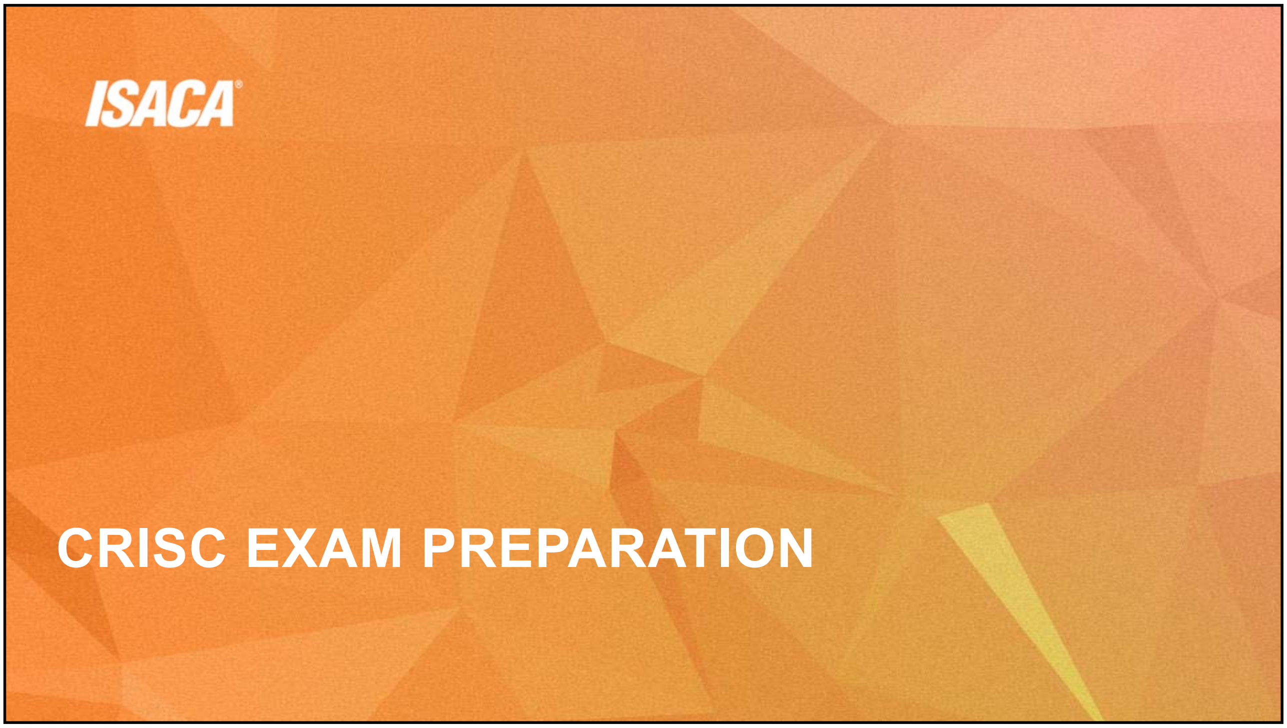
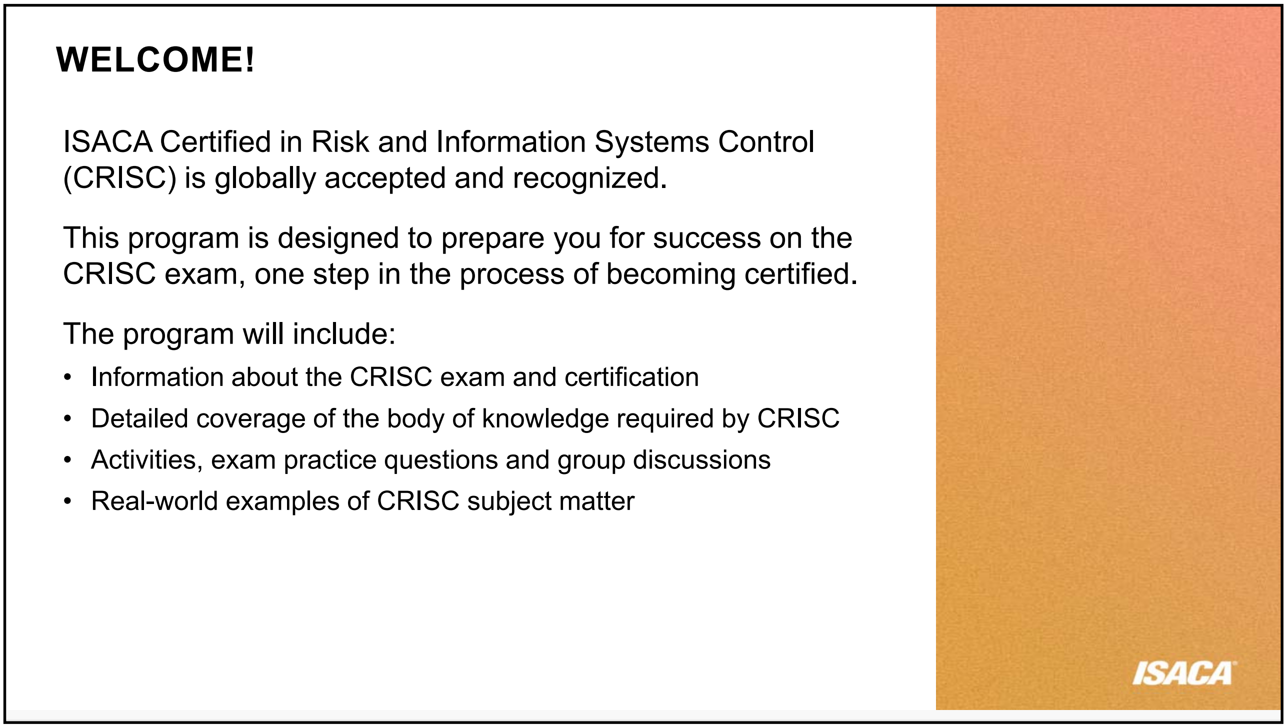


CRISC EXAM PREPARATION

ABOUT THE CRISC EXAM



WELCOME!

ISACA Certified in Risk and Information Systems Control (CRISC) is globally accepted and recognized.

This program is designed to prepare you for success on the CRISC exam, one step in the process of becoming certified.

The program will include:

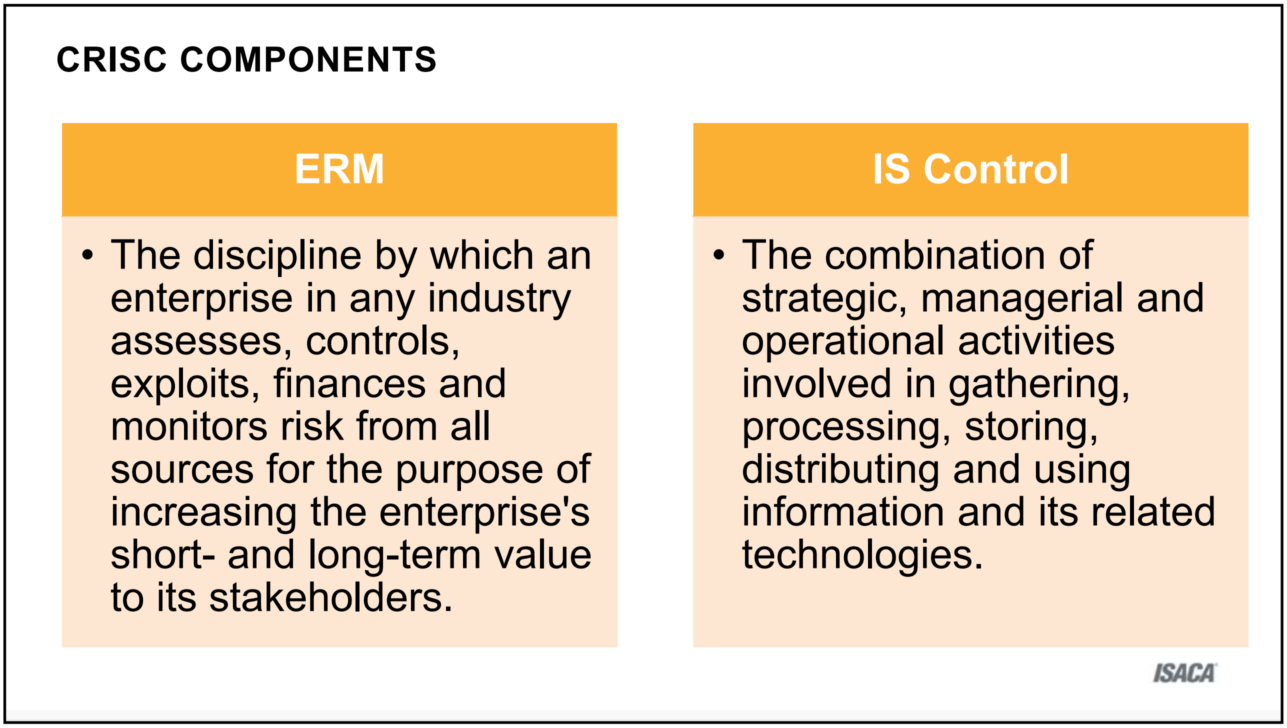
- Information about the CRISC exam and certification
- Detailed coverage of the body of knowledge required by CRISC
- Activities, exam practice questions and group discussions
- Real-world examples of CRISC subject matter

CRISC CERTIFICATION

The CRISC professional demonstrates skills in both of the following:

- Enterprise risk management (ERM)
- Information system (IS) control

CRISC addresses the need for professionals who understand both technology and how to implement and align effective risk management and control frameworks with enterprise goals.



CRISC COMPONENTS

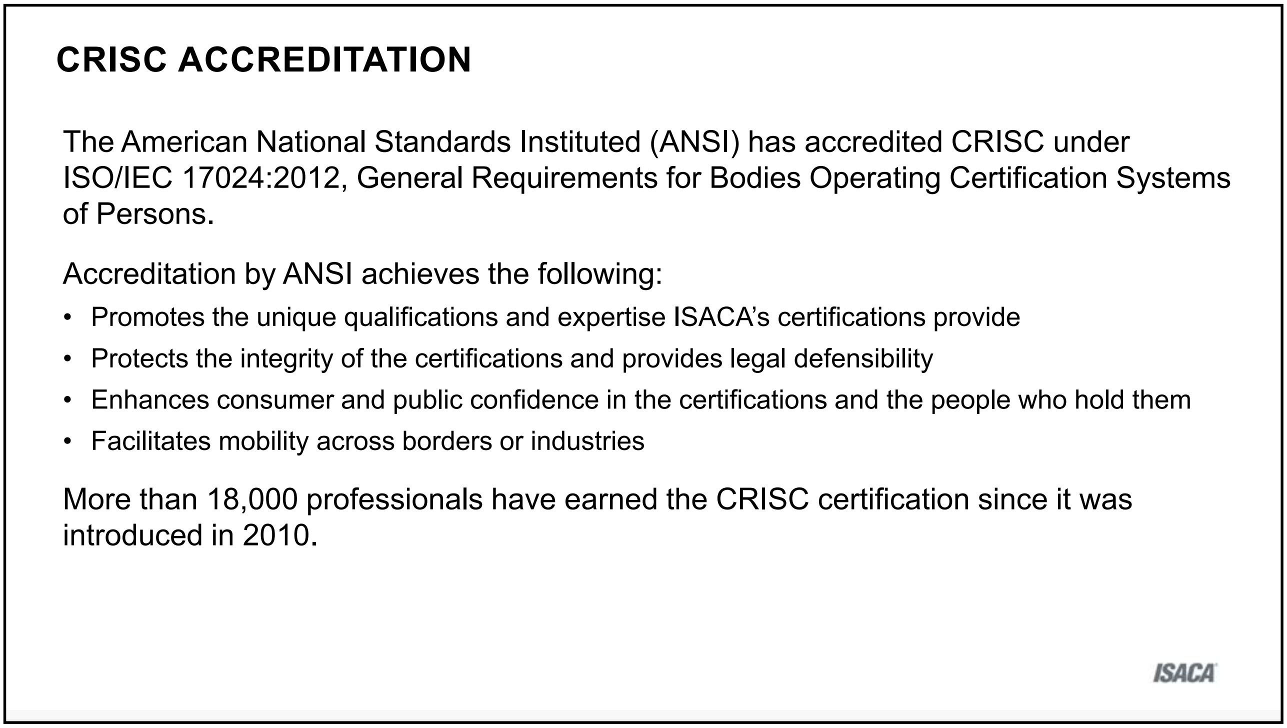
ERM

- The discipline by which an enterprise in any industry assesses, controls, exploits, finances and monitors risk from all sources for the purpose of increasing the enterprise's short- and long-term value to its stakeholders.

IS Control

- The combination of strategic, managerial and operational activities involved in gathering, processing, storing, distributing and using information and its related technologies.

ISACA



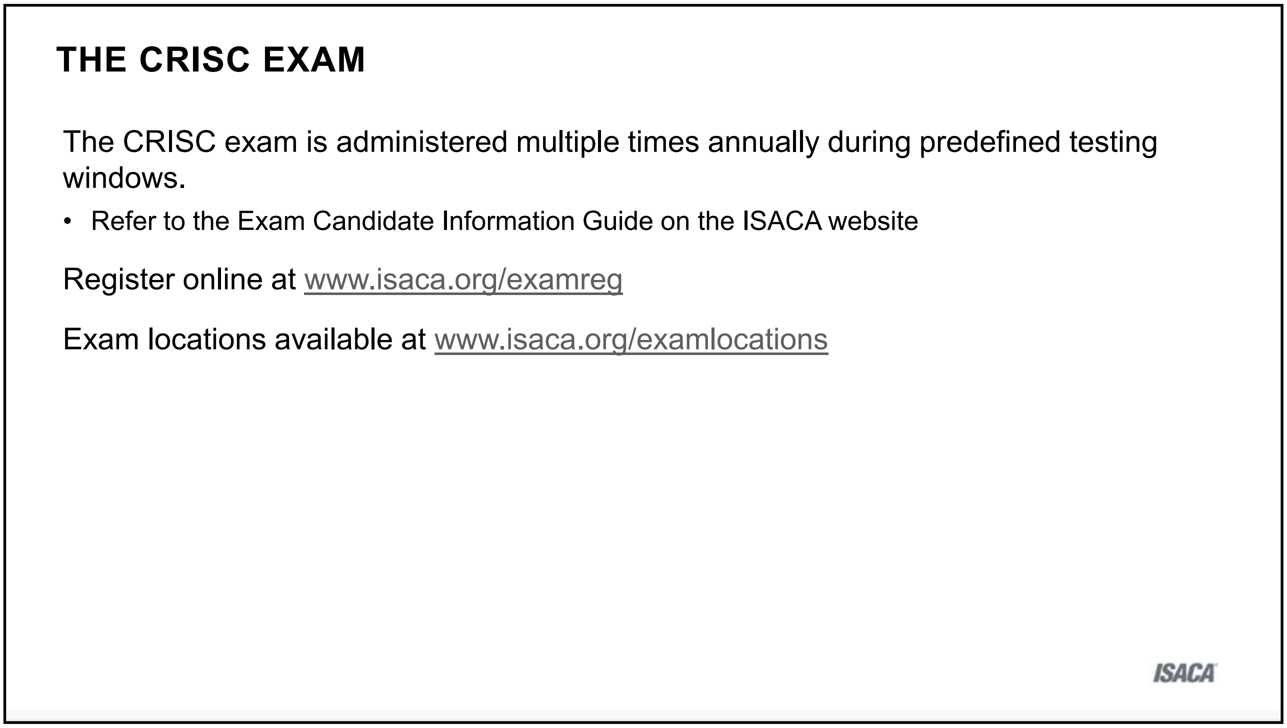
CRISC ACCREDITATION

The American National Standards Instituted (ANSI) has accredited CRISC under ISO/IEC 17024:2012, General Requirements for Bodies Operating Certification Systems of Persons.

Accreditation by ANSI achieves the following:

- Promotes the unique qualifications and expertise ISACA’s certifications provide
- Protects the integrity of the certifications and provides legal defensibility
- Enhances consumer and public confidence in the certifications and the people who hold them
- Facilitates mobility across borders or industries

More than 18,000 professionals have earned the CRISC certification since it was introduced in 2010.



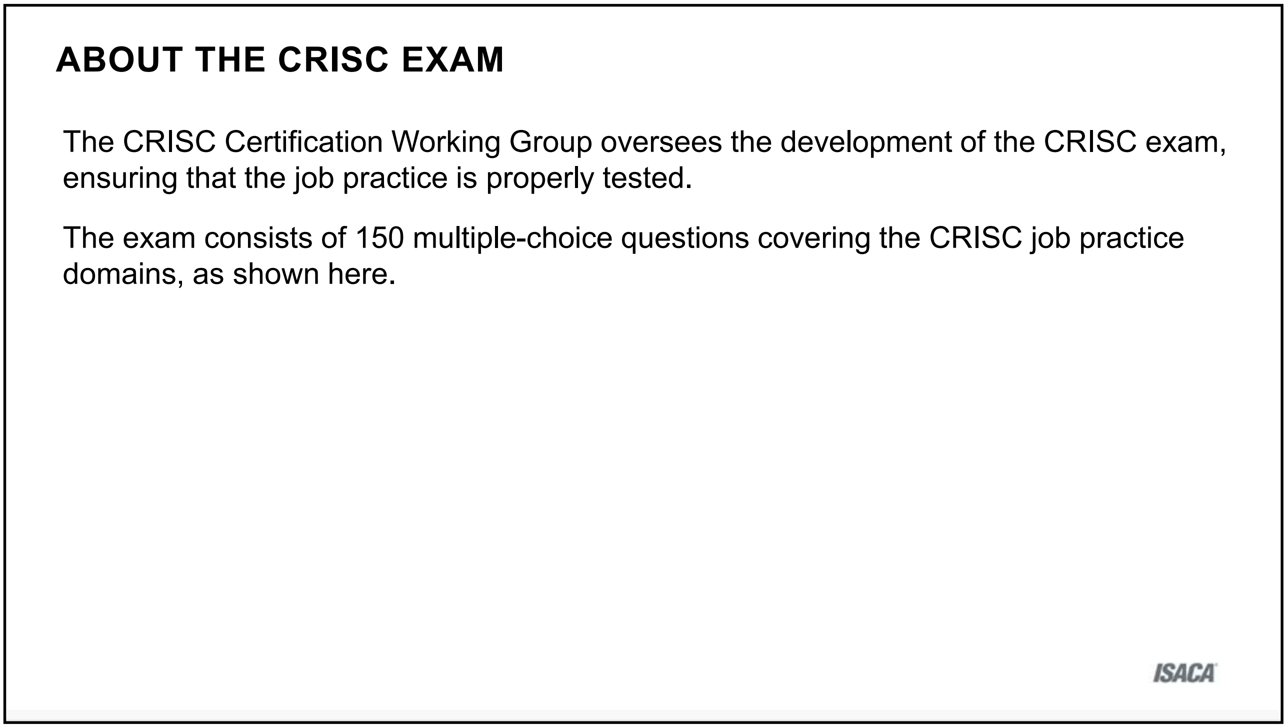
THE CRISC EXAM

The CRISC exam is administered multiple times annually during predefined testing windows.

- Refer to the Exam Candidate Information Guide on the ISACA website

Register online at www.isaca.org/examreg

Exam locations available at www.isaca.org/examlocations

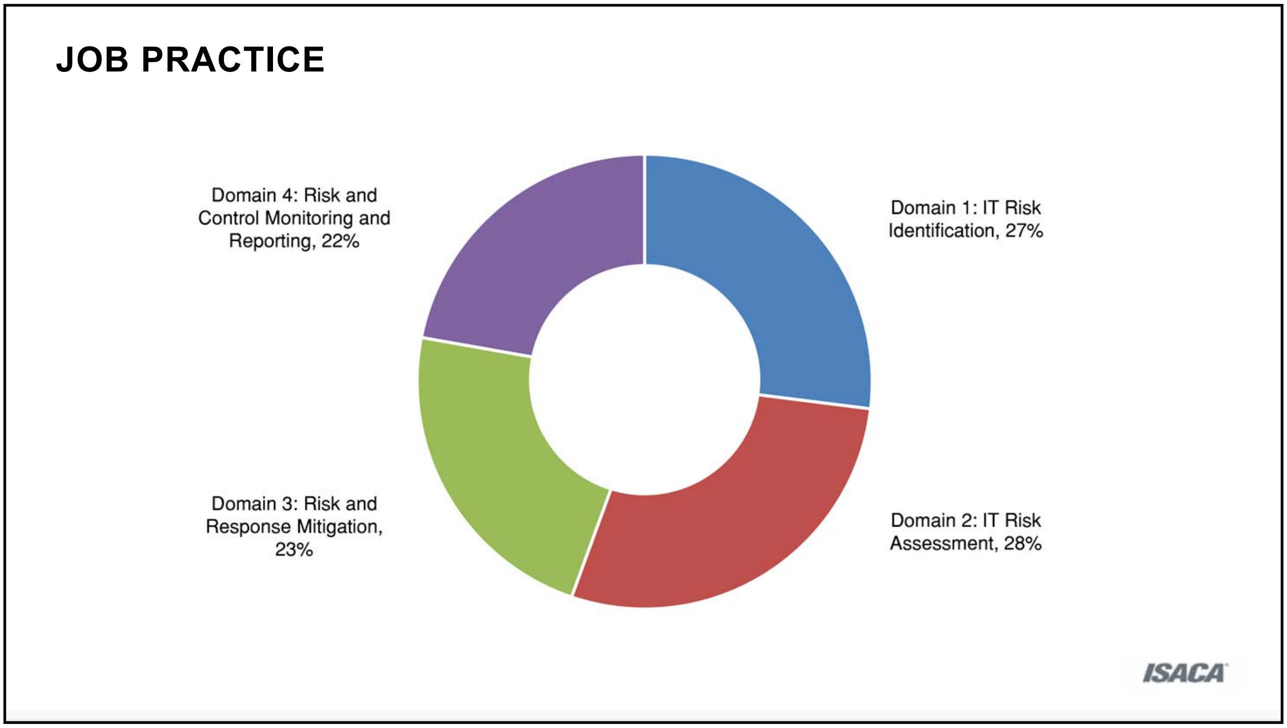


ABOUT THE CRISC EXAM

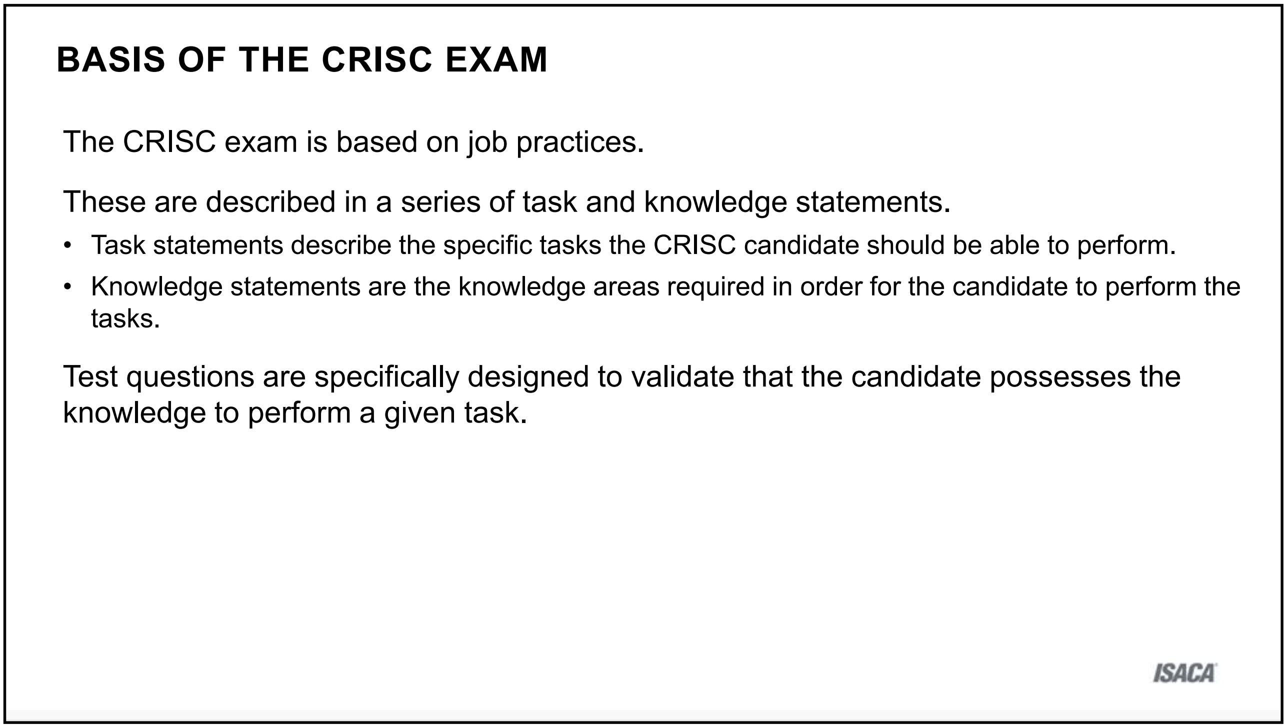
The CRISC Certification Working Group oversees the development of the CRISC exam, ensuring that the job practice is properly tested.

