CRISC EXAM PREP COURSE: SESSION 2

Job Practice

DOMAIN 2

IT RISK ASSESSMENT

Domain 2

Analyze and evaluate IT risk to determine the likelihood and impact on business objectives to enable risk-based decision making.

- The focus of Domain 2 is the assessment of risk scenarios to determine risk probability and significance.

Learning Objectives

- The objective of this domain is to ensure that the CRISC candidate has the knowledge necessary to:
  - 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
  - Communicate IT risk assessment results to relevant stakeholders

On the CRISC Exam

- Domain 2 represents 28% of the questions on the CRISC exam (approximately 42 questions).
- Domain 2 incorporates six tasks related to IT risk assessment.

Domain Tasks

- **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.

Task 2.1

Certified in Risk and Information Systems Control™
An ISACA® Certification

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.

Task to Knowledge Statements

Certified in Risk and Information Systems Control™ (CRISC™) — An ISACA® Certification

How does Task 2.1 relate to each of the following knowledge statements?

Knowledge Statement	Connection
13. Risk analysis methodologies (quantitative and qualitative)	The selection of risk analysis methodology is generally based on the value and significance of the process/asset, the amount of data present and the quality of the data available.
19. Analysis techniques (e.g. root cause, gap, cost-benefit, ROI)	Analysis techniques vary in terms of what data is used and the determinations made from that data.
21. Data analysis, validation and aggregation techniques	Before conducting quantitative analysis on risk scenarios, the data must be requested and prepared for analysis with the assistance of the data owner.
22. Data collection and extraction tools and techniques	In preparation for the analysis of risk scenarios based on organizational criteria, data collection and extraction criteria and methods must be set.

Comparing Processes

Risk Identification

- Determines and documents the risk faced by an enterprise
- Recognizes threats, vulnerabilities, assets and controls in the operational environment
- Incorporates historical data, available resources, enterprise culture and adversary persistence

Risk Assessment

- Evaluates risks and their likelihood and potential effects
- Gauges impacts on critical functions of the enterprise
- Defines and evaluates the cost of the controls in place

Risk Impact Factors

Organizational Structure and Culture

- What is the organizational maturity level regarding risk management and incident response?
- Is there enterprisewide support for and participation in risk management?
- Does the organizational culture encourage communication and action around problems?

Policies

- Are policies present and enforced?
- Do existing policies succeed in providing direction regarding appropriate behaviors across the organization?
- Do policies communicate a clear message from senior management regarding the risk culture?
- Are policies and their enforcement, or lack of enforcement, creating risk through employee non-compliance?

Risk Impact Factors (cont'd)

Certified in Risk and Information Systems Control™
An ISACA® Certification

Standards and Procedures

- Are organizational practices and operations based on external standards such as an ISO standard, or internal standards, such as requiring staff members to use the same operating system?
- Is the performance of specific operations described in procedures that reflect external or internal standards?
- Do procedures describe operations in a consistent and measurable way, allowing for correct performance and detection of abnormal operations?

Technology

- Does the age and condition of organizational technology present a risk?
- Does the organization's technology system consist of products from a varied mix of vendors, languages, configurations or vintages, resulting in risk from a highly complex system?
- What issues arise from difficulties in obtaining, supporting and maintain existing technologies?

Risk Impact Factors (cont'd)

Architecture

- Are organizational processes and practices built around an enterprisewide approach to risk management, IT architecture and business continuity?
- Does this approach promote consistency, repeatability, compliance, accountability and visibility to senior management?
- Are any of the following present in the organizational architecture:
  - Controls that overlap and/or conflict with one another?
  - Unidentified single points of failure?
  - Unidentified methods of bypassing controls?
  - Inadequate network isolation?

The Control Environment

- Controls are implemented to mitigate risk or to comply with regulations, but may present unidentified vulnerabilities as a result of the following:
  - The control may not work correctly or be properly maintained.
  - The control may be unsuitable or misconfigured for the risk it addresses.
  - The control may be implemented incorrectly due to poorly trained staff or other issues.
  - The presence of a problematic control may lead to a false sense of security and complacency regarding existing risk.

