought to you by:

CYBRARY | FOR BUSINESS

*Develop your team with the **fastest growing catalog** in the cybersecurity industry. Enterprise-grade workforce development management, advanced training features and detailed skill gap and competency analytics.*

6. risk appetite and tolerance
7. risk analysis methodologies (quantitative and qualitative)
8. organizational structures
9. organizational culture, ethics and behavior
10. organizational assets (e.g., people, technology, data, trademarks, intellectual property) and business processes, including enterprise risk management (ERM)
11. organizational policies and standards
12. business process review tools and techniques
13. analysis techniques (e.g., root cause, gap, cost-benefit, return on investment [ROI])
14. capability assessment models and improvement techniques and strategies
15. data analysis, validation and aggregation techniques (e.g., trend analysis, modeling)
16. data collection and extraction tools and techniques
17. principles of risk and control ownership
18. characteristics of inherent and residual risk
19. exception management practices
20. risk assessment standards, frameworks and techniques
21. risk response options (i.e., accept, mitigate, avoid, transfer) and criteria for selection
22. information security concepts and principles, including confidentiality, integrity and availability of information
23. systems control design and implementation, including testing methodologies and practices
24. the impact of emerging technologies on design and implementation of controls
25. requirements, principles, and practices for educating and training on risk and control activities
26. key risk indicators (KRIs)
27. risk monitoring standards and frameworks
28. risk monitoring tools and techniques
29. risk reporting tools and techniques
30. IT risk management best practices
31. key performance indicator (KPIs)
32. control types, standards, and frameworks
33. control monitoring and reporting tools and techniques
34. control assessment types (e.g., self-assessments, audits, vulnerability assessments, penetration tests, third-party assurance)

CYBRARY

35. control activities, objectives, practices and metrics related to:

41.1. business processes
41.2. information security, including technology certification and accreditation practices
41.3. third-party management, including service delivery
41.4. data management
41.5. the system development life cycle (SDLC)
41.6. project and program management
41.7. business continuity and disaster recovery management (DRM)
41.8. IT operations management
41.9. the information systems architecture (e.g., platforms, networks, applications, databases and operating systems)

CYBRARY