The exam consists of 150 multiple-choice questions covering the CRISC job practice domains, as shown here.

ISACA



JOB PRACTICE



BASIS OF THE CRISC EXAM

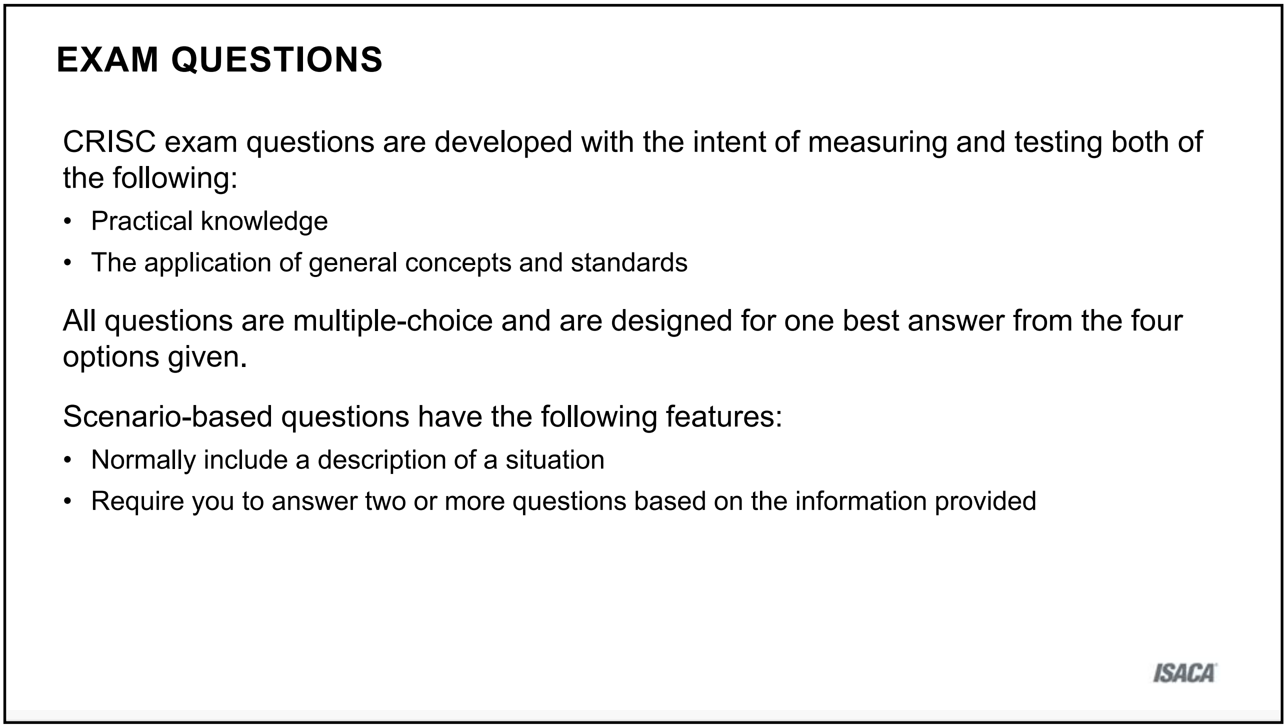
The CRISC exam is based on job practices.

These are described in a series of task and knowledge statements.

- Task statements describe the specific tasks the CRISC candidate should be able to perform.
- Knowledge statements are the knowledge areas required in order for the candidate to perform the tasks.

Test questions are specifically designed to validate that the candidate possesses the knowledge to perform a given task.

ISACA



EXAM QUESTIONS

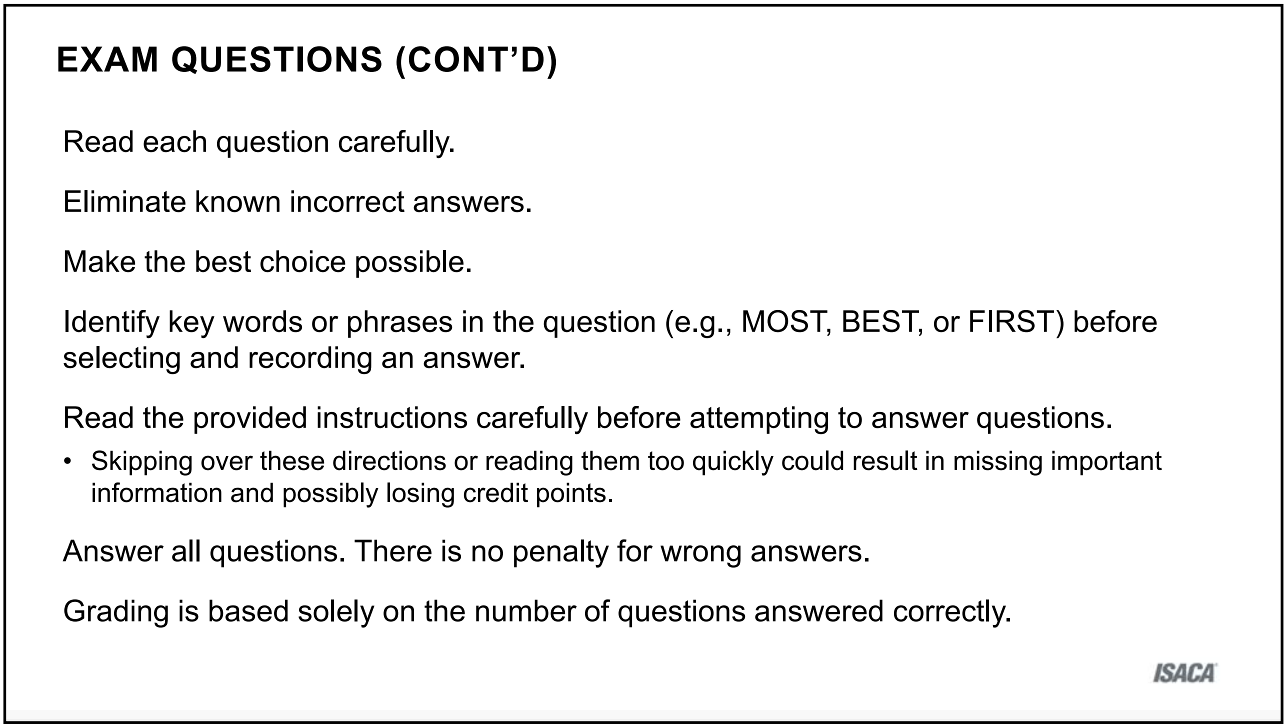
CRISC exam questions are developed with the intent of measuring and testing both of the following:

- Practical knowledge
- The application of general concepts and standards

All questions are multiple-choice and are designed for one best answer from the four options given.

Scenario-based questions have the following features:

- Normally include a description of a situation
- Require you to answer two or more questions based on the information provided



EXAM QUESTIONS (CONT’D)

Read each question carefully.

Eliminate known incorrect answers.

Make the best choice possible.

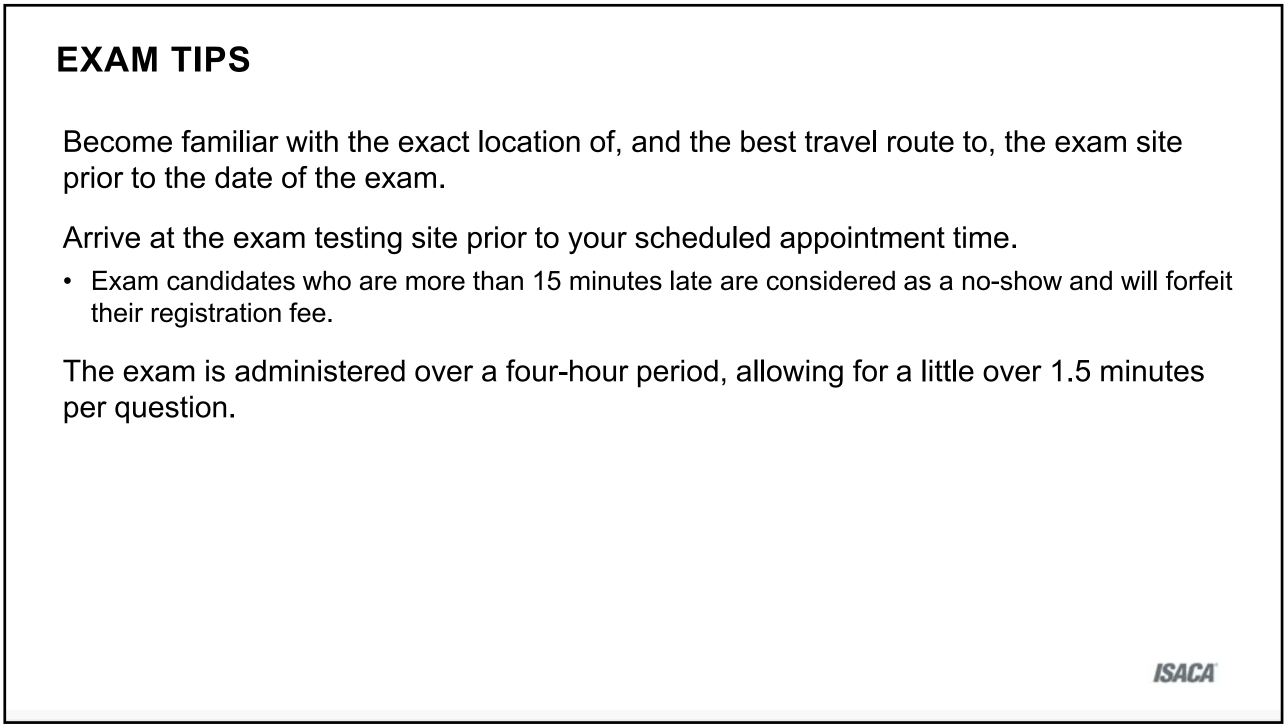
Identify key words or phrases in the question (e.g., MOST, BEST, or FIRST) before selecting and recording an answer.

Read the provided instructions carefully before attempting to answer questions.

- Skipping over these directions or reading them too quickly could result in missing important information and possibly losing credit points.

Answer all questions. There is no penalty for wrong answers.

Grading is based solely on the number of questions answered correctly.



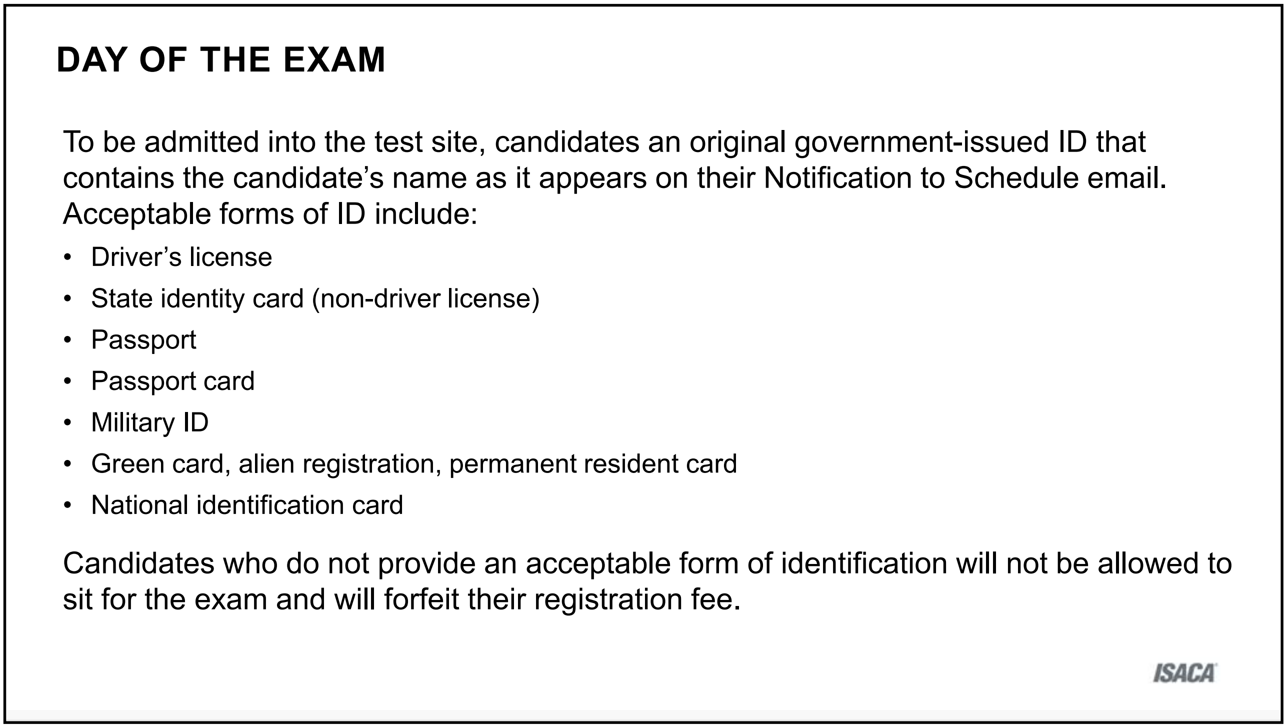
EXAM TIPS

Become familiar with the exact location of, and the best travel route to, the exam site prior to the date of the exam.

Arrive at the exam testing site prior to your scheduled appointment time.

- Exam candidates who are more than 15 minutes late are considered as a no-show and will forfeit their registration fee.

The exam is administered over a four-hour period, allowing for a little over 1.5 minutes per question.

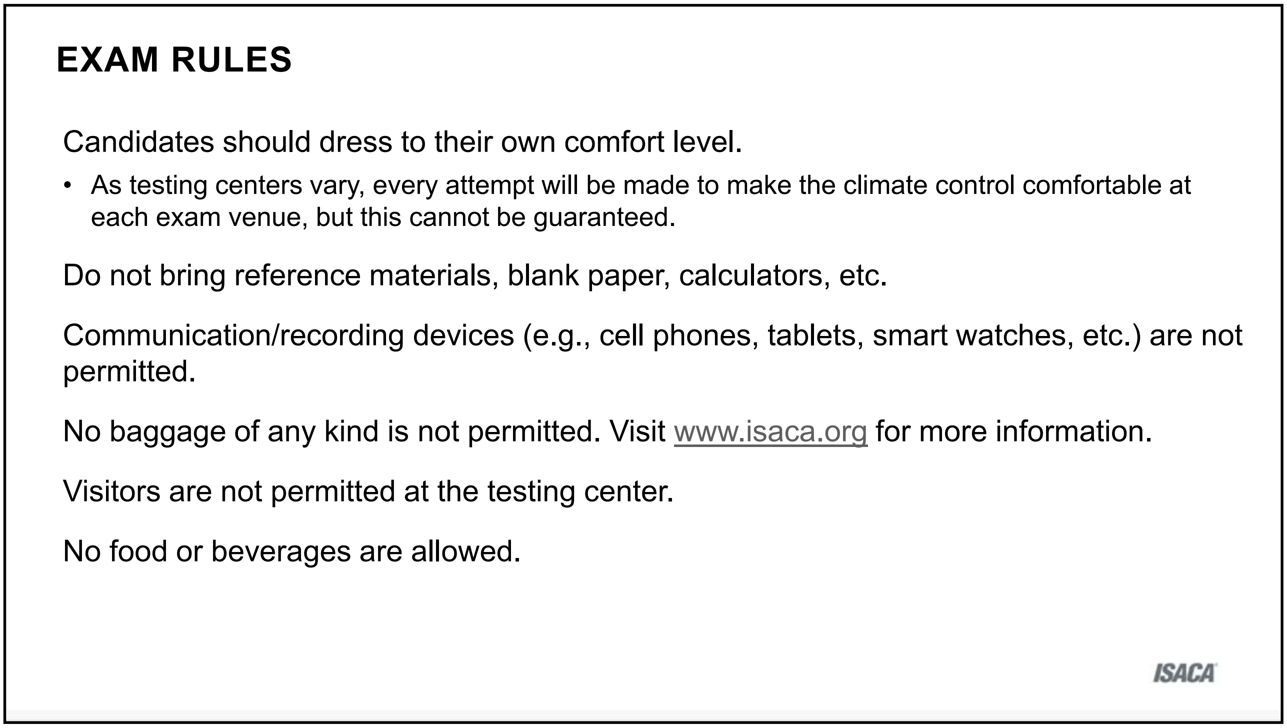


DAY OF THE EXAM

To be admitted into the test site, candidates an original government-issued ID that contains the candidate’s name as it appears on their Notification to Schedule email. Acceptable forms of ID include:

- Driver’s license
- State identity card (non-driver license)
- Passport
- Passport card
- Military ID
- Green card, alien registration, permanent resident card
- National identification card

Candidates who do not provide an acceptable form of identification will not be allowed to sit for the exam and will forfeit their registration fee.



EXAM RULES

Candidates should dress to their own comfort level.

- As testing centers vary, every attempt will be made to make the climate control comfortable at each exam venue, but this cannot be guaranteed.

Do not bring reference materials, blank paper, calculators, etc.

Communication/recording devices (e.g., cell phones, tablets, smart watches, etc.) are not permitted.

No baggage of any kind is not permitted. Visit www.isaca.org for more information.

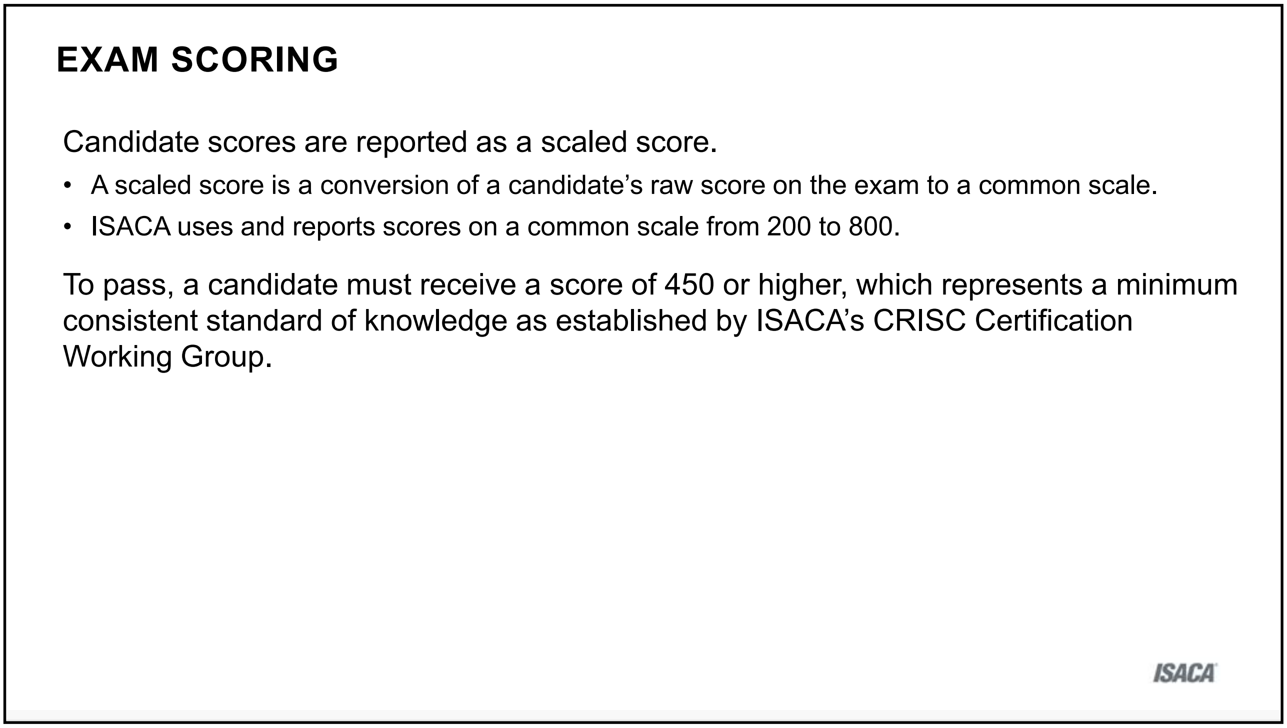
Visitors are not permitted at the testing center.