Control Categories

Category	Description	Interactions	Example
Compensating	An internal control that corrects a deficiency or weakness in the control structure of the enterprise	Reduces the likelihood of a threat event	The addition of a challenge response component to weak access controls that can compensate for the deficiency in the access control mechanism
Corrective	A control that remediates errors, omissions and unauthorized uses and intrusions, once they are detected	Reduces the impact of a threat event that exploits a vulnerability	Backup restore procedures that enable a system to be recovered if harm is so extensive that processing cannot continue without recourse to corrective measures
Detective	A control that warns of violations or attempted violations of security policy	Discovers a threat event and triggers preventive control	Controls such as audit trails, intrusion detection methods and checksums

Control Categories (cont'd)

Category	Description	Interactions	Example
Deterrent	A control that provides warnings that may deter potential compromise	Reduces the likelihood of a threat event	Controls such as warning banners on login screens or offering rewards for the arrest of hackers
Directive	A control that mandates the behavior of an entity by specifying what actions are, or are not, permitted. A directive control may also be considered to be a type of deterrent control.	Reduces the likelihood of a threat event	Controls that arise through the outlining and enforcement of policies
Preventive	A control that inhibits attempts to violate security policy	Protects against vulnerabilities and reduces the impact of a threat event that exploits a vulnerability	Controls such as access control enforcement, encryption and authentication

Discussion Question

- Which of the following **BEST** ensures that identified risk is kept at an acceptable level?
  A. Reviewing of the controls periodically, according to the risk action plan
  B. Listing each risk as a separate entry in the risk register
  C. Creating a separate risk register for every department
  D. Maintaining a key risk indicator (KRI) for assets in the risk register

Discussion Question

- The **MOST** effective method to conduct a risk assessment on an internal system in an organization is to start by understanding the:

A. performance metrics and indicators.
B. policies and standards.
C. recent audit findings and recommendations.
D. system and its subsystems.

Task 2.2

Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation.

Task to Knowledge Statements

Certified in Risk and Information Systems Control™ (CRISC™) An ISACA® Certification

How does Task 2.2 relate to each of the following knowledge statements?

Knowledge Statement	Connection
20. Capability assessment models and improvement techniques and strategies	Assessment models such as CMMI and PAM and ISO15504 aid organizations in identifying the current state of the existing controls and evaluating their current effectiveness and need for further mitigation.
25. Exception management practices	Exception management practices are a form of control designed to address situations where an administrative control such as a policy, procedure or process is knowingly being violated.
26. Risk assessment standards, frameworks and techniques	Risk assessment standards, frameworks and techniques are adopted by organizations to bring repeatability and credibility to the risk assessment process, thereby contributing to the effectiveness of IT risk mitigation.

Task to Knowledge Statements

Certified in Risk and Information Systems Control™ (CRISC™)
An ISACA® Certification

How does Task 2.2 relate to each of the following knowledge statements?

Knowledge Statement	Connection
27. Risk response options (i.e., accept, mitigate, avoid, transfer) and criteria for selection	During the assessment process, the current states of controls are identified and evaluated for their effectiveness in reducing the likelihood or impact should a vulnerability be exploited. Based on this, risk response options are developed.

Controls

- Controls are implemented to mitigate risk or to comply with regulations.
- Inadequate controls are often present. Some sources of inadequacy include the following:
  - The wrong controls are being used.
  - Controls are ignored or bypassed.
  - Controls are poorly maintained.
  - Logs or control data are not reviewed.
  - Controls are not tested.
  - Changes to the configuration of controls are not managed.
  - Controls can be physically accessed and altered.