No food or beverages are allowed.

EXAM RULES (CONT'D)

Candidates must gain authorization by a test proctor to leave the testing area. The proctor will pause the exam whenever a candidate leaves the testing station or an interruption occurs. If the reason for the interruption is not confirmed as an emergency, the test will end.

Candidates may leave the testing area with authorization during the examination to visit the facilities. Candidates will be required to check-out and check-in again upon re-entering the testing area. Note the examination time will not stop and no extra time will be allotted.

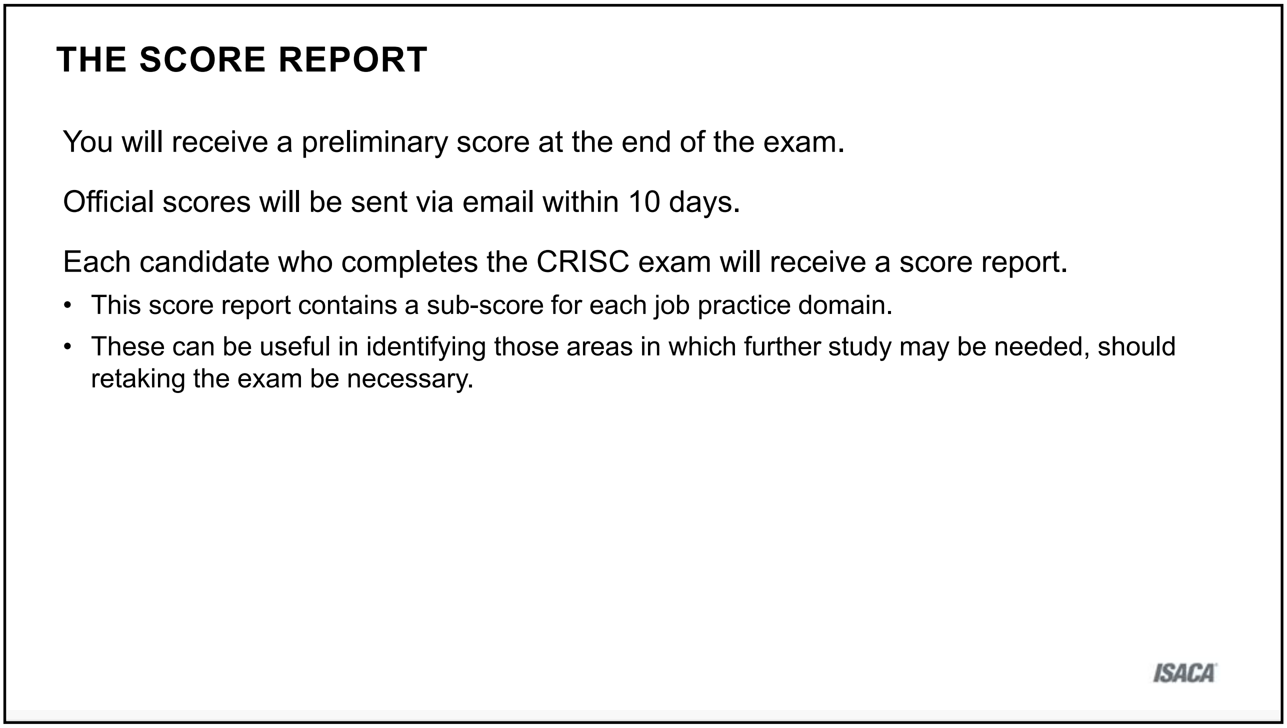


EXAM SCORING

Candidate scores are reported as a scaled score.

- A scaled score is a conversion of a candidate's raw score on the exam to a common scale.
- ISACA uses and reports scores on a common scale from 200 to 800.

To pass, a candidate must receive a score of 450 or higher, which represents a minimum consistent standard of knowledge as established by ISACA's CRISC Certification Working Group.



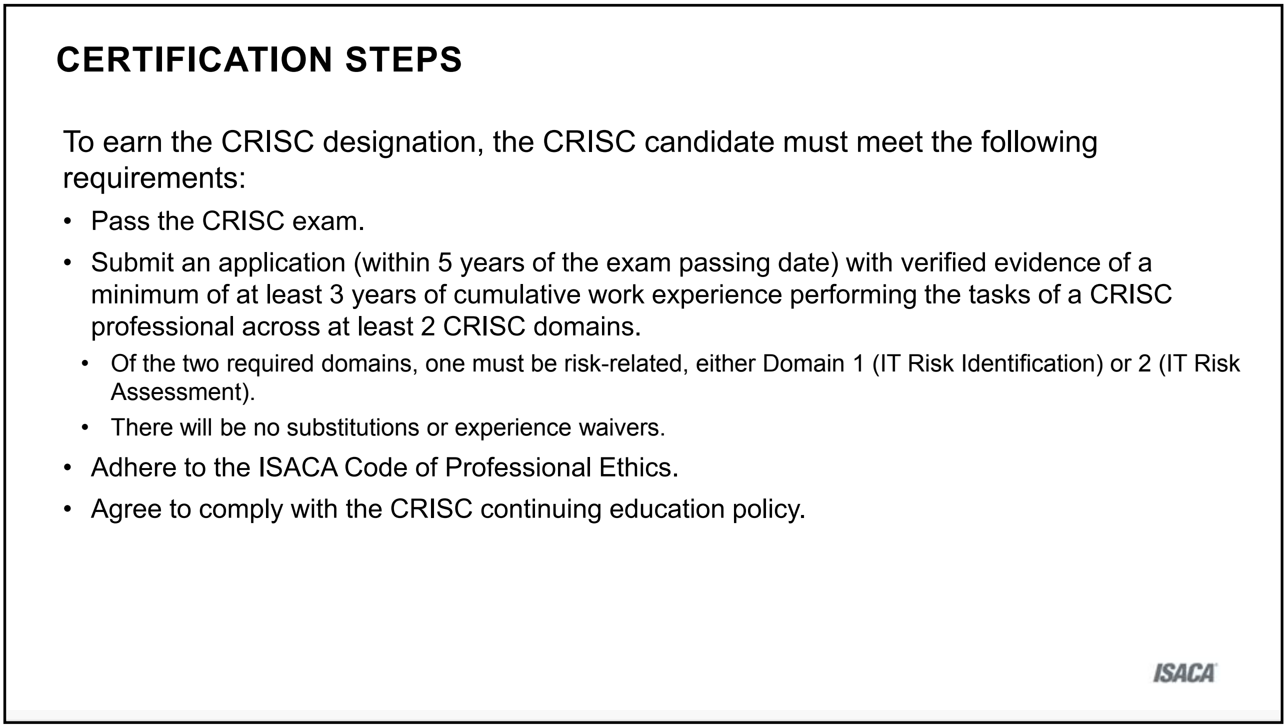
THE SCORE REPORT

You will receive a preliminary score at the end of the exam.

Official scores will be sent via email within 10 days.

Each candidate who completes the CRISC exam will receive a score report.

- This score report contains a sub-score for each job practice domain.
- These can be useful in identifying those areas in which further study may be needed, should retaking the exam be necessary.



CERTIFICATION STEPS

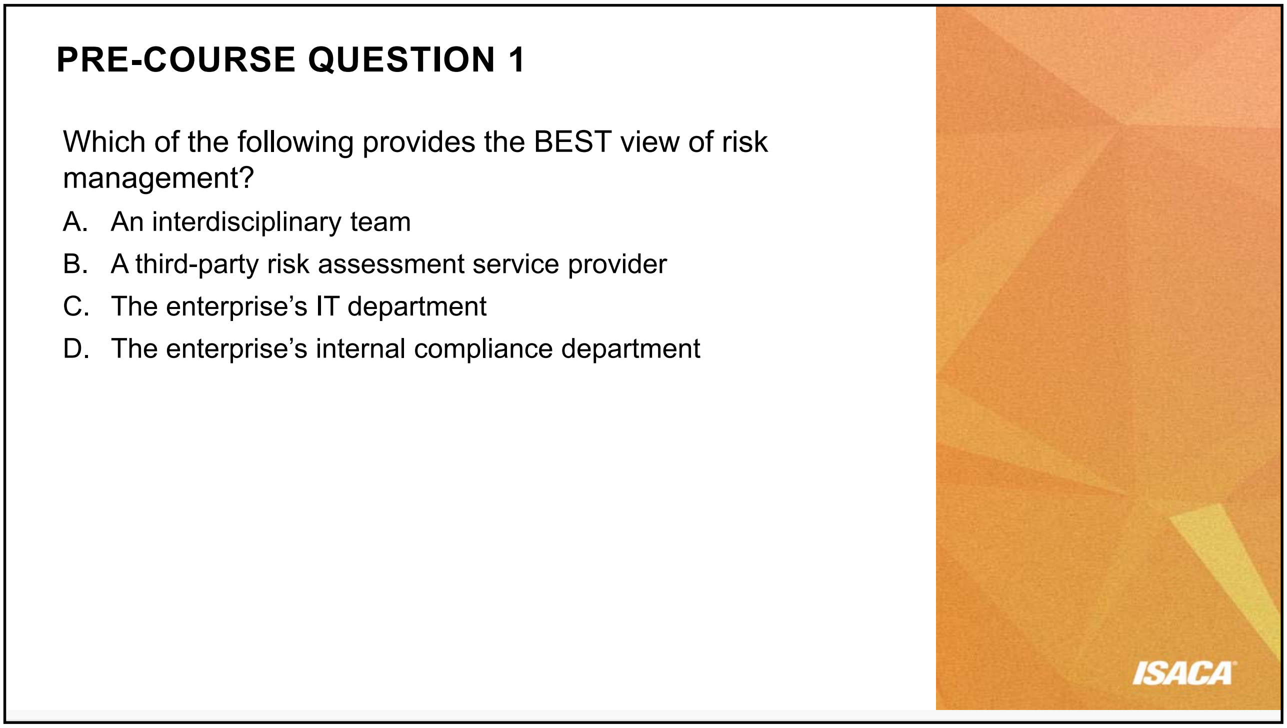
To earn the CRISC designation, the CRISC candidate must meet the following requirements:

- Pass the CRISC exam.
- Submit an application (within 5 years of the exam passing date) with verified evidence of a minimum of at least 3 years of cumulative work experience performing the tasks of a CRISC professional across at least 2 CRISC domains.
  - Of the two required domains, one must be risk-related, either Domain 1 (IT Risk Identification) or 2 (IT Risk Assessment).
  - There will be no substitutions or experience waivers.
- Adhere to the ISACA Code of Professional Ethics.
- Agree to comply with the CRISC continuing education policy.

ISACA

PRE-COURSE QUESTIONS

20



PRE-COURSE QUESTION 1

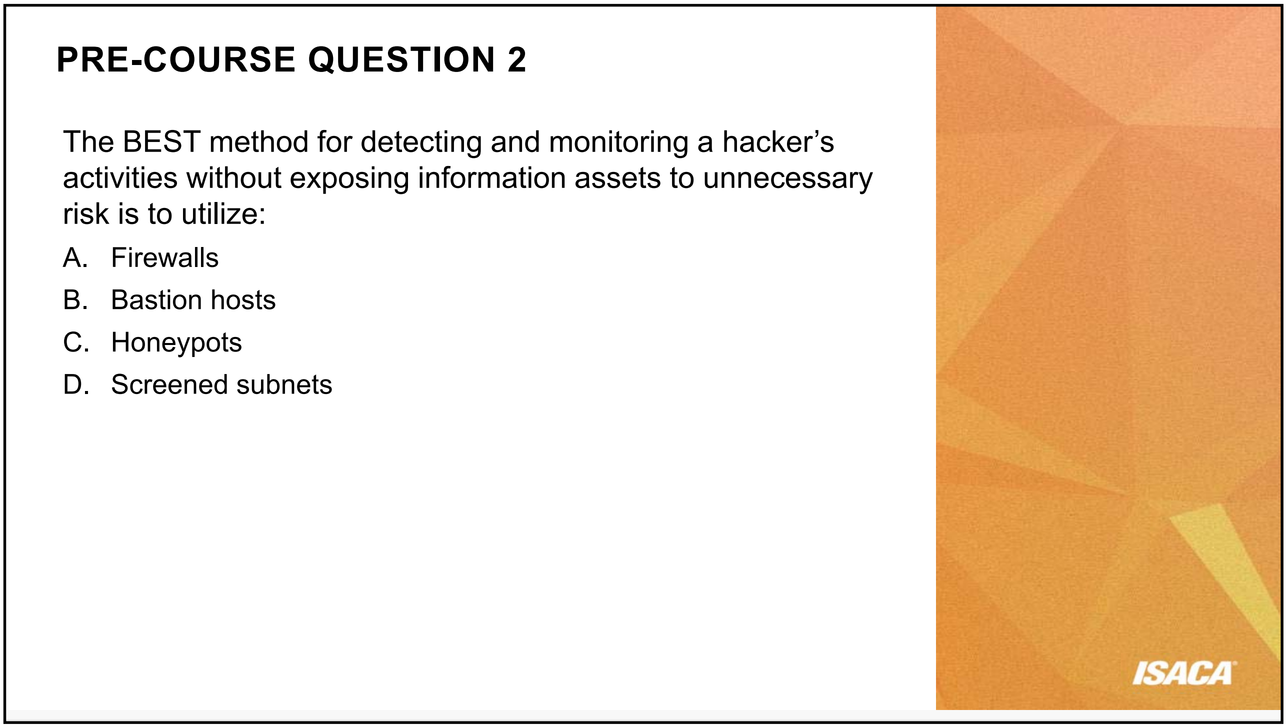
Which of the following provides the BEST view of risk management?

A. An interdisciplinary team

B. A third-party risk assessment service provider

C. The enterprise’s IT department

D. The enterprise’s internal compliance department



PRE-COURSE QUESTION 2

The BEST method for detecting and monitoring a hacker’s activities without exposing information assets to unnecessary risk is to utilize:

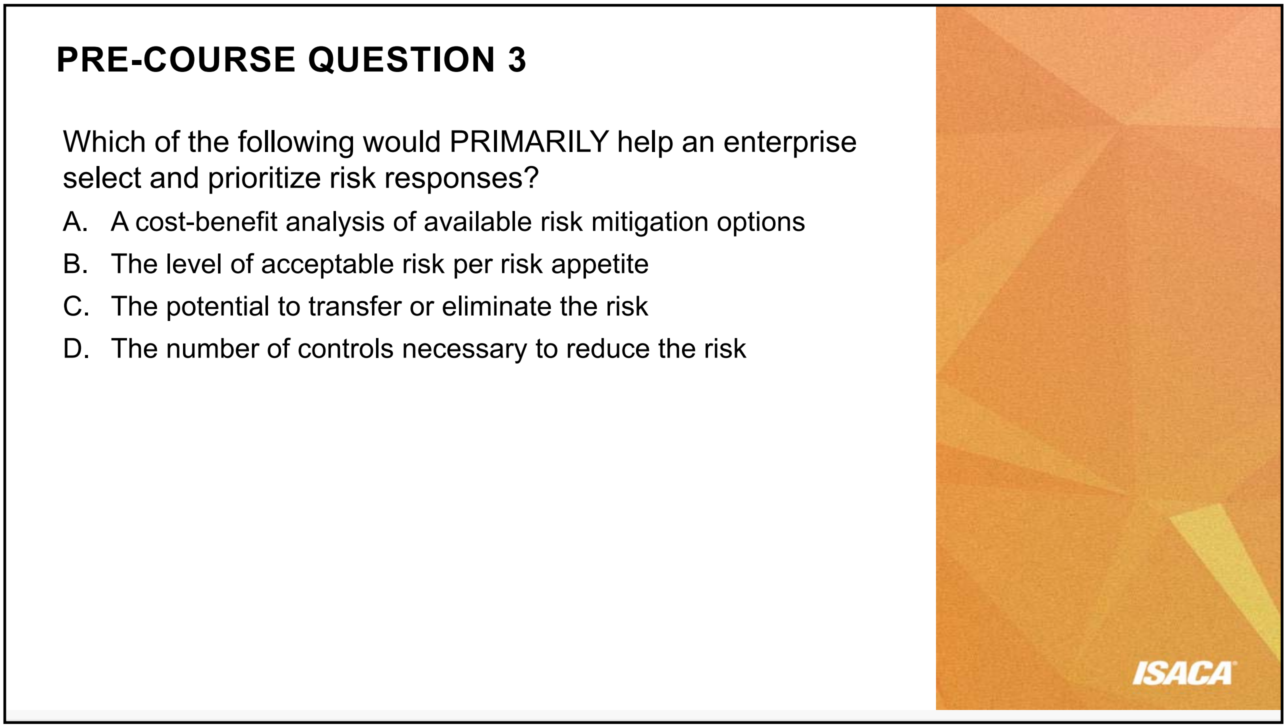
A. Firewalls

B. Bastion hosts

C. Honeypots

D. Screened subnets

ISACA



PRE-COURSE QUESTION 3

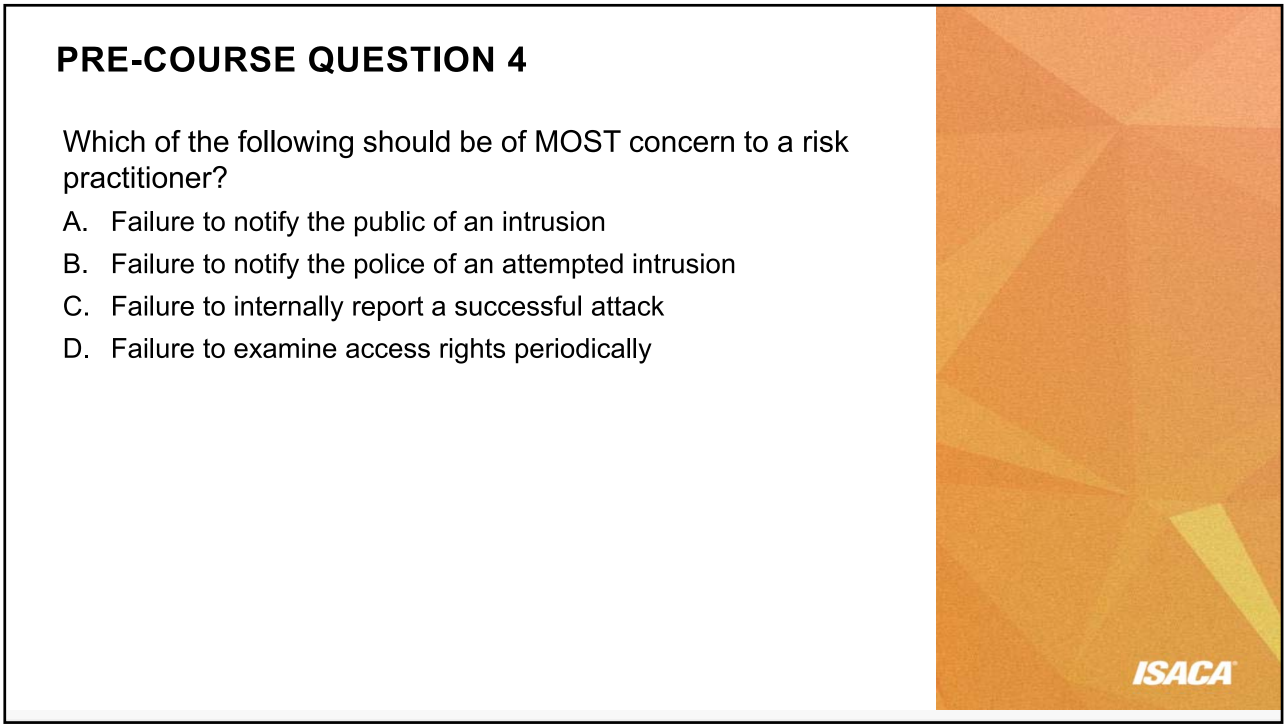
Which of the following would PRIMARILY help an enterprise select and prioritize risk responses?

A. A cost-benefit analysis of available risk mitigation options

B. The level of acceptable risk per risk appetite

C. The potential to transfer or eliminate the risk

D. The number of controls necessary to reduce the risk



PRE-COURSE QUESTION 4

Which of the following should be of MOST concern to a risk practitioner?

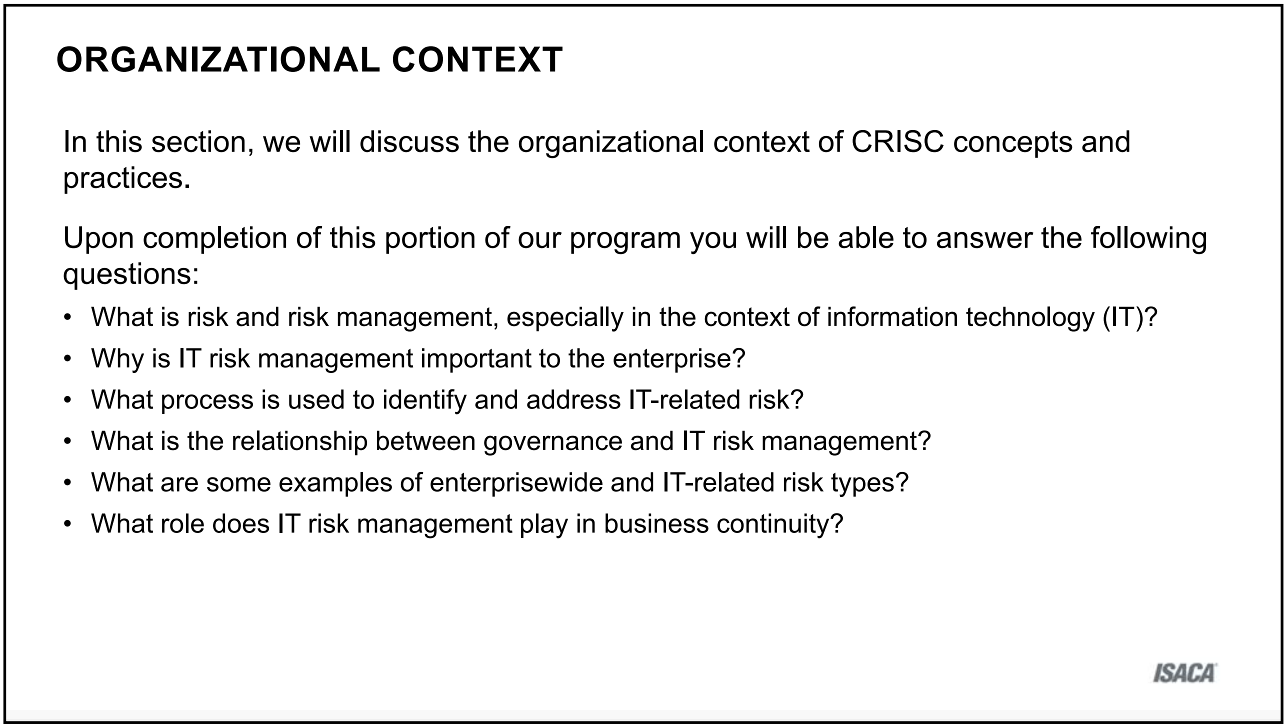
A. Failure to notify the public of an intrusion

B. Failure to notify the police of an attempted intrusion

C. Failure to internally report a successful attack

D. Failure to examine access rights periodically

THE CONTEXT OF IT RISK MANAGEMENT



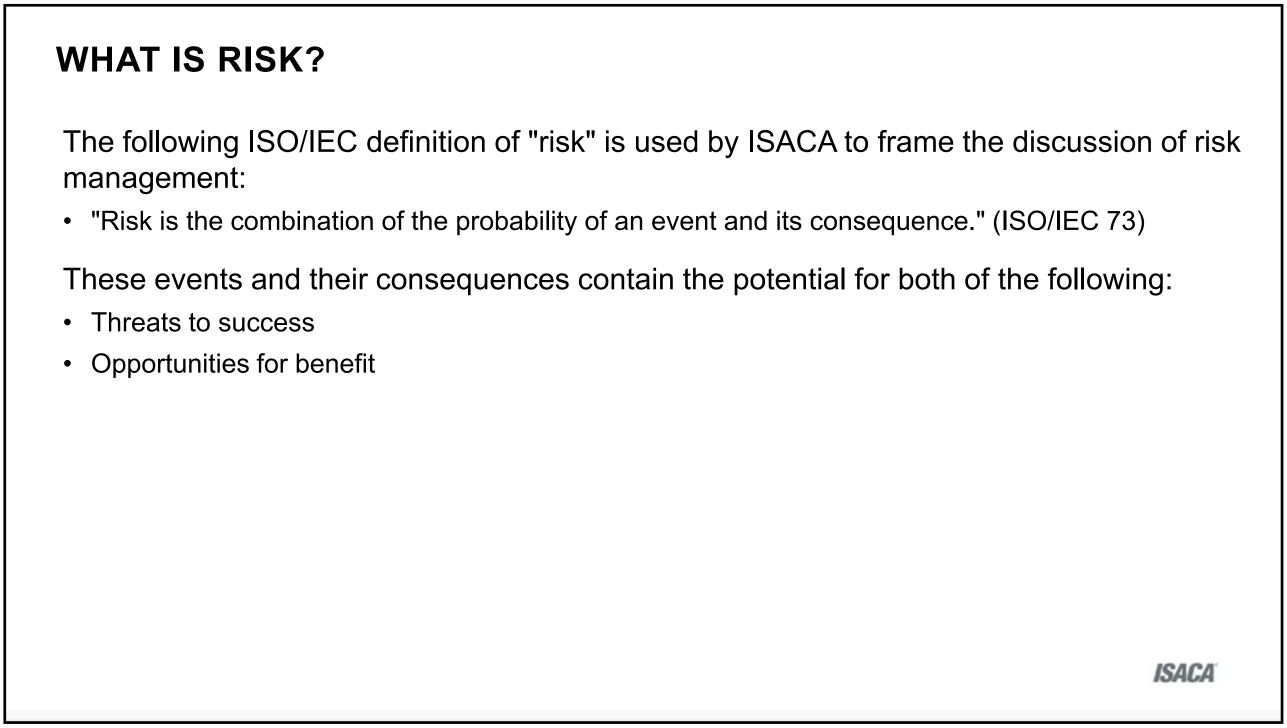
ORGANIZATIONAL CONTEXT

In this section, we will discuss the organizational context of CRISC concepts and practices.

Upon completion of this portion of our program you will be able to answer the following questions:

- What is risk and risk management, especially in the context of information technology (IT)?
- Why is IT risk management important to the enterprise?
- What process is used to identify and address IT-related risk?
- What is the relationship between governance and IT risk management?
- What are some examples of enterprisewide and IT-related risk types?
- What role does IT risk management play in business continuity?

ISACA



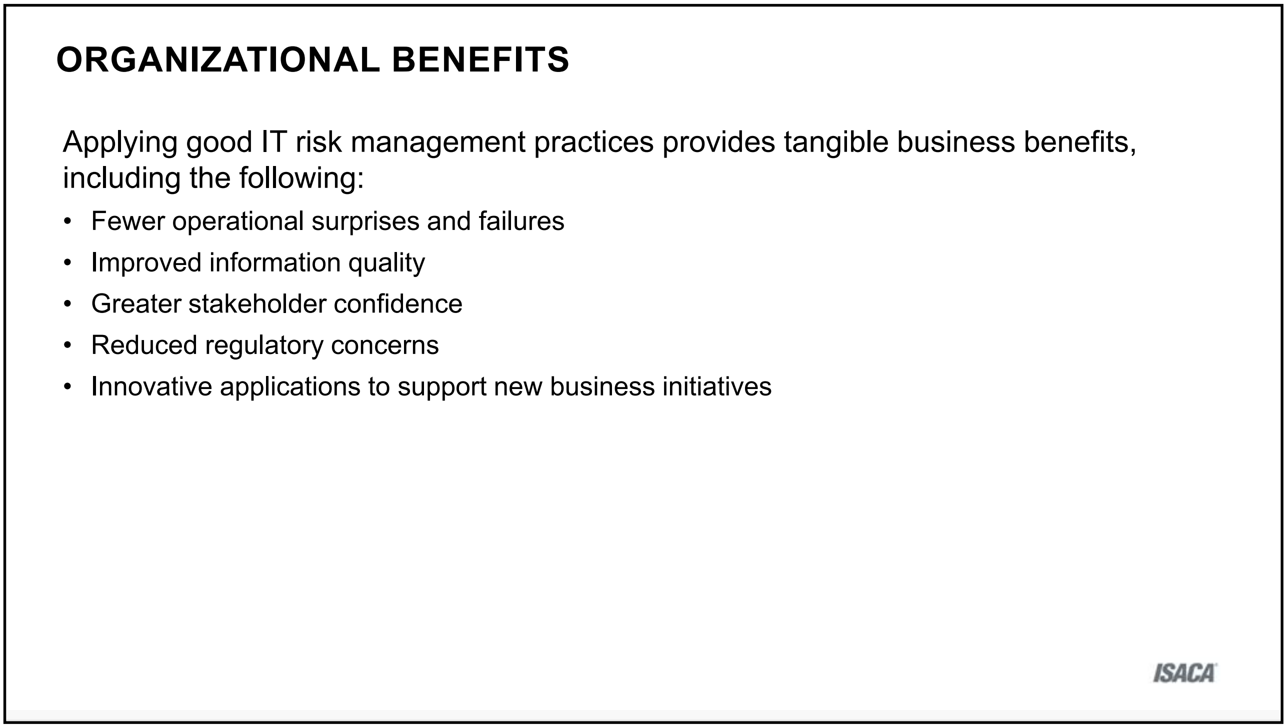
WHAT IS RISK?

The following ISO/IEC definition of "risk" is used by ISACA to frame the discussion of risk management:

- "Risk is the combination of the probability of an event and its consequence." (ISO/IEC 73)

These events and their consequences contain the potential for both of the following:

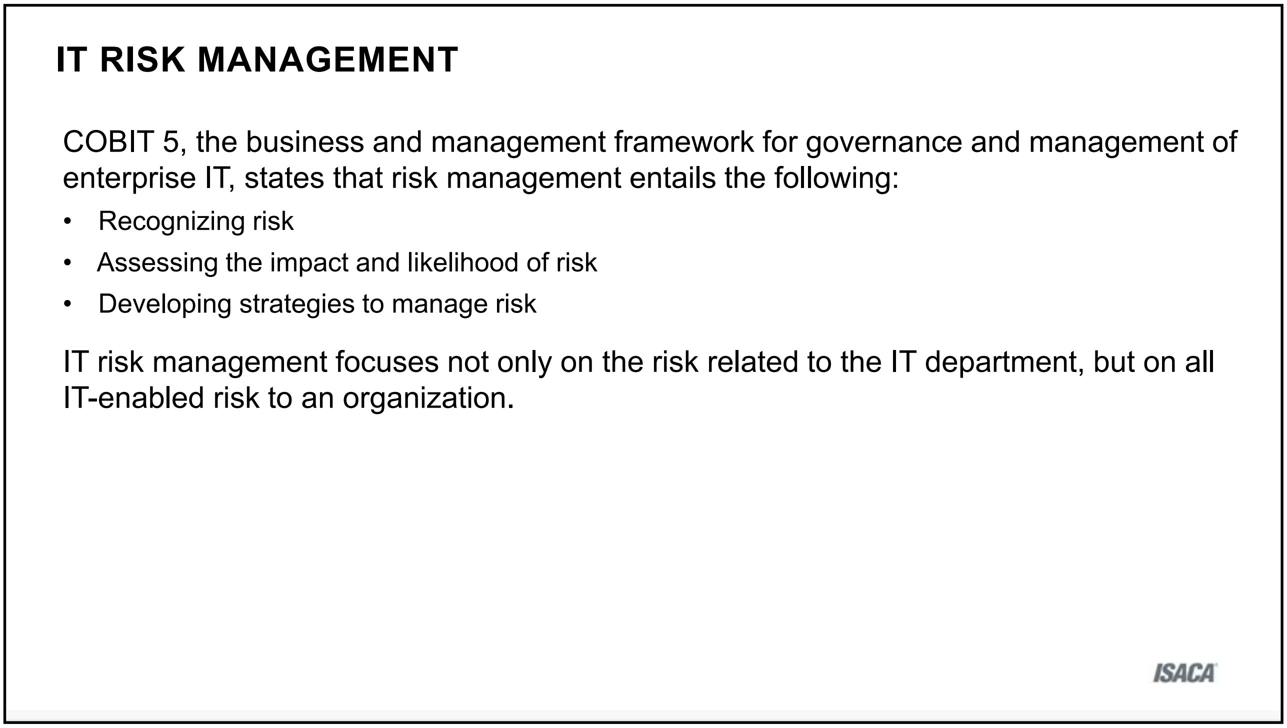
- Threats to success
- Opportunities for benefit



ORGANIZATIONAL BENEFITS

Applying good IT risk management practices provides tangible business benefits, including the following:

- Fewer operational surprises and failures
- Improved information quality
- Greater stakeholder confidence
- Reduced regulatory concerns
- Innovative applications to support new business initiatives

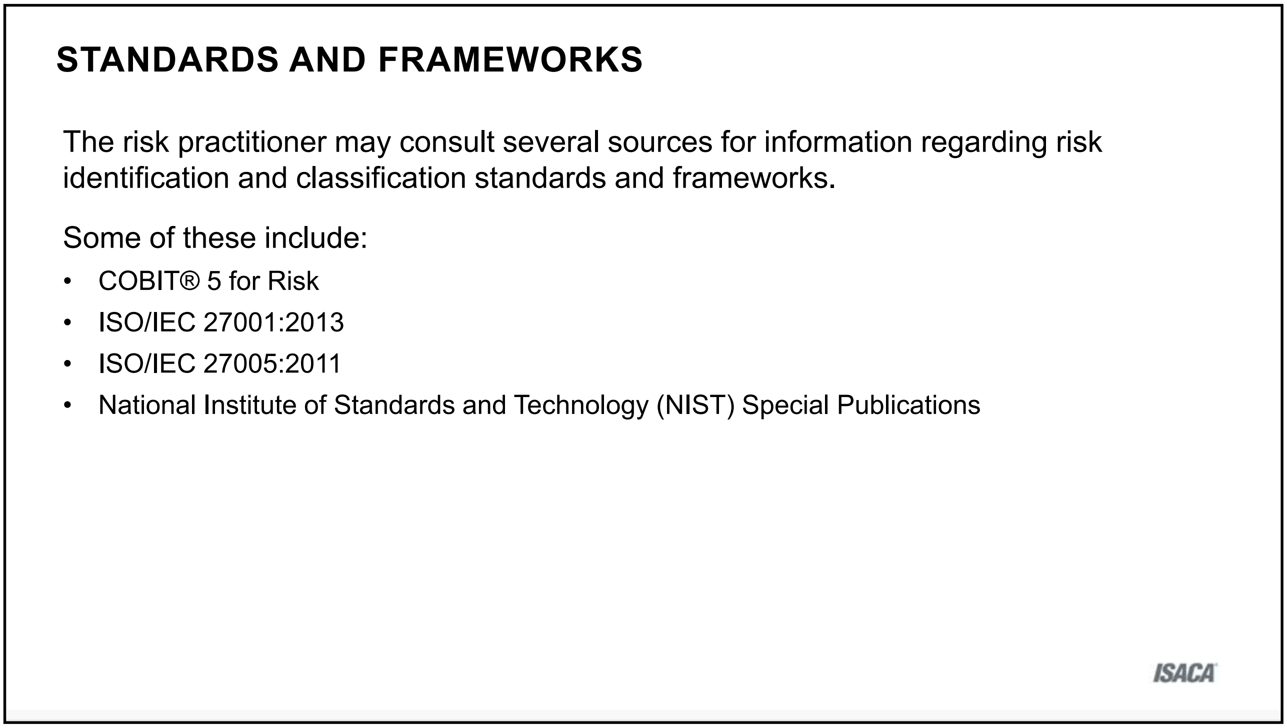


IT RISK MANAGEMENT

COBIT 5, the business and management framework for governance and management of enterprise IT, states that risk management entails the following:

- Recognizing risk
- Assessing the impact and likelihood of risk
- Developing strategies to manage risk

IT risk management focuses not only on the risk related to the IT department, but on all IT-enabled risk to an organization.

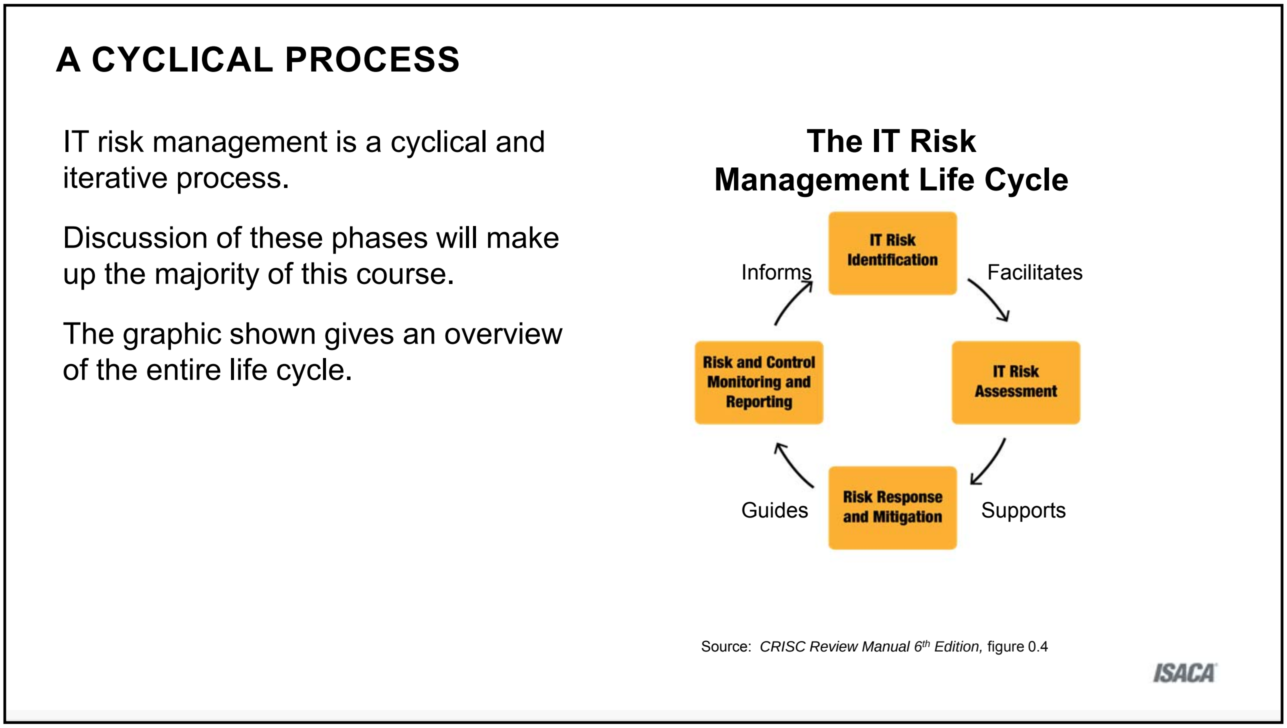


STANDARDS AND FRAMEWORKS

The risk practitioner may consult several sources for information regarding risk identification and classification standards and frameworks.

Some of these include:

- COBIT® 5 for Risk
- ISO/IEC 27001:2013
- ISO/IEC 27005:2011
- National Institute of Standards and Technology (NIST) Special Publications



A CYCLICAL PROCESS

IT risk management is a cyclical and iterative process.

Discussion of these phases will make up the majority of this course.

The graphic shown gives an overview of the entire life cycle.

The IT Risk Management Life Cycle

IT Risk Identification

Facilitates

IT Risk Assessment

Supports

Risk Response and Mitigation

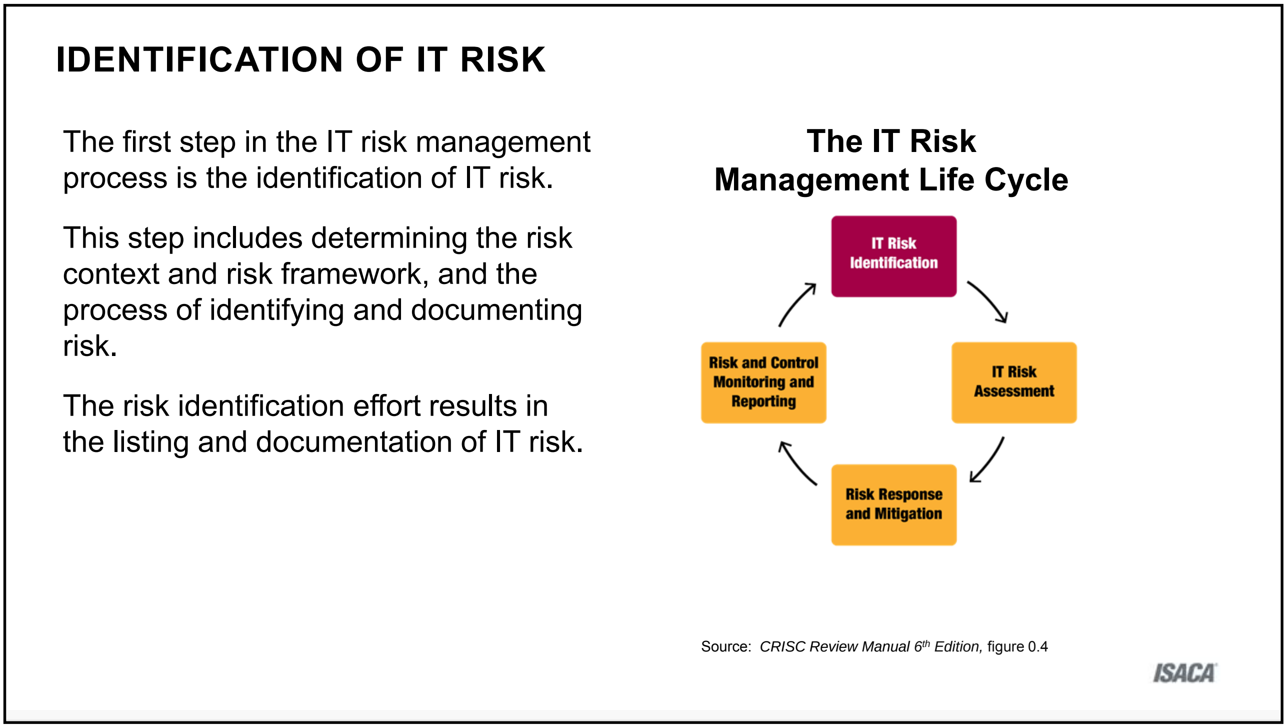
Guides

Risk and Control Monitoring and Reporting

Informs

Source: *CRISC Review Manual 6th Edition,* figure 0.4

ISACA



IDENTIFICATION OF IT RISK

The first step in the IT risk management process is the identification of IT risk.

This step includes determining the risk context and risk framework, and the process of identifying and documenting risk.

The risk identification effort results in the listing and documentation of IT risk.