Risk Analysis Methods

- Three primary methods are used to analyze risk and the controls related to mitigating these risks, as follows:

Method	Based On	Benefit	Challenges
Quantitative methods	Numerical calculations, especially monetary	Facilitates cost/benefit analysis of controls	Reliance on forecasts, estimates and assumptions
Qualitative methods	Scenarios and descriptions of real or anticipated events	Facilitates analysis of scenario impacts	Does not provide objective cost-benefit data; tends to overemphasize low-level risk
Semiquantitative methods	A hybrid approach combining the realistic input of qualitative assessment and the numerical scale of quantitative into a risk ranking methodology	Facilitates analysis of controls on both a scenario and a numerical basis	Accurate decisions about risk levels must be clearly discernible to those who provide input

Assessment Methods

- An array of risk assessment methods allow the identification of control-related risk.
- Using a consistent methodology or framework is more important than which one is used.
- Some available methods include the following:

Methods	Notes
Brainstorming/ Structured interview	Effective for ranking a large group of potential risks, via team or individual input
Cause-and-effect analysis	Examines the factors that contributed to a certain outcome, grouping the causes into categories, often through brainstorming
Checklists	List of potential or typical threats developed from experience, codes and standards

Assessment Methods (cont'd)

Methods	Notes
Delphi method	A collaborative technique often used to build consensus among experts. Uses expert opinion, often gathered via two or more rounds of questionnaires. Results are gathered, then communicated by a facilitator.
Monte-Carlo analysis	Used to establish the aggregate variation in a system, modeling situations in which the interactions of various inputs can be mathematically defined
Root-cause analysis	A process of diagnosis to establish the origins of events, which can be used for learning from consequences, typically from errors and problems
Scenario analysis	Examines the risk scenarios previously developed for controls issues related to organizational structure/culture, policies, standards and procedures and technology
Structured "what-if" technique	A form of structured brainstorming usually executed in a facilitated workshop. Uses prompts and guide words; typically paired with another risk assessment technique.

Areas of Focus

- Control assessment, by its nature, spans many aspects of the enterprise and its operating environment.
- Each of the following questions represents an area of focus for control assessment:
  - Does the IT department consistently monitor and adapt to relevant trends in the industry?
  - Are emerging technologies deployed only after risk impacts are delineated?
  - Are new threats and vulnerabilities analyzed against existing system and application controls?
  - Is data ownership and management consistently reviewed and assessed for compliance with data management policies and procedures?
  - Are effective incident response, business continuity and disaster recovery plans in place to protect against system failure?
  - In the event that an exception to policies and procedures is required, is a management practice in place to ensure appropriate approval and documentation?

Information Sources

- Tools used by the risk practitioner to determine the current state of IT risk controls include:

Audits	Control tests conducted by the control owner or custodian	Incident reports	IT operations feedback
Logs	Media reports of new vulnerabilities and threats	Observation	Self-assessments
Third-party assurance	User feedback	Vendor reports	Vulnerability assessments and penetration tests

Focus On: Third Parties

- Outsourcing refers to a formal agreement with a third party to perform information systems or other business functions for an enterprise.
- This arrangement, which includes cloud computing, can be beneficial, but presents risk.
- The presence of a control may be required for each of the following:
  - The potential for a data breach at the third party location due to issues with data protection
  - The risk of losing access to source code should the supplier go out of business, fail to support its work or dishonor the contract
  - The necessity of protecting intellectual property owned by the contracting enterprise
  - The potential for communication issues between the third party supplier and the contracting enterprise
- Many of these risks also pertain to similar arrangements made with enterprise customers.

Discussion Question

- Which type of risk assessment methods involves conducting interviews and using anonymous questionnaires by subject matter experts?
  A. Quantitative
  B. Probabilistic
  C. Monte Carlo
  D. Qualitative

Discussion Question

- The board of directors wants to know the financial impact of specific, individual risk scenarios. What type of approach is **BEST** suited to fulfill this requirement?
  A. Delphi method
  B. Quantitative analysis
  C. Qualitative analysis
  D. Financial risk modeling

Task 2.3

Review the results of risk and control analysis to assess any gaps between current and desired states of the IT risk environment.

Task to Knowledge Statements

Certified in Risk and Information Systems Control™ (CRISC™) An ISACA® Certification

How does Task 2.3 relate to each of the following knowledge statements?

Knowledge Statement	Connection
32. Key risk indicators (KRIs)	Key Risk Indicators allow management to monitor and measure situations that may give rise to risk in order to make corrective actions before an adverse event materializes.
37. Key performance indicator (KPIs)	A Key Performance Indicator permits management to validate that controls are performing as expected (desired) and show trends in control behavior.
38. Control types, standards, and frameworks	Control types, standards and frameworks are adopted by organizations to bring repeatability and credibility to the control development, monitoring and classification process.
39. Control monitoring and reporting tools and techniques	Once controls are implemented, they must be monitored. The results must be provided to the risk and control owner on a timely basis for assessment.

Focus On: Capability

- When assessing risk, it is important to measure the capability and maturity of the risk management processes of the organization.
- An organization with a capable and mature risk management process is much more likely to do the following:
  - Prevent incidents
  - Detect incidents sooner
  - Recover rapidly from incidents

Focus On: Capability (cont'd)

- Examples of key elements used to measure IT risk management capability include the following:
  - Support of senior management
  - Regular communication between stakeholders
  - Existence of policy, procedures and standards
  - Logging and monitoring of system activity
  - Scheduled risk assessments and review
  - Testing of business continuity plans and disaster recovery plans
  - Involvement of risk principles and personnel in IT projects
  - Staff training
  - Time to detect and resolve security incidents

Data Analysis Challenges

- The information yielded by data sources serves as the basis of risk and control analyses.
- The presence of too much data can present risk of its own, as follows:
  - Too much data may hide or obscure important but less visible events.
  - Incorrect analysis of data may lead to erroneous conclusions.
  - Completeness and trustworthiness of data may be unknown.
- Each of these issues must be considered with respect to the risk that data may not provide the information needed for defining and responding to vulnerabilities.

Data Analysis Approaches

- Some approaches to conducting the analysis of data are shown below.

Approach	Description
Root cause analysis	Predictive or diagnostic tools used to explore root causes, underlying conditions and core factors leading to an event, used to identify potential risk. Often expressed in fishbone or Ishikawa diagram format.
Fault tree analysis	Provides a systematic description of the combination of possible occurrences in a system resulting from a top-level event, including hardware failures and human error. Focus is on locating the root causes and their preconditions.
Sensitivity analysis	Quantitative technique designed to determine which risk factors present the most significant impact, especially in regard to uncertainty associated with each factor.
Threat and misuse case modeling	Through mapping the potential methods, approaches, steps and techniques used by an adversary to perpetrate an attack, appropriate controls can be designed to protect vulnerabilities.

Gap Analysis

- Gap analysis is based on a comparison of the current state or conditions with respect to risk and the desired state or conditions.
- The difference between these two is the “gap.”
- When the gap has been defined, appropriate means of reducing the gap may be identified and executed.
- Three unique data sets based on performance indicators may be used to derive the gap analysis and monitor progress toward its closing, as shown on the next slide.

Gap Analysis (cont'd)

Indicator	Description
Key performance indicator (KPI)	Measure of how well a process enables a goal to be reached. An indicator of capabilities, practices and skills; can be used to indicate whether current risk levels match desired risk levels
Key risk indicator (KRI)	A risk indicator is a metric 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; KRIs are the subset of indicators that possess a high likelihood of predicting of indicating important risk
Key goal indicator (KGI)	A measure that tells management, after the fact, whether an IT process has achieved its business requirements; usually expressed in terms of information criteria. Used to notify management on the status of critical reporting criteria

Risk Ranking

- The total level of risk associated with a threat is derived from combining the following information sets:
  - Identification of the threat
  - Characteristics and capabilities of the threat source
  - Likelihood of attack
  - Vulnerabilities and their severity
  - Effectiveness of controls
  - Level of impact of a successful attack
- A given risk, as expressed in magnitude and frequency, may be also be ranked according to the enterprise's risk appetite.
- Where the ranking of a given risk exceeds the risk appetite of the enterprise, the risk practitioner must provide recommendations on how to mitigate that risk.