The IT Risk Management Life Cycle

IT Risk Identification

IT Risk Assessment

Risk Response and Mitigation

Risk and Control Monitoring and Reporting

Source: *CRISC Review Manual 6th Edition,* figure 0.4

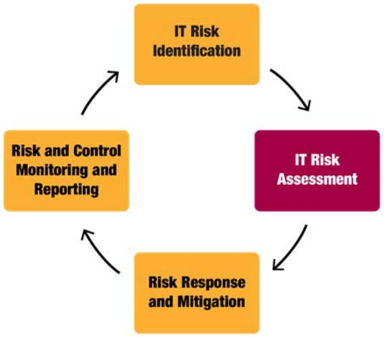
ISACA

ASSESSMENT

During the IT risk assessment, risk identified in the first phase is evaluated along several dimensions

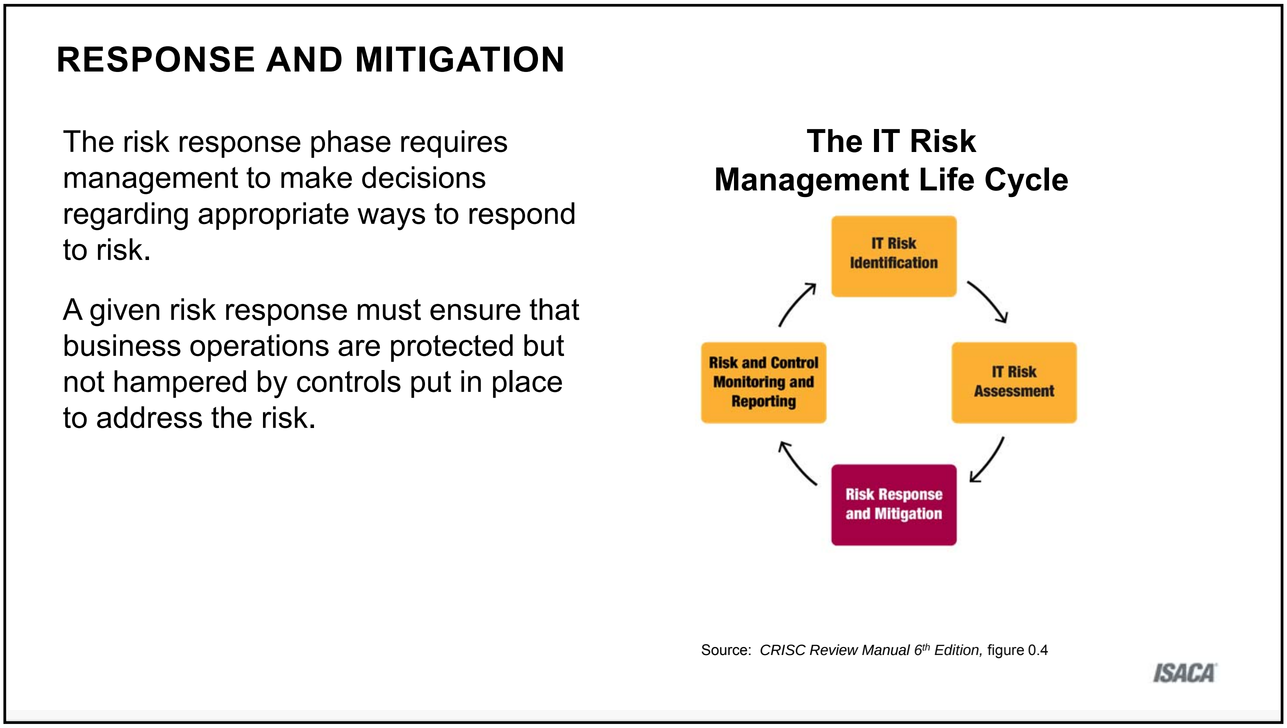
This step provides management with the data required for consideration in the next phase, risk response and mitigation.

The IT Risk Management Life Cycle


IT Risk Identification
IT Risk Assessment
Risk Response and Mitigation
Risk and Control Monitoring and Reporting

Source: *CRISC Review Manual 6th Edition,* figure 0.4

ISACA



RESPONSE AND MITIGATION

The risk response phase requires management to make decisions regarding appropriate ways to respond to risk.

A given risk response must ensure that business operations are protected but not hampered by controls put in place to address the risk.

The IT Risk Management Life Cycle

IT Risk Identification
IT Risk Assessment
Risk Response and Mitigation
Risk and Control Monitoring and Reporting

Source: *CRISC Review Manual 6th Edition,* figure 0.4

ISACA

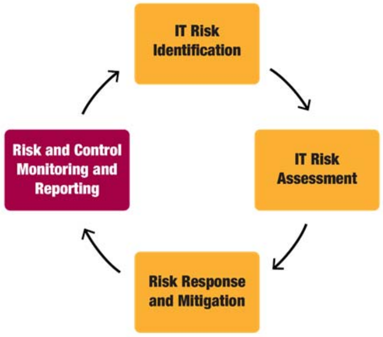
CONTROL AND MONITORING

The final phase is risk and control monitoring and reporting.

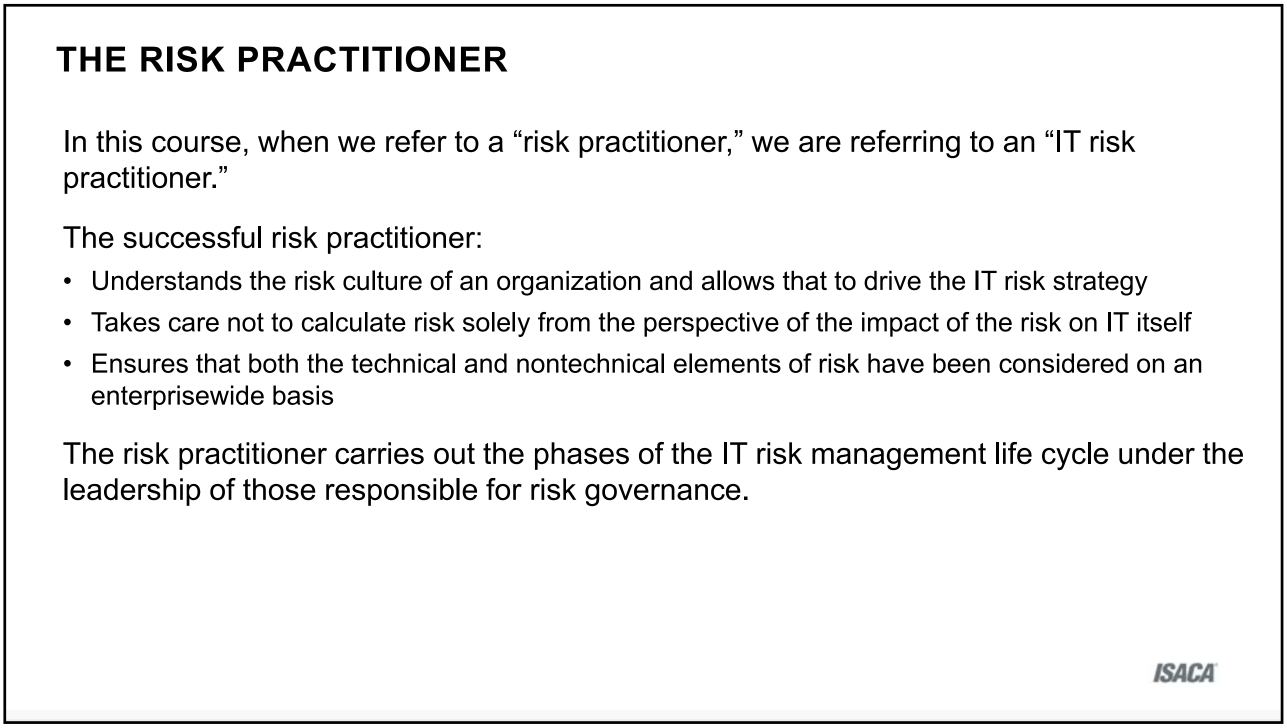
In this phase, controls and risk management efforts, as well as the current risk state, are monitored.

Results are reported back to senior management, which determines the need to return to any of the previous phases of the process.

The IT Risk Management Life Cycle


IT Risk Identification
IT Risk Assessment
Risk Response and Mitigation
Risk and Control Monitoring and Reporting

Source: *CRISC Review Manual 6th Edition,* figure 0.4



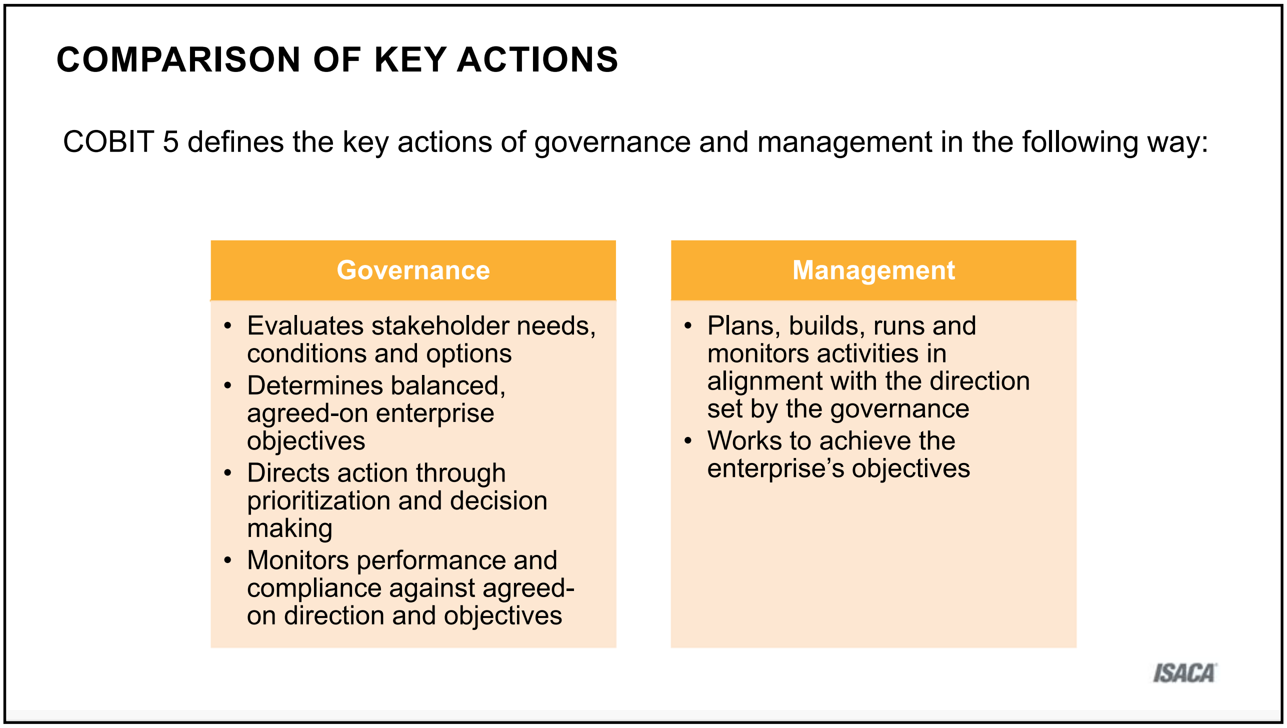
THE RISK PRACTITIONER

In this course, when we refer to a “risk practitioner,” we are referring to an “IT risk practitioner.”

The successful risk practitioner:

- Understands the risk culture of an organization and allows that to drive the IT risk strategy
- Takes care not to calculate risk solely from the perspective of the impact of the risk on IT itself
- Ensures that both the technical and nontechnical elements of risk have been considered on an enterprisewide basis

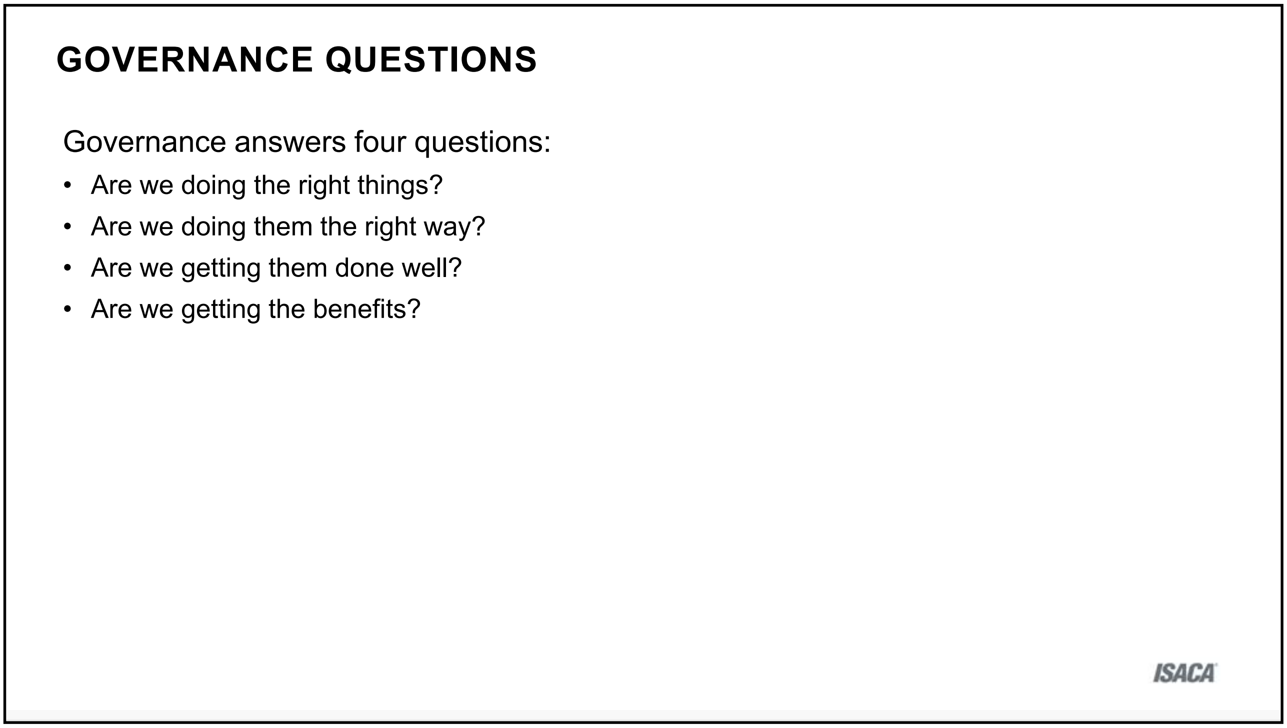
The risk practitioner carries out the phases of the IT risk management life cycle under the leadership of those responsible for risk governance.



COMPARISON OF KEY ACTIONS

COBIT 5 defines the key actions of governance and management in the following way:

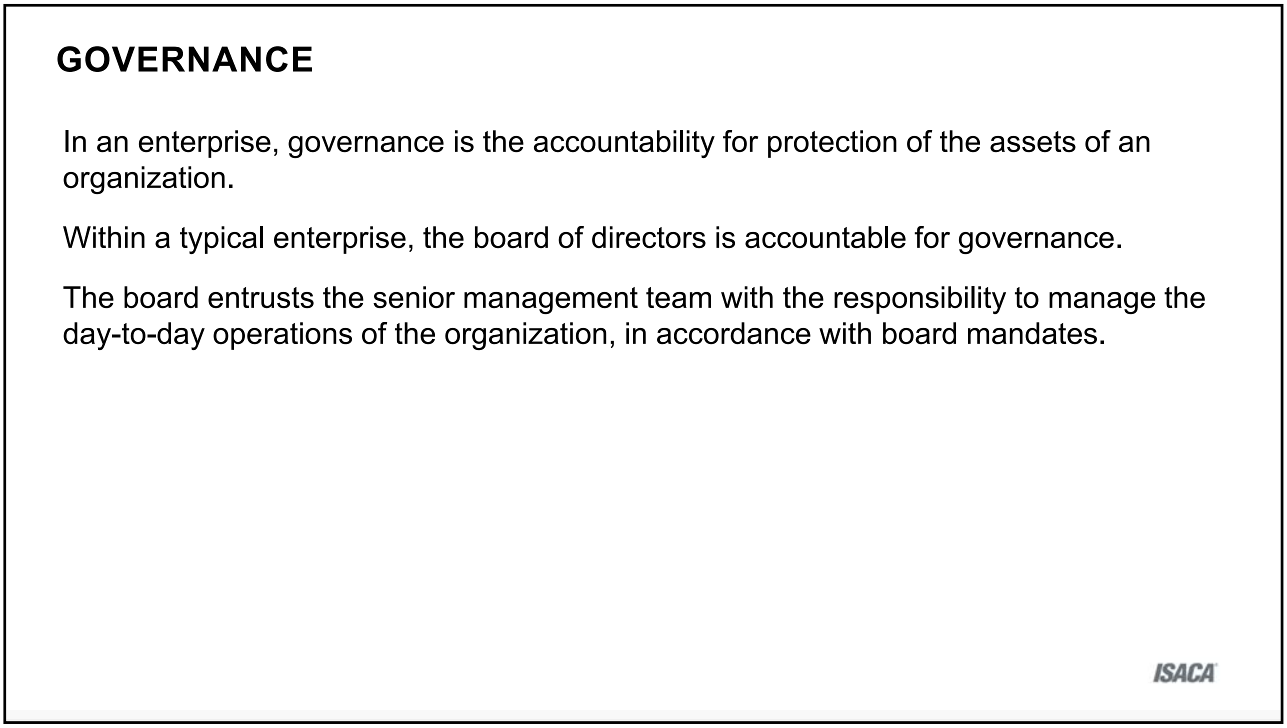
Governance	Management
• Evaluates stakeholder needs, conditions and options • Determines balanced, agreed-on enterprise objectives • Directs action through prioritization and decision making • Monitors performance and compliance against agreed-on direction and objectives	• Plans, builds, runs and monitors activities in alignment with the direction set by the governance • Works to achieve the enterprise's objectives



GOVERNANCE QUESTIONS

Governance answers four questions:

- Are we doing the right things?
- Are we doing them the right way?
- Are we getting them done well?
- Are we getting the benefits?

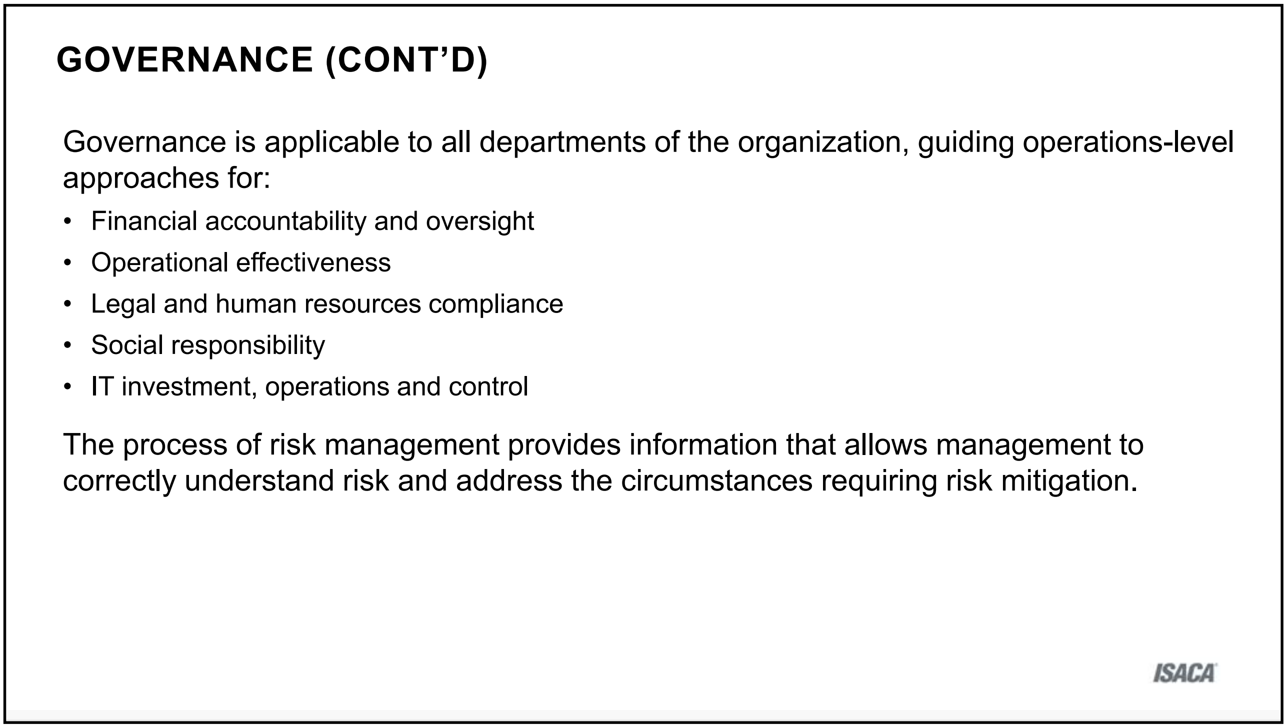


GOVERNANCE

In an enterprise, governance is the accountability for protection of the assets of an organization.

Within a typical enterprise, the board of directors is accountable for governance.

The board entrusts the senior management team with the responsibility to manage the day-to-day operations of the organization, in accordance with board mandates.

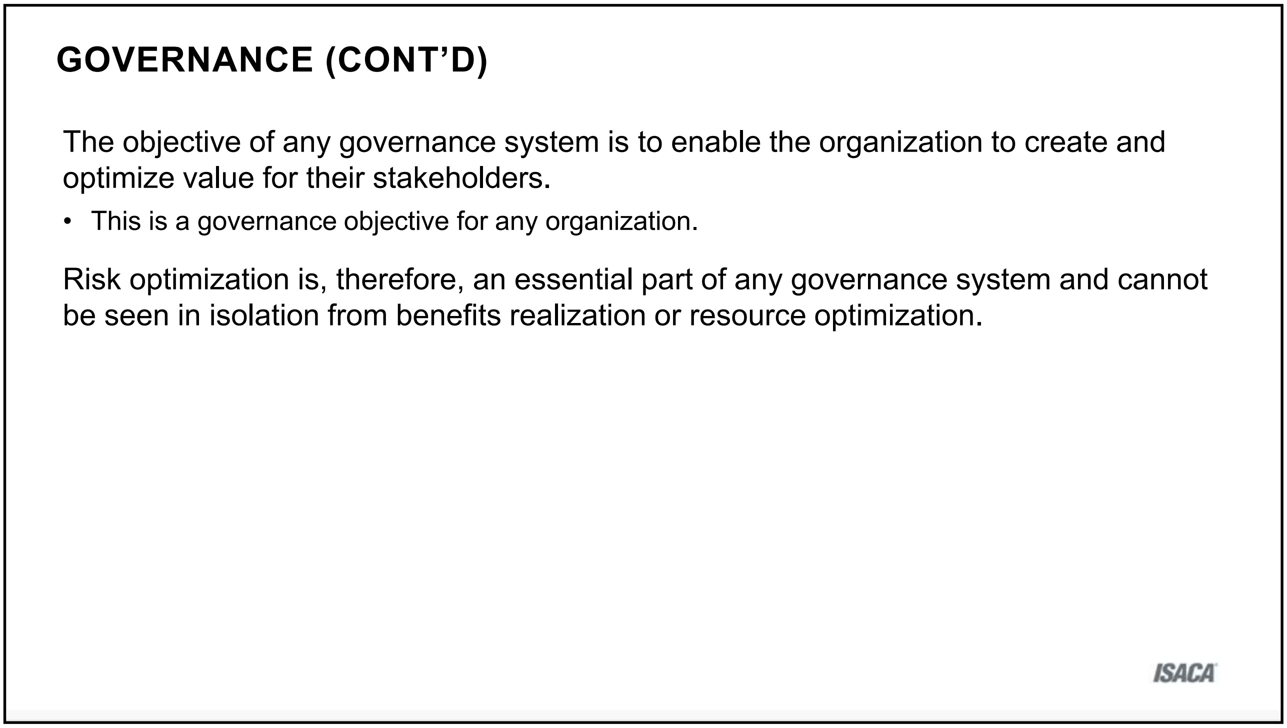


GOVERNANCE (CONT'D)

Governance is applicable to all departments of the organization, guiding operations-level approaches for:

- Financial accountability and oversight
- Operational effectiveness
- Legal and human resources compliance
- Social responsibility
- IT investment, operations and control

The process of risk management provides information that allows management to correctly understand risk and address the circumstances requiring risk mitigation.