Discussion Question

- The **PRIMARY** benefit of using a maturity model to assess the enterprise's data management process is that it:

A. can be used for benchmarking.
B. helps identify gaps.
C. provides goals and objectives.
D. enforces continuous improvement.

Discussion Question

- An enterprise is hiring a consultant to help determine the maturity level of the risk management program. The **MOST** important element of the request for proposal (RFP) is the:
  A. sample deliverable.
  B. past experience of the engagement team.
  C. methodology used in the assessment.
  D. references from other organizations.

Task 2.4

Ensure that risk ownership is assigned at the appropriate level to establish clear lines of accountability.

Task to Knowledge Statements

Certified in Risk and Information Systems Control™ (CRISC™) An ISACA® Certification

How does Task 2.4 relate to each of the following knowledge statements?

Knowledge Statement	Connection
10. Risk events/incident concepts (e.g., contributing conditions, lessons learned, loss result)	Complex risk scenarios, as well as the results of lessons learned, root cause analysis and any actual loss event results, must be assigned ownership in order to ensure prompt evaluation and proper ranking, if necessary.
35. Risk reporting tools and techniques	While risk-related information should only be communicated on a need to know basis, developing a communication plan aids in timely decision making.
36. IT risk management best practices	Risk ownership is fundamental to risk management "good" practices, because it ensures accountability.

Risk Ownership

- Upon completion of the risk and controls assessment process, risk has been documented and prioritized with respect to risk response.
- Next, each risk must be linked to an individual who has the responsibility to accept risk ownership.
- The risk owner is tasked with deciding on the best response to the identified risk.

Risk Accountability

- To ensure accountability, the ownership of a risk must always be assigned to an individual, not a department or the organization as a whole.
- It is also important that the individual to whom the risk is assigned is located at a level in the organizational hierarchy in which the following occurs:
  - He/she is authorized to make decisions on behalf of the organization.
  - He/she can be held accountable for those decisions.

Discussion Question

- Which of the following **BEST** describes the risk-related roles and responsibilities of an organizational business unit (BU)? The BU management team:

  A. owns the mitigation plan for the risk belonging to their BU, while board members are responsible for identifying and assessing risk as well as reporting on that risk to the appropriate support functions.

  B. owns the risk and is responsible for identifying, assessing and mitigating risk as well as reporting on that risk to the appropriate support functions and the board of directors.

  C. carries out the respective risk-related responsibilities, but ultimate accountability for the day-to-day work of risk management and goal achievement belongs to the board members.

  D. is ultimately accountable for the day-to-day work of risk management and goal achievement, and board members own the risk.

Discussion Question

- Which of the following is **BEST** suited for the review of IT risk analysis results before the results are sent to management for approval and use in decision making?

A. An internal audit review

B. A peer review

C. A compliance review

D. A risk policy review

Task 2.5

Communicate the results of risk assessments to senior management and appropriate stakeholders to enable risk-based decision making.

Task to Knowledge Statements

Certified in Risk and Information Systems Control™ (CRISC™) An ISACA® Certification

How does Task 2.5 relate to each of the following knowledge statements?

Knowledge Statement	Connection
14. Organizational structures	Organizational structure both within the risk management function as well as the enterprise overall play a role in how an organization communicates about risk assessment results.
23. Principles of risk and control ownership	Each risk scenario should be assigned to a risk owner to make sure the assessment results are thoroughly analyzed and corrective actions are taken as necessary.
28. Information security concepts and principles, including confidentiality, integrity and availability of information	Generally speaking, senior leadership and appropriate stakeholders need to know the results of assessment regarding the potential impacts regarding the confidentiality, integrity and availability of systems or information/data.

Risk Assessment Report

- The results of the risk assessment process should be compiled into a risk assessment report and submitted to senior management.
- As possible, the report should also include the recommended response(s) to the risk.
- Note that these recommendations may not be followed by management during the response and mitigation phase.

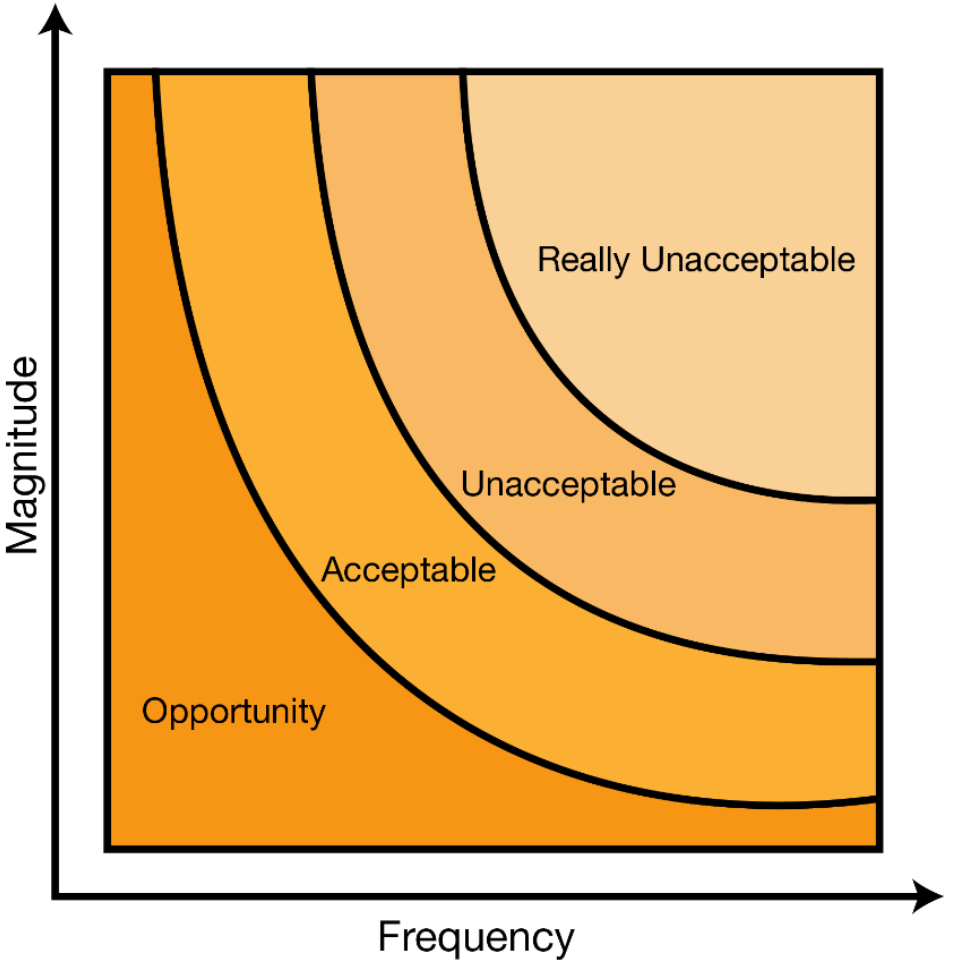
Report All Risk

- All risk items should be noted in the risk assessment report, including issues that have already been resolved. This ensures the following:
  - There is a record of the detected risk and actions taken to resolve the risk.
  - A control put in place to resolve the risk is not inadvertently removed.
  - There will be no concern that the risk was simply missed during the identification and assessment processes.
- It is also a good practice to include information regarding the following:
  - External or internal factors affecting an assessment of a risk
  - Any assumptions that were used to assess a given risk
  - Any potential unknown factors affecting the reliability of the assessment

Ensure Understanding

- To perform the following, it is important to use a consistent method for reporting risk:
  - Facilitate comparisons across time.
  - Ensure that report data is fully understood.
- The report must be clear, concise and accurate.
- Care should be taken to use terminology that is easily understood and interpreted.
- In addition, all risk must be documented in a manner that clearly states the risk levels and priorities.