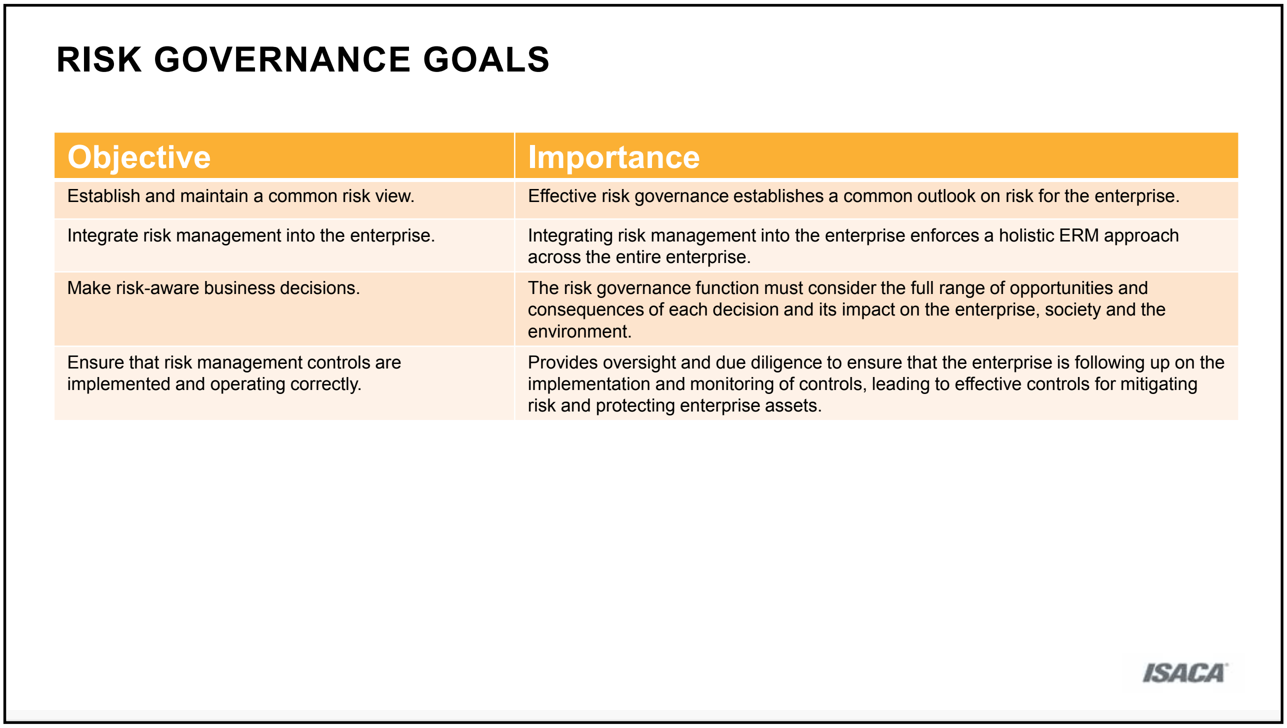


GOVERNANCE (CONT'D)

The objective of any governance system is to enable the organization to create and optimize value for their stakeholders.

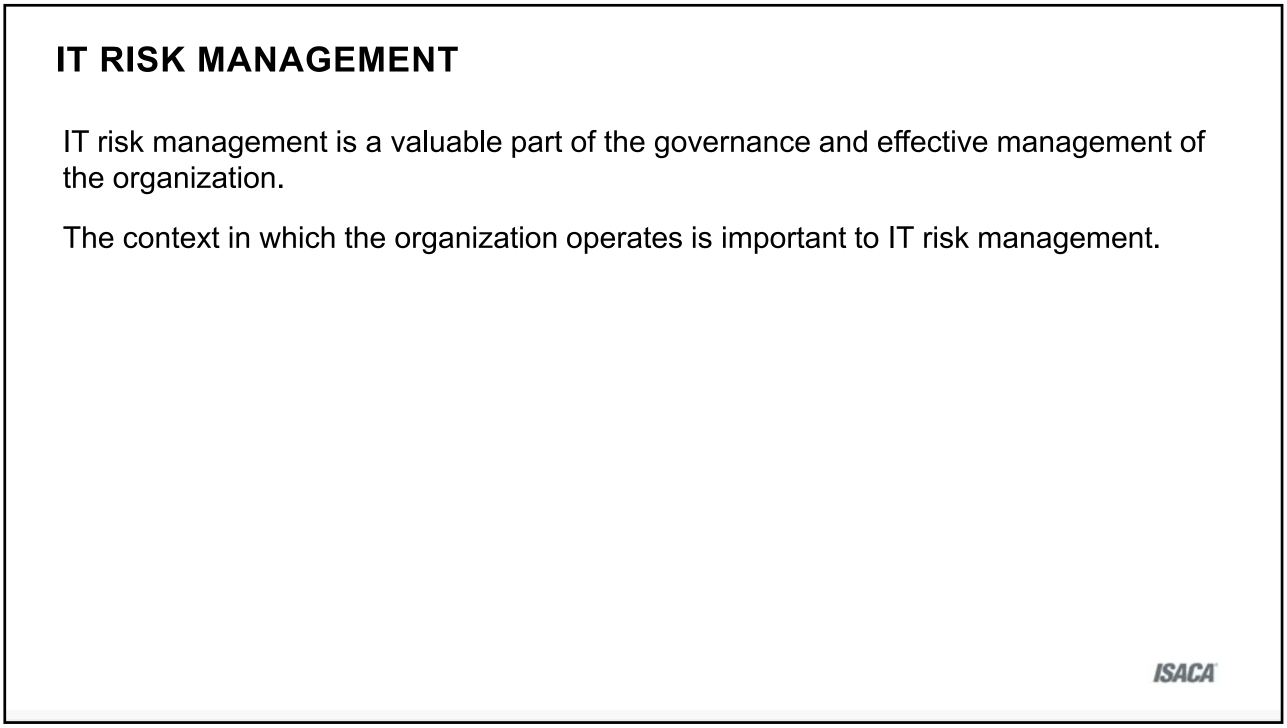
- This is a governance objective for any organization.

Risk optimization is, therefore, an essential part of any governance system and cannot be seen in isolation from benefits realization or resource optimization.



RISK GOVERNANCE GOALS

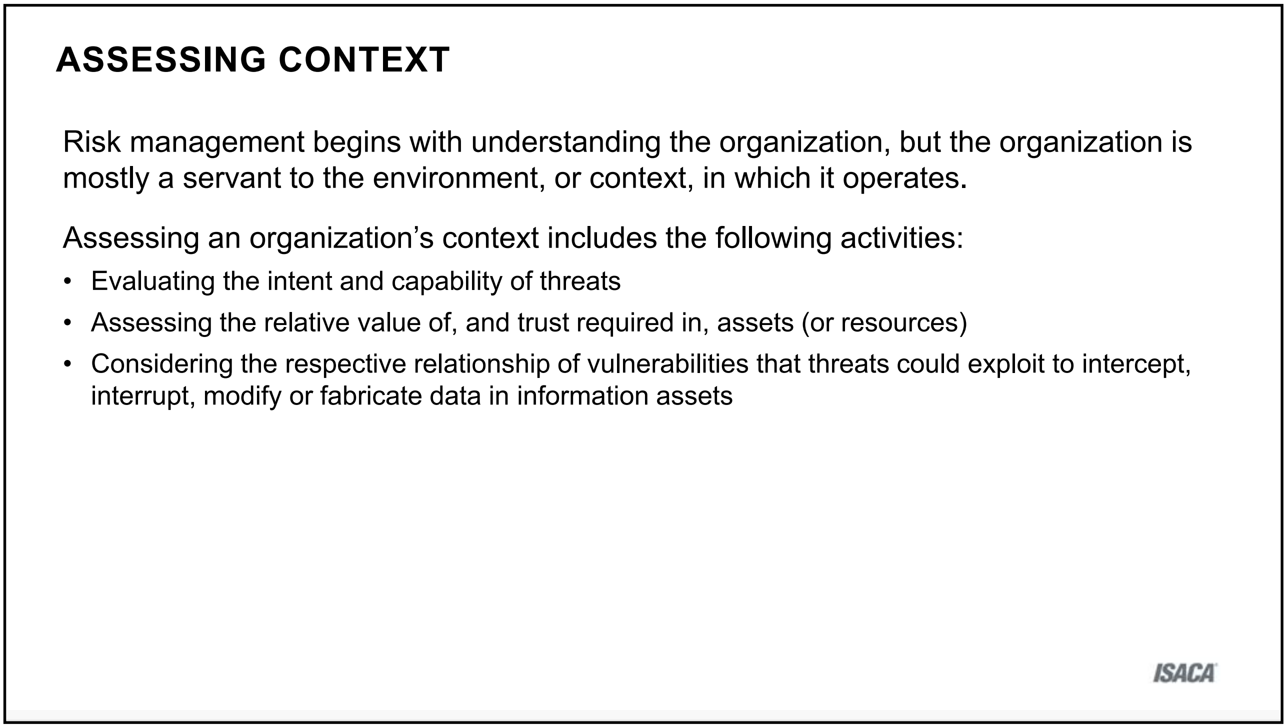
Objective	Importance
Establish and maintain a common risk view.	Effective risk governance establishes a common outlook on risk for the enterprise.
Integrate risk management into the enterprise.	Integrating risk management into the enterprise enforces a holistic ERM approach across the entire enterprise.
Make risk-aware business decisions.	The risk governance function must consider the full range of opportunities and consequences of each decision and its impact on the enterprise, society and the environment.
Ensure that risk management controls are implemented and operating correctly.	Provides oversight and due diligence to ensure that the enterprise is following up on the implementation and monitoring of controls, leading to effective controls for mitigating risk and protecting enterprise assets.



IT RISK MANAGEMENT

IT risk management is a valuable part of the governance and effective management of the organization.

The context in which the organization operates is important to IT risk management.

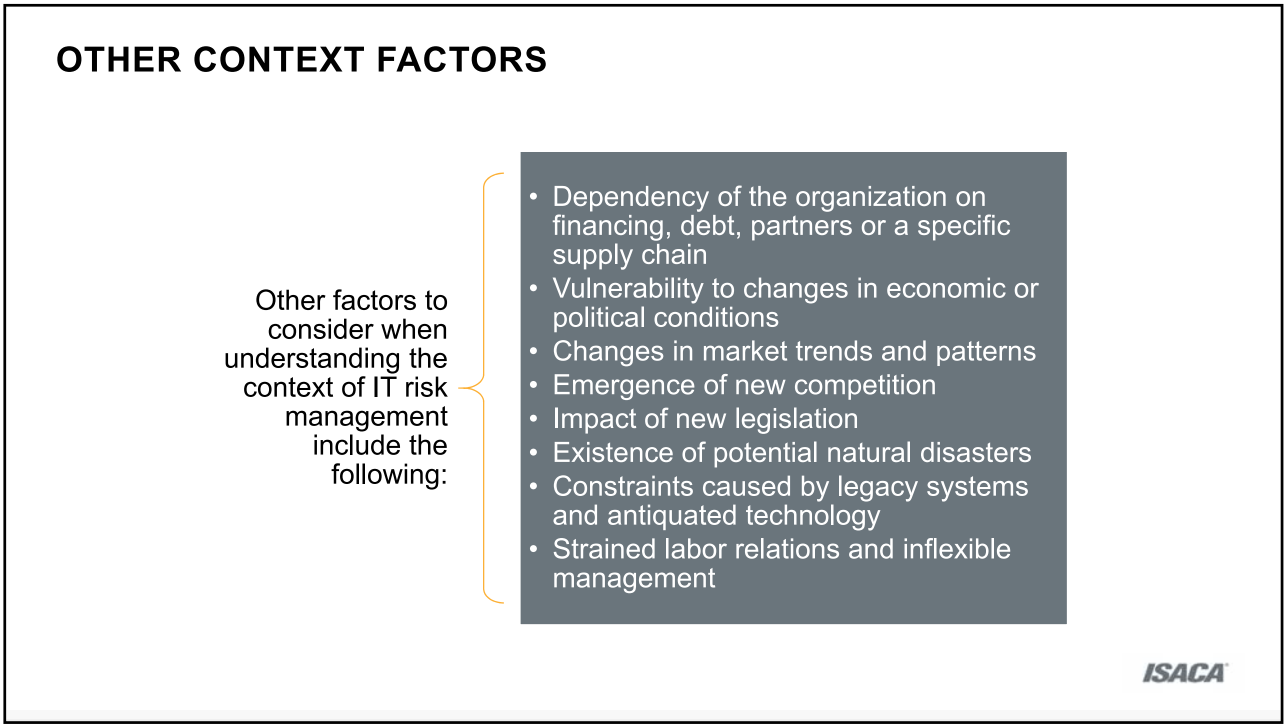


ASSESSING CONTEXT

Risk management begins with understanding the organization, but the organization is mostly a servant to the environment, or context, in which it operates.

Assessing an organization's context includes the following activities:

- Evaluating the intent and capability of threats
- Assessing the relative value of, and trust required in, assets (or resources)
- Considering the respective relationship of vulnerabilities that threats could exploit to intercept, interrupt, modify or fabricate data in information assets



OTHER CONTEXT FACTORS

Other factors to consider when understanding the context of IT risk management include the following:

- Dependency of the organization on financing, debt, partners or a specific supply chain
- Vulnerability to changes in economic or political conditions
- Changes in market trends and patterns
- Emergence of new competition
- Impact of new legislation
- Existence of potential natural disasters
- Constraints caused by legacy systems and antiquated technology
- Strained labor relations and inflexible management

BENEFITS

A focus on IT risk management brings a variety of benefits to the enterprise, as follows:

Improves oversight of organizational assets

Minimizes loss

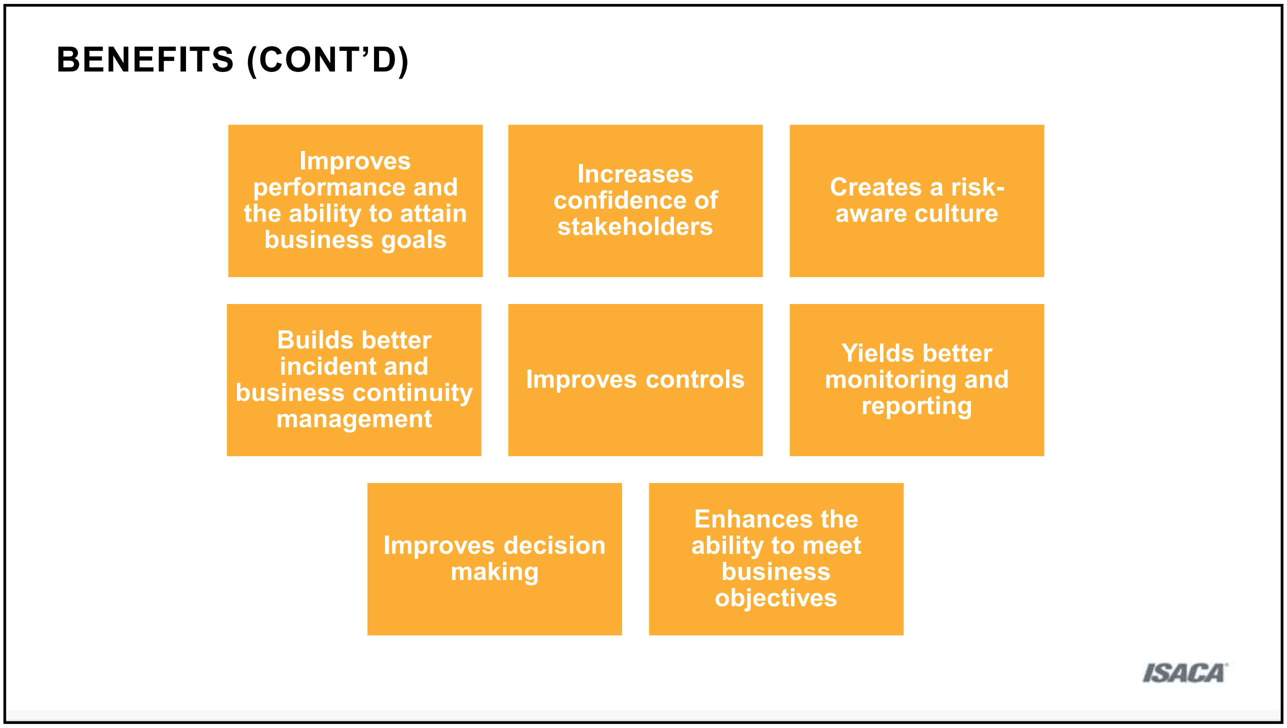
Identifies threats, vulnerabilities and risk

Prioritizes risk response efforts

Ensures legal and regulatory compliance

Increases likelihood of project success

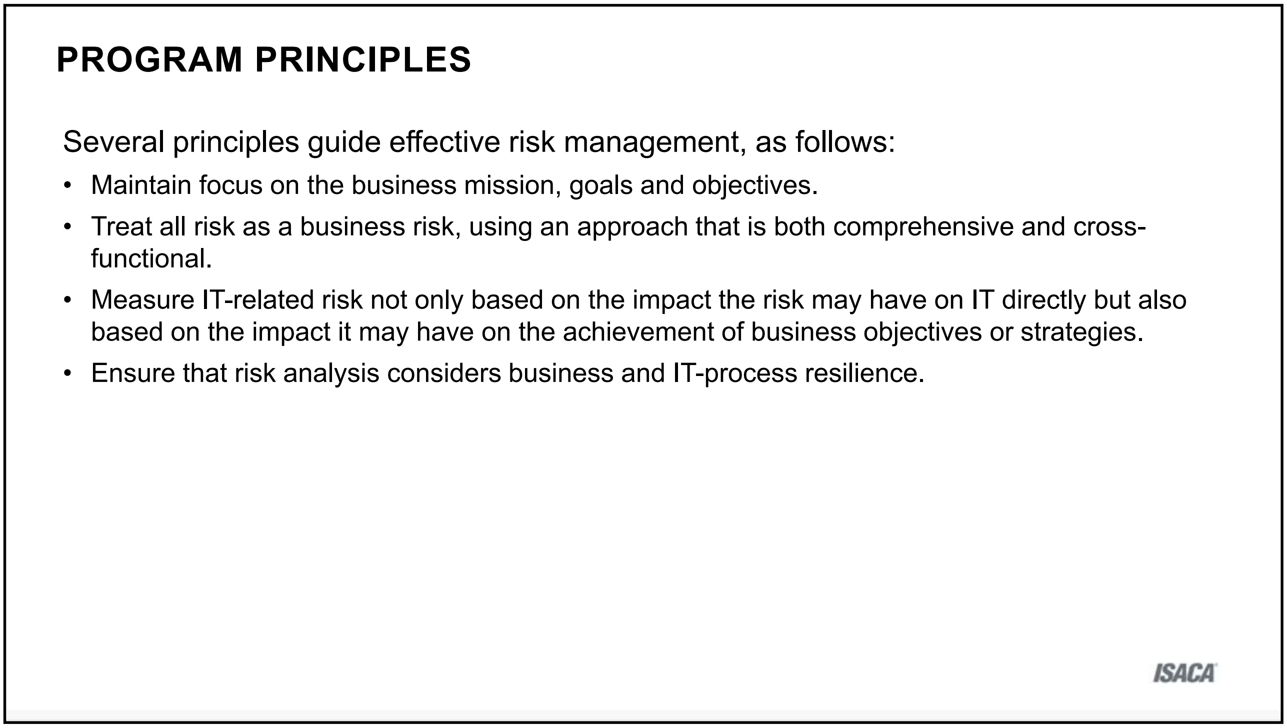
ISACA



BENEFITS (CONT'D)

- Improves performance and the ability to attain business goals
- Increases confidence of stakeholders
- Creates a risk-aware culture
- Builds better incident and business continuity management
- Improves controls
- Yields better monitoring and reporting
- Improves decision making
- Enhances the ability to meet business objectives