Risk Appetite Bands



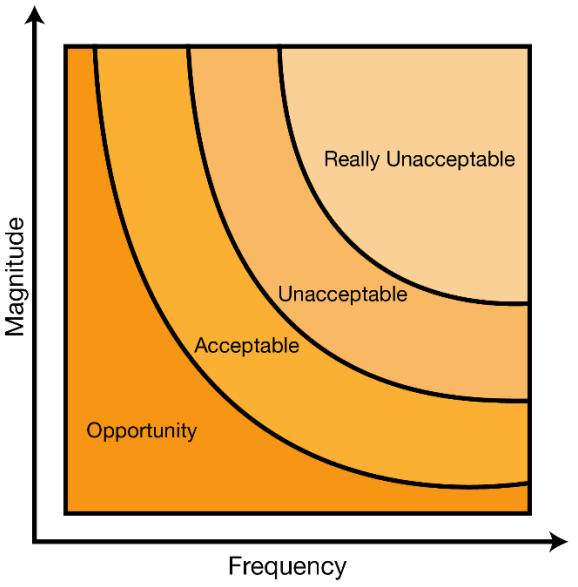
Source: *CRISC Review Manual 6th Edition,* figure 2.9

Discussion Question

- The goal of IT risk analysis is to:
  A. enable the alignment of IT risk management with enterprise risk management (ERM).
  B. enable the prioritization of risk responses.
  C. satisfy legal and regulatory compliance requirements.
  D. identify known threats and vulnerabilities to information assets.

Discussion Question

- What do different risk scenarios on the same bands/curve on a risk map indicate?



A. All risk scenarios on the same curve of a risk map have the same level of risk.

B. All risk scenarios on the same curve of a risk map have the same magnitude of impact.

C. All risk scenarios on the same curve of a risk map require the same risk response.

D. All risk scenarios on the same curve of a risk map are of the same type.

Task 2.6

Update the risk register with the results of the risk assessment.

Task to Knowledge Statements

How does Task 2.6 relate to each of the following knowledge statements?

Knowledge Statement	Connection
11. Elements of a risk register	The risk register contains a summarized account of the assessment process and is updated at regularly, including upon completion of the risk assessment.
12. Risk appetite and tolerance	Management risk appetite and tolerance can change for a variety of reasons. This change can in turn necessitate updates to the risk register.
26. Risk assessment standards, frameworks and techniques	One common element in most risk assessment standards, frameworks and techniques is an emphasis on ensuring that risk is appropriately documented in order to convey the current state.

A “Living” Document

- As an ongoing process with an emphasis on continual improvement, each step of risk management will be repeated on a regular basis.
- One tool that assures the success of this process is the risk register.
- As a living document, the risk register is continuously updated with new data pertaining to the following:
  - Emerging risk
  - Changes in existing risk
  - Resolutions or completion of a risk response
  - Status updates
  - Changes in risk ownership and accountability
- Any new information acquired or learned during the risk assessment phase is also added to the risk register, ensuring that it is both complete and up-to-date.

Focus On: The CIA Triad

- Information security ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability).
- These three elements are referred to as the CIA Triad.
- Triad elements are defined as follows:
  - **Confidentiality**: Pertains to the requirement to maintain the secrecy and privacy of data
  - **Integrity**: The guarding against improper information modification, exclusion or destruction; includes ensuring information nonrepudiation and authenticity
  - **Availability**: Availability refers to ensuring timely and reliable access to and use of information

Focus On: The CIA Triad (cont'd)

- Several practical approaches help to increase information security. These include:

Segregation of duties	• The principle of ensuring that no one person controls an entire transaction or operation that could result in fraudulent acts or errors
Job rotation	• Job rotation is the process of cross-training and developing personnel with various skills that can step in where needed
Mandatory vacation	• Mandatory vacations are used in some organizations as a means to deter and detect fraud; these are often required by law
Secure state	• Consistent protection of a process to ensure that there is no time during a process in which data or a system are vulnerable

Access Control

- One of the most critical risks associated with information systems is the challenge of managing access control.
- Risk is often caused through misuse of access, especially in cases where an individual has a level of access that is not appropriate for his or her current job responsibilities.

The IAAA Model

- Access control is usually addressed through the following, referred to by the acronym IAAA:

Identification	The unique identification of each person or process that uses a system allows tracking and logging of the activity by the user and the possibility to investigate a problem if it were to arise.
Authentication	Authentication is the process of validating an identity. After a person or process has claimed or stated his/her identity, the process of authentication verifies that the person is who they say they are.
Authorization	Refers to the privileges or permissions the person will have, including read-only, write-only, read/write, create, update, delete, full control, etc. This is where the concept of least privilege applies.
Accountability	This action logs or records all activity on a system and indicates the user ID responsible for the activity.

Identity Management

- Identity management is the process of managing the identities of the entities (users, processes, etc.) that require access to information or information systems.
- It is currently one of the most difficult challenges for system administrators.

Identity Authentication

- Identity authentication is usually done using three methods, as follows:

Authentication	Description	Challenge
Knowledge	Requires users to know a password, code phrase or other secret value to validate their identity	The risk in this method of authentication is that learning the password of another person allows an individual other than the password owner to log in.
Ownership (possession)	Requires the use of a smart card, token, ID badge or other similar item; a person validates their identity by possessing the item	The cost of installing this type of system, issuing the cards and operating and maintaining the system may be prohibitive. Also, in the event the authorized user loses his or her card, it may be used by an imposter if the card has not been reported as lost or stolen.
Characteristic (biometrics)	Uses either physiological (e.g., fingerprints, iris scan, palm scan) or behavioral (e.g., voice print, signature dynamics) elements to authenticate a person	Biometrics is expensive, and some users find it to be intrusive and may be resistant to it.

Discussion Question

- Risk assessments should be repeated at regular intervals because:
  A. omissions in earlier assessments can be addressed.
  B. periodic assessments allow various methodologies.
  C. business threats are constantly changing.
  D. they help raise risk awareness among staff.

Discussion Question

- Once a risk assessment has been completed, the documented test results should be:
  A. destroyed.
  B. retained.
  C. summarized.
  D. published.

Identify and apply risk assessment techniques.

- A wide variety of risk assessment techniques are available to the risk practitioner.
- In general, these fall into one of three categories:
  - Quantitative
  - Qualitative
  - Semiqualitative

Analyze risk scenarios.

- The impact of a risk event is difficult to calculate with any degree of accuracy because there are many factors that affect the outcome of an event.
- Some factors that can affect risk assessment include the following:
  - Organizational structure and culture
  - Policies, standards and procedures
  - Technology and technology architecture

Identify current state of controls.

- Current state refers to the condition of controls at a point in time.
- To determine the current state of controls, the following data sources are used:
  - Regular reports generated by controls
  - Results of control testing activities
  - Results of incident management programs

Learning Objective 4

Certified in Risk and Information Systems Control™
An ISACA® Certification

Assess gaps between current and desired states of the IT risk environment.

- Gap analysis is a process of reviewing data sources to learn about the current state of IT risk.
- The results of this analysis are compared to the desired states.
- The difference is a gap that may be narrowed through focused action.

Communicate IT risk assessment results to relevant stakeholders.

- The responsibility of risk ownership must be assigned to individuals (not departments or organizations) with the authority to take action to respond to risk.
- Regular communications is one method of ensuring that senior leadership and other stakeholders are aware of the current state of IT risk management.


CRISC™
Certified in Risk and Information Systems Control™
An ISACA® Certification

THANK YOU!