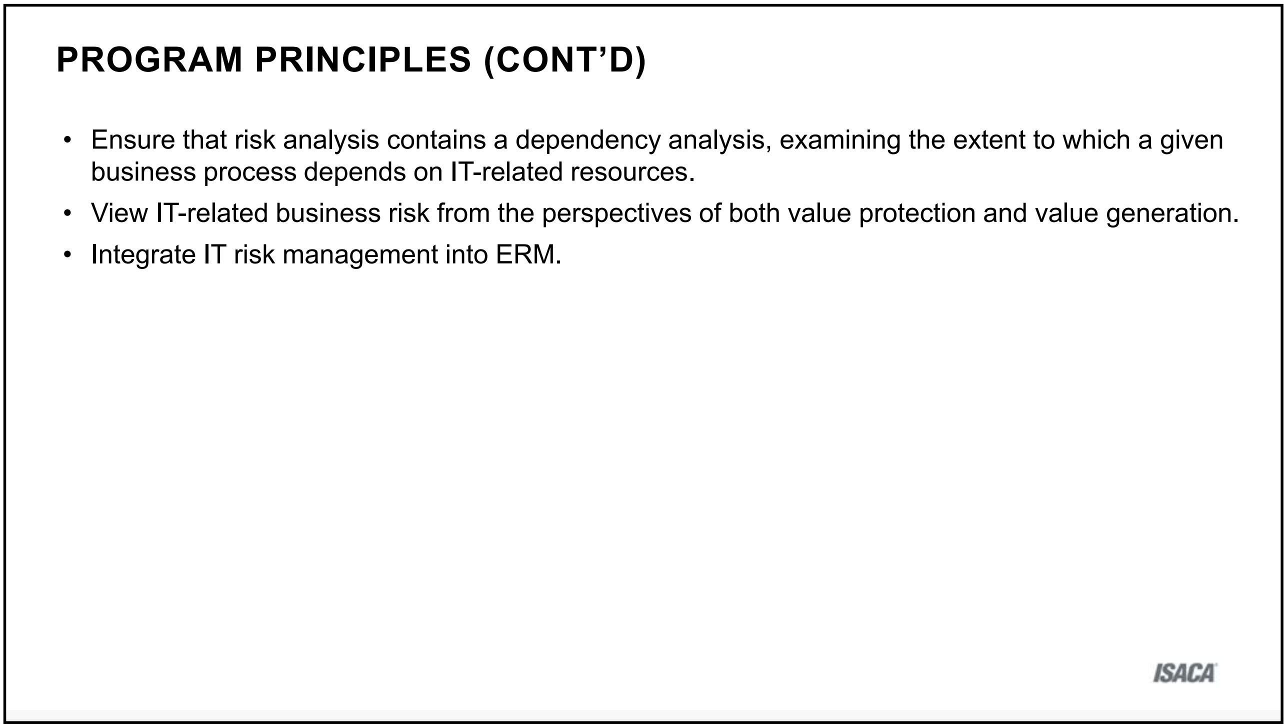
ISACA



PROGRAM PRINCIPLES

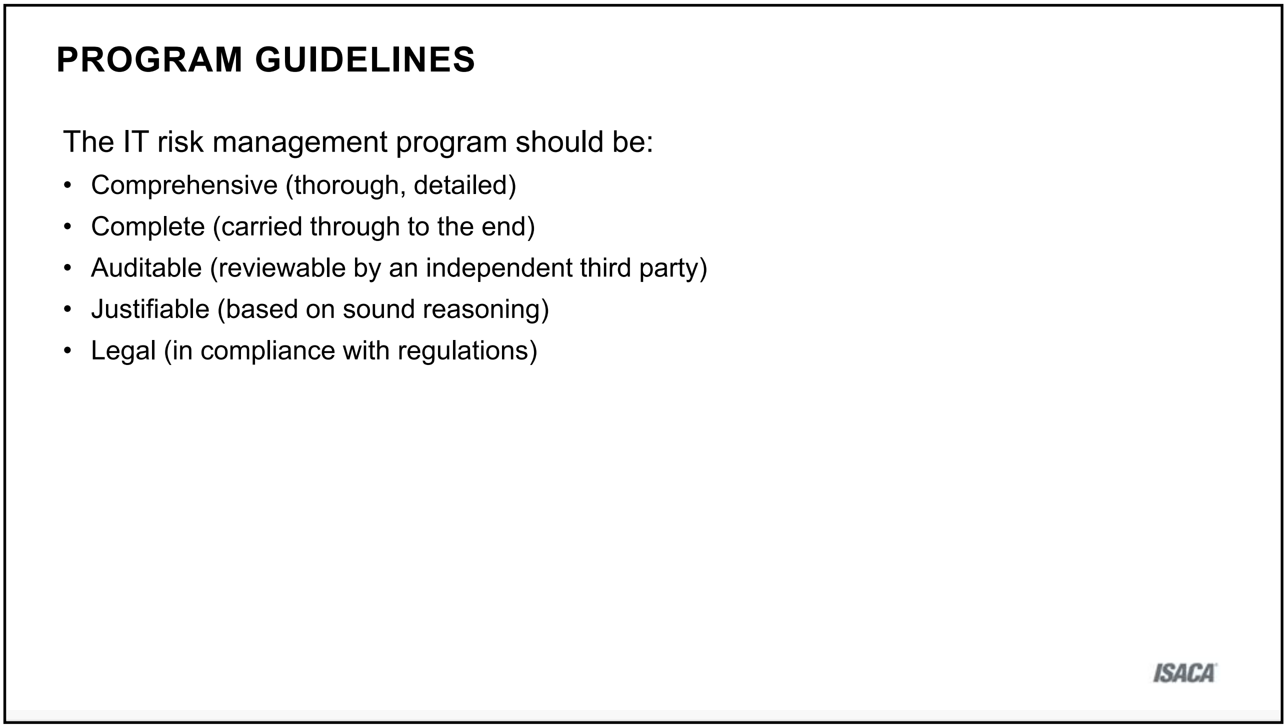
Several principles guide effective risk management, as follows:

- Maintain focus on the business mission, goals and objectives.
- Treat all risk as a business risk, using an approach that is both comprehensive and cross-functional.
- Measure IT-related risk not only based on the impact the risk may have on IT directly but also based on the impact it may have on the achievement of business objectives or strategies.
- Ensure that risk analysis considers business and IT-process resilience.



PROGRAM PRINCIPLES (CONT'D)

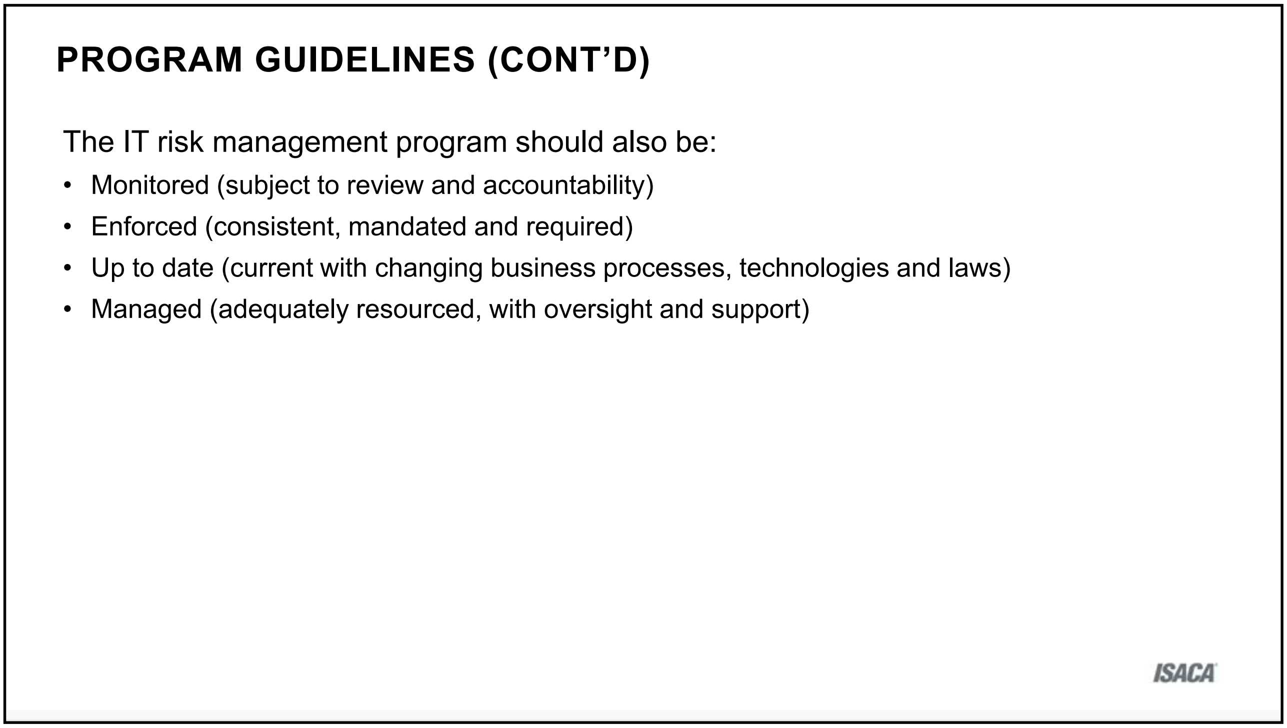
- Ensure that risk analysis contains a dependency analysis, examining the extent to which a given business process depends on IT-related resources.
- View IT-related business risk from the perspectives of both value protection and value generation.
- Integrate IT risk management into ERM.



PROGRAM GUIDELINES

The IT risk management program should be:

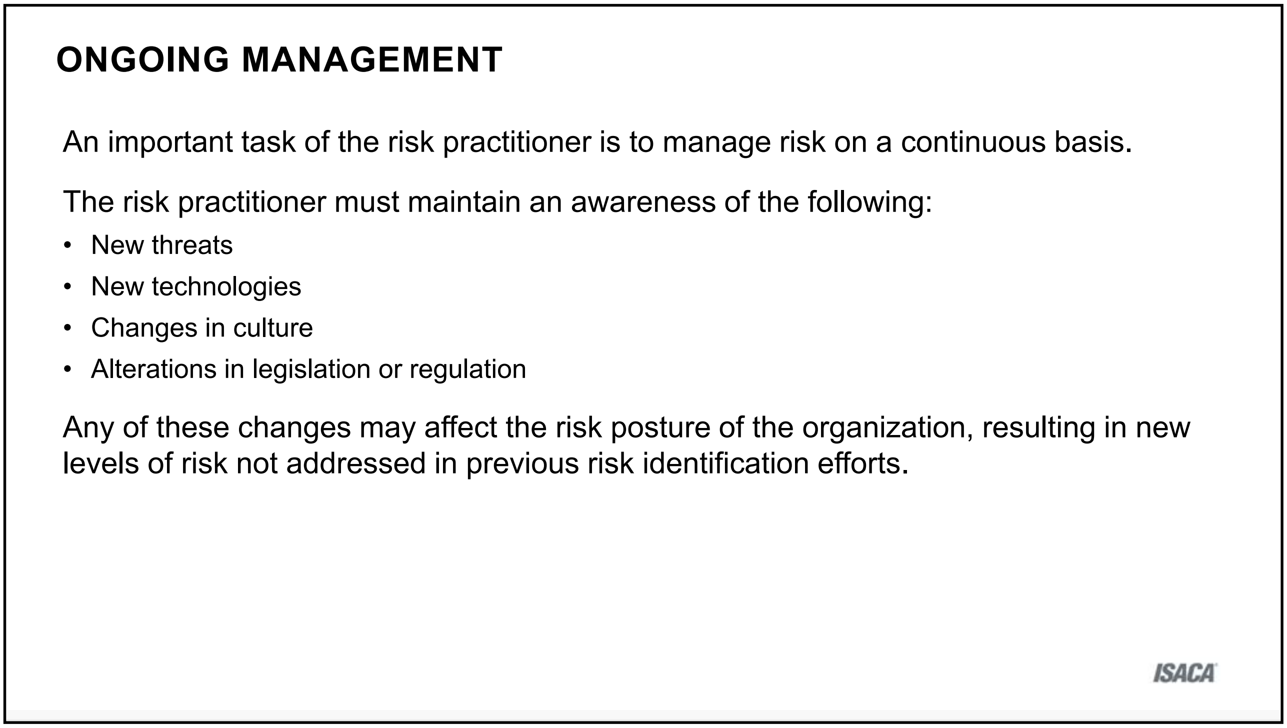
- Comprehensive (thorough, detailed)
- Complete (carried through to the end)
- Auditable (reviewable by an independent third party)
- Justifiable (based on sound reasoning)
- Legal (in compliance with regulations)



PROGRAM GUIDELINES (CONT'D)

The IT risk management program should also be:

- Monitored (subject to review and accountability)
- Enforced (consistent, mandated and required)
- Up to date (current with changing business processes, technologies and laws)
- Managed (adequately resourced, with oversight and support)



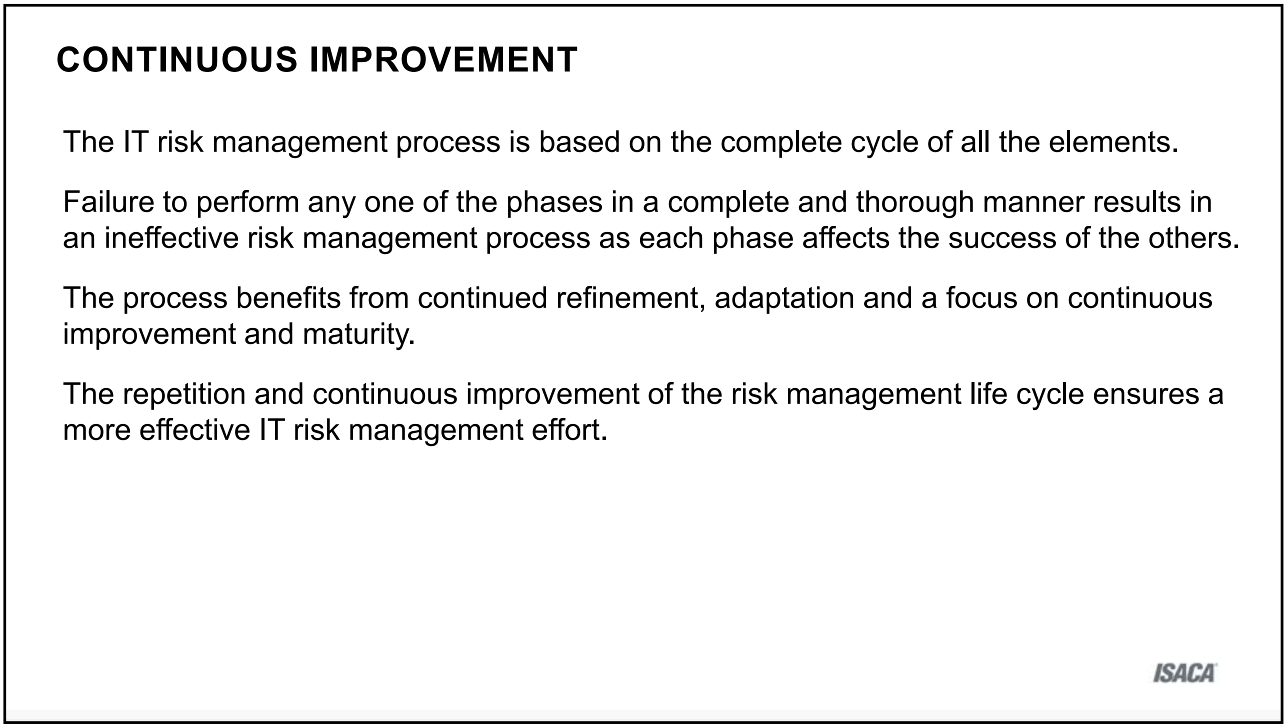
ONGOING MANAGEMENT

An important task of the risk practitioner is to manage risk on a continuous basis.

The risk practitioner must maintain an awareness of the following:

- New threats
- New technologies
- Changes in culture
- Alterations in legislation or regulation

Any of these changes may affect the risk posture of the organization, resulting in new levels of risk not addressed in previous risk identification efforts.



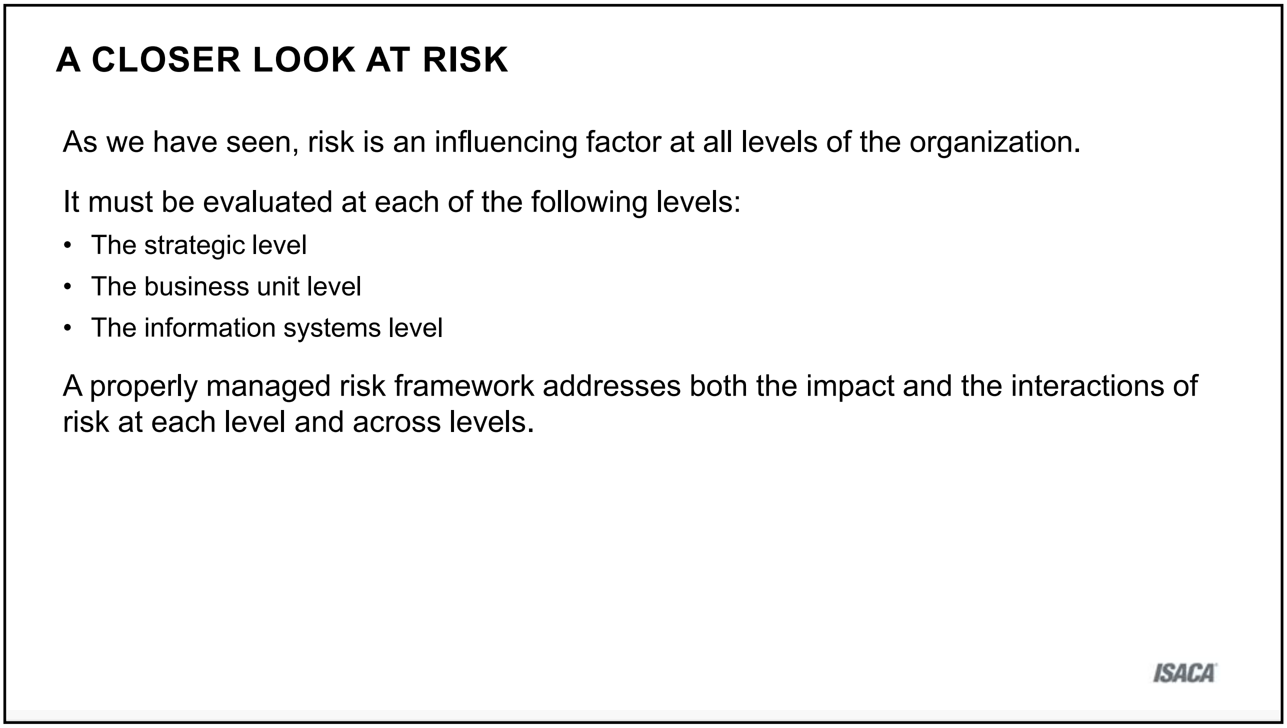
CONTINUOUS IMPROVEMENT

The IT risk management process is based on the complete cycle of all the elements.

Failure to perform any one of the phases in a complete and thorough manner results in an ineffective risk management process as each phase affects the success of the others.

The process benefits from continued refinement, adaptation and a focus on continuous improvement and maturity.

The repetition and continuous improvement of the risk management life cycle ensures a more effective IT risk management effort.



A CLOSER LOOK AT RISK

As we have seen, risk is an influencing factor at all levels of the organization.

It must be evaluated at each of the following levels:

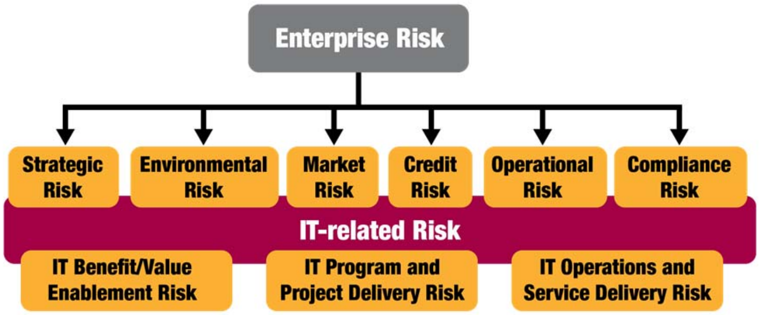
- The strategic level
- The business unit level
- The information systems level

A properly managed risk framework addresses both the impact and the interactions of risk at each level and across levels.

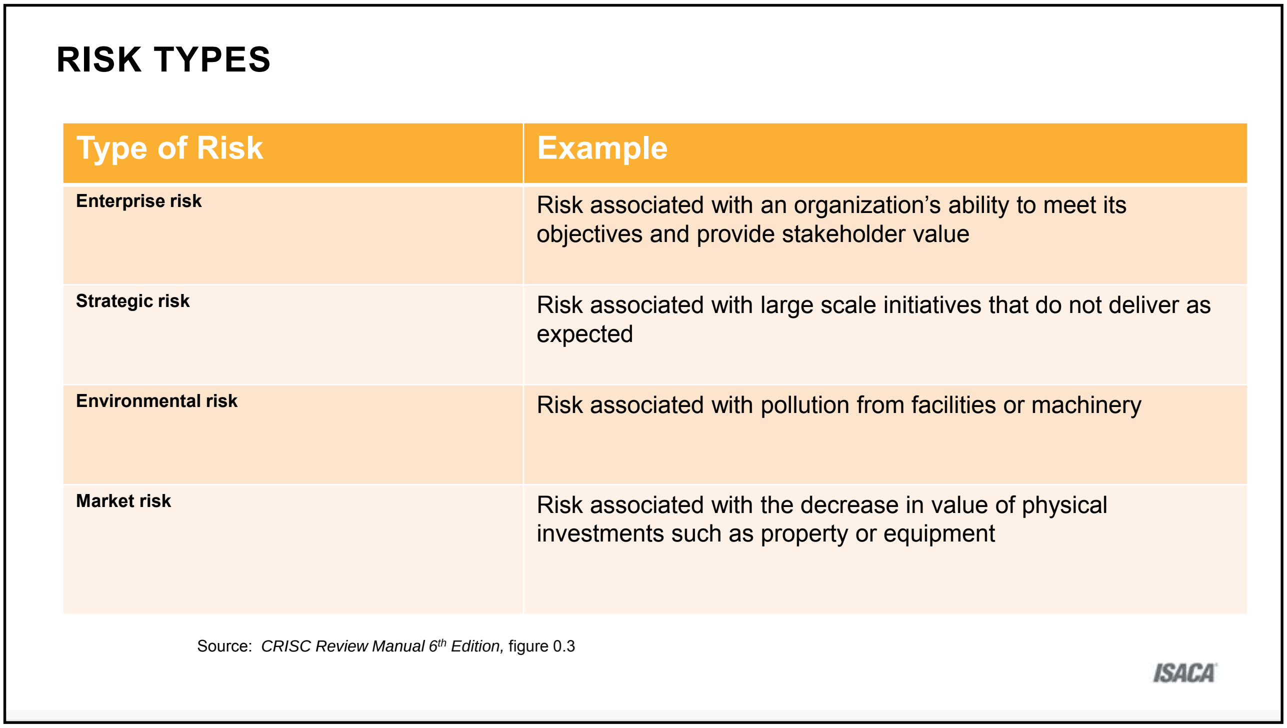
ENTERPRISE RISK TYPES

Risk does not describe a single type of event or consequence. Instead, it is highly contextual.

The IT Risk Hierarchy, for example, depicts a number of risk types, as follows:



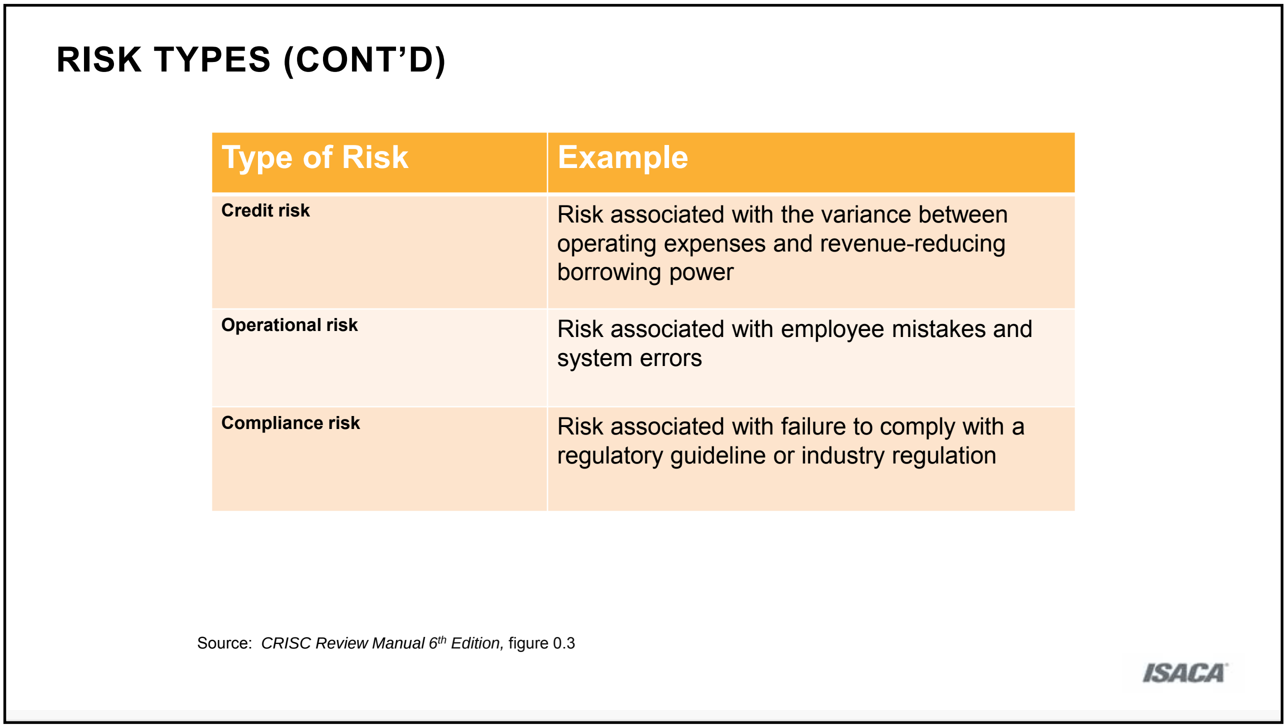
Source: *CRISC Review Manual 6th Edition,* figure 0.3



RISK TYPES

Type of Risk	Example
Enterprise risk	Risk associated with an organization’s ability to meet its objectives and provide stakeholder value
Strategic risk	Risk associated with large scale initiatives that do not deliver as expected
Environmental risk	Risk associated with pollution from facilities or machinery
Market risk	Risk associated with the decrease in value of physical investments such as property or equipment

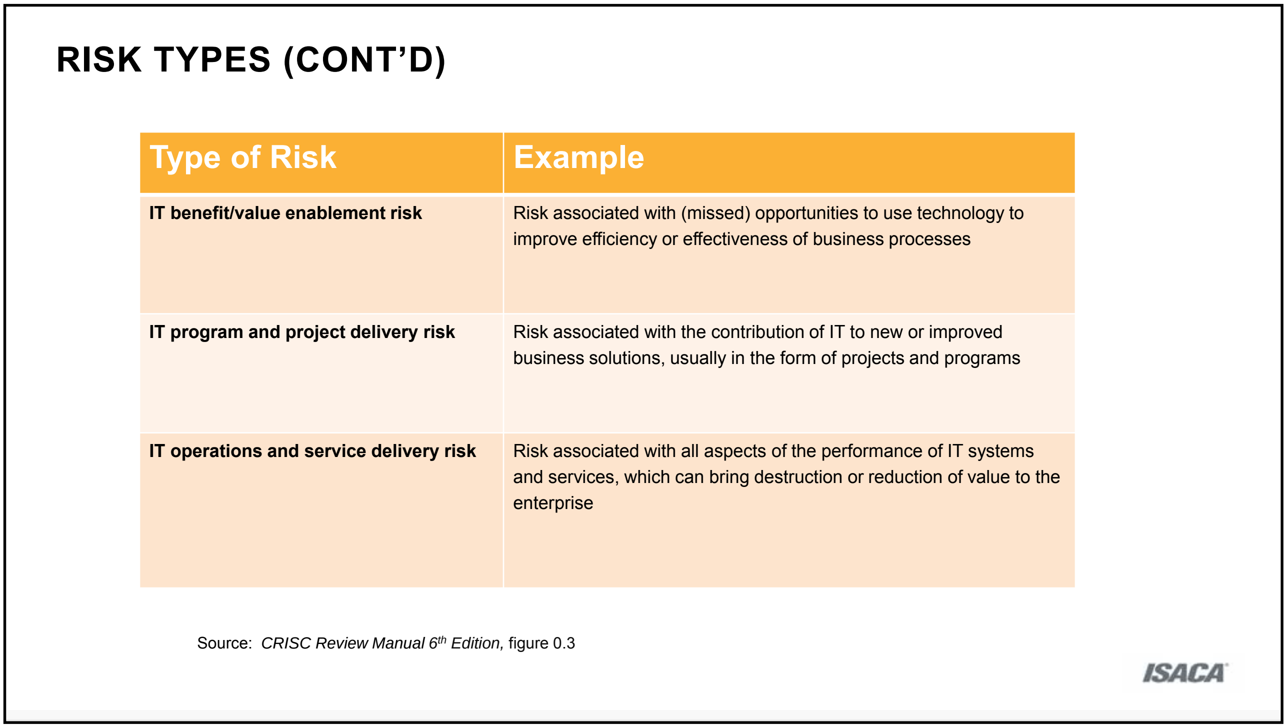
Source: *CRISC Review Manual 6th Edition,* figure 0.3



RISK TYPES (CONT'D)

Type of Risk	Example
Credit risk	Risk associated with the variance between operating expenses and revenue-reducing borrowing power
Operational risk	Risk associated with employee mistakes and system errors
Compliance risk	Risk associated with failure to comply with a regulatory guideline or industry regulation

Source: *CRISC Review Manual 6th Edition,* figure 0.3

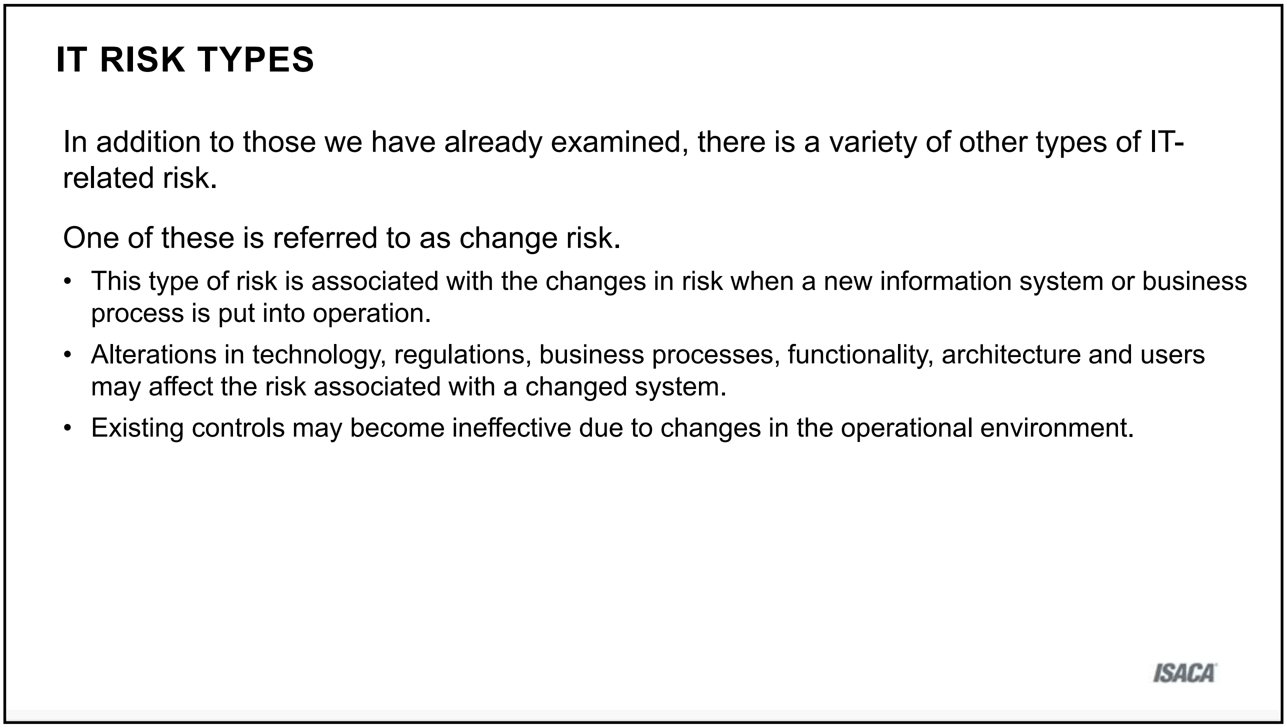


RISK TYPES (CONT'D)

Type of Risk	Example
IT benefit/value enablement risk	Risk associated with (missed) opportunities to use technology to improve efficiency or effectiveness of business processes
IT program and project delivery risk	Risk associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programs
IT operations and service delivery risk	Risk associated with all aspects of the performance of IT systems and services, which can bring destruction or reduction of value to the enterprise

Source: *CRISC Review Manual 6th Edition,* figure 0.3

ISACA

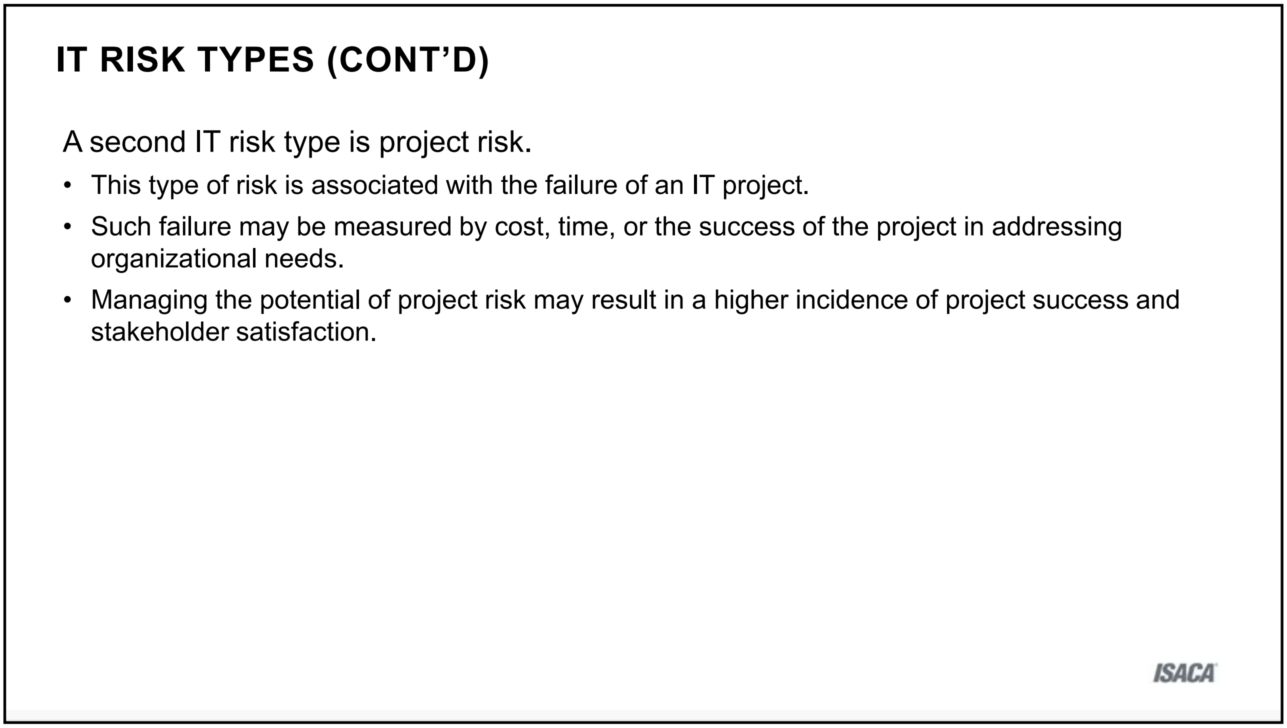


IT RISK TYPES

In addition to those we have already examined, there is a variety of other types of IT-related risk.

One of these is referred to as change risk.

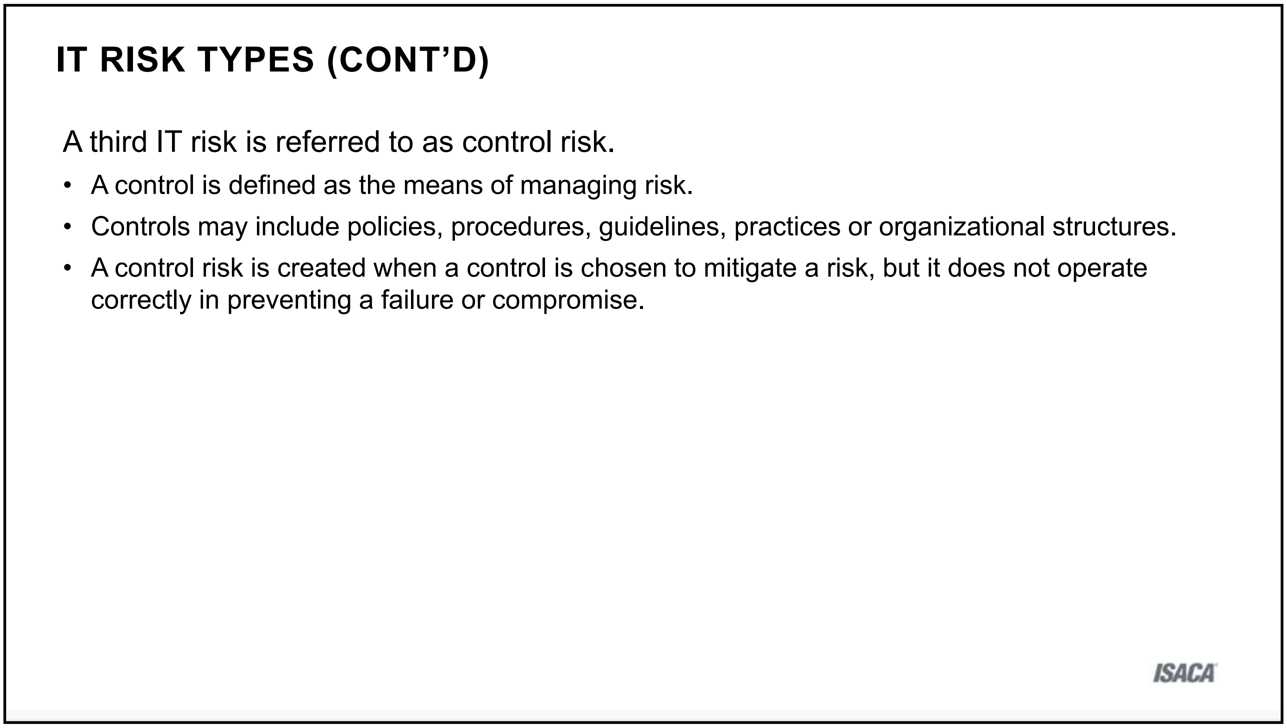
- This type of risk is associated with the changes in risk when a new information system or business process is put into operation.
- Alterations in technology, regulations, business processes, functionality, architecture and users may affect the risk associated with a changed system.
- Existing controls may become ineffective due to changes in the operational environment.



IT RISK TYPES (CONT'D)

A second IT risk type is project risk.

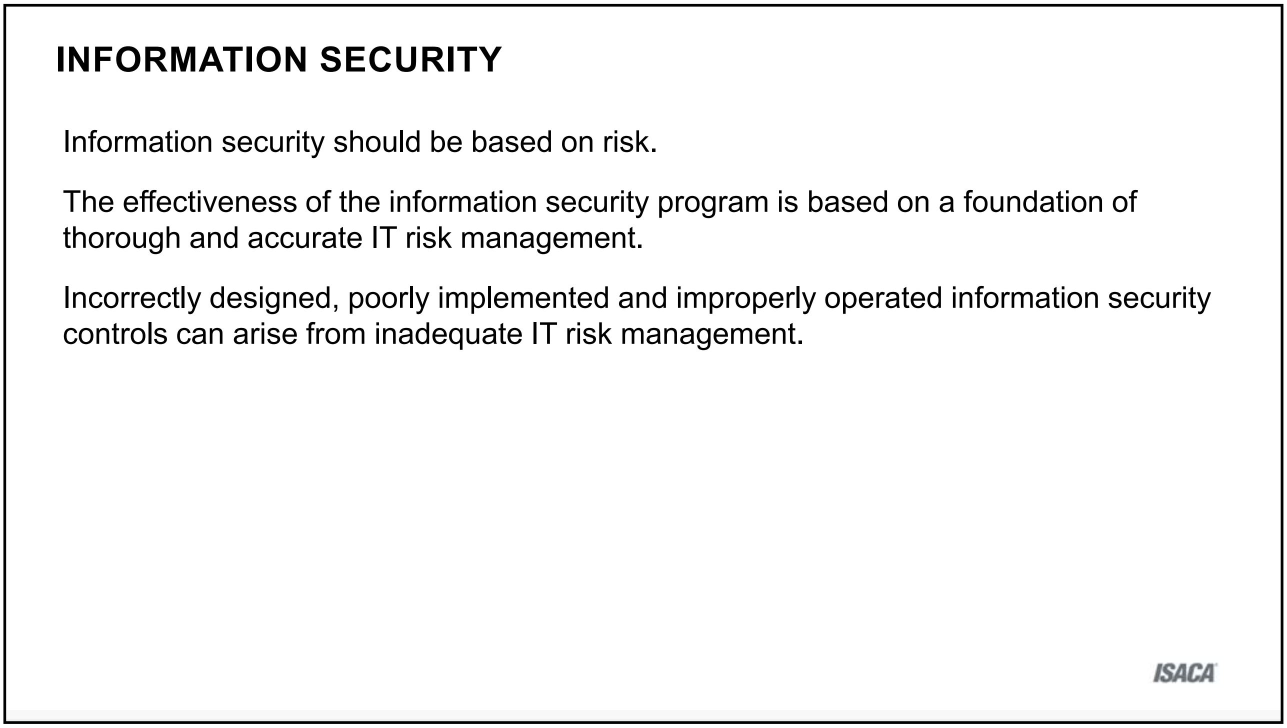
- This type of risk is associated with the failure of an IT project.
- Such failure may be measured by cost, time, or the success of the project in addressing organizational needs.
- Managing the potential of project risk may result in a higher incidence of project success and stakeholder satisfaction.



IT RISK TYPES (CONT'D)

A third IT risk is referred to as control risk.

- A control is defined as the means of managing risk.
- Controls may include policies, procedures, guidelines, practices or organizational structures.
- A control risk is created when a control is chosen to mitigate a risk, but it does not operate correctly in preventing a failure or compromise.

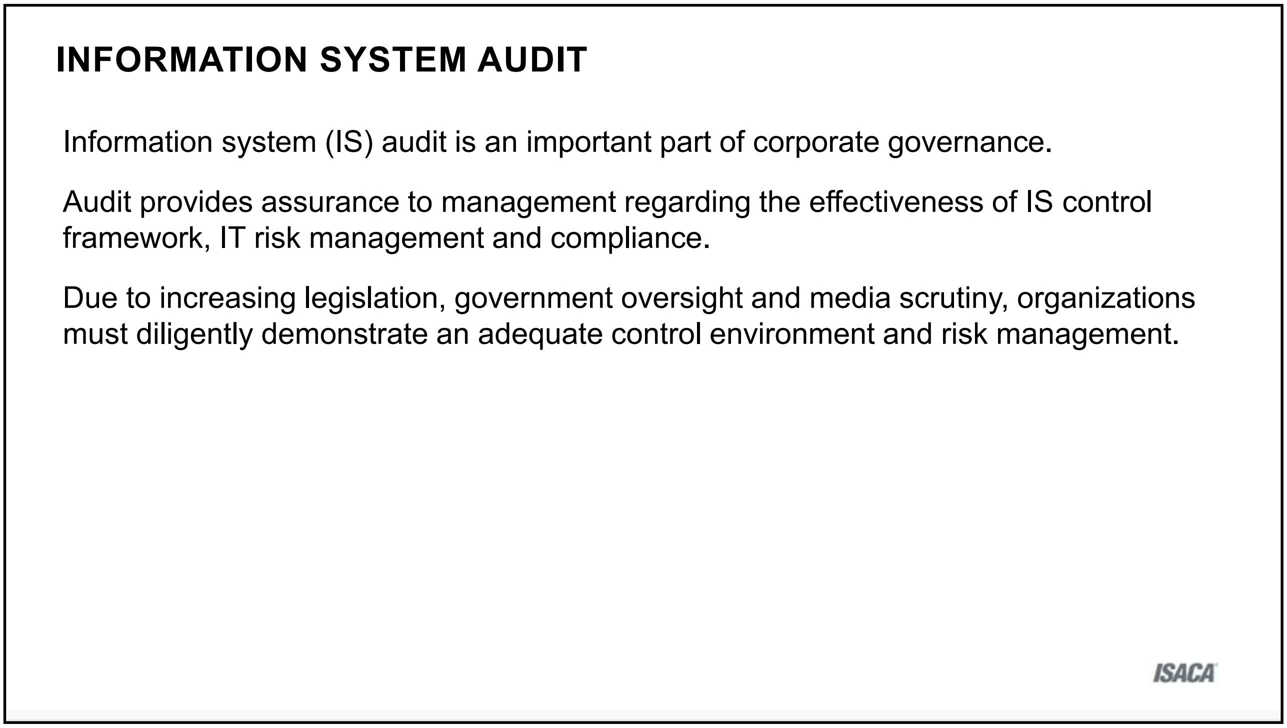


INFORMATION SECURITY

Information security should be based on risk.

The effectiveness of the information security program is based on a foundation of thorough and accurate IT risk management.

Incorrectly designed, poorly implemented and improperly operated information security controls can arise from inadequate IT risk management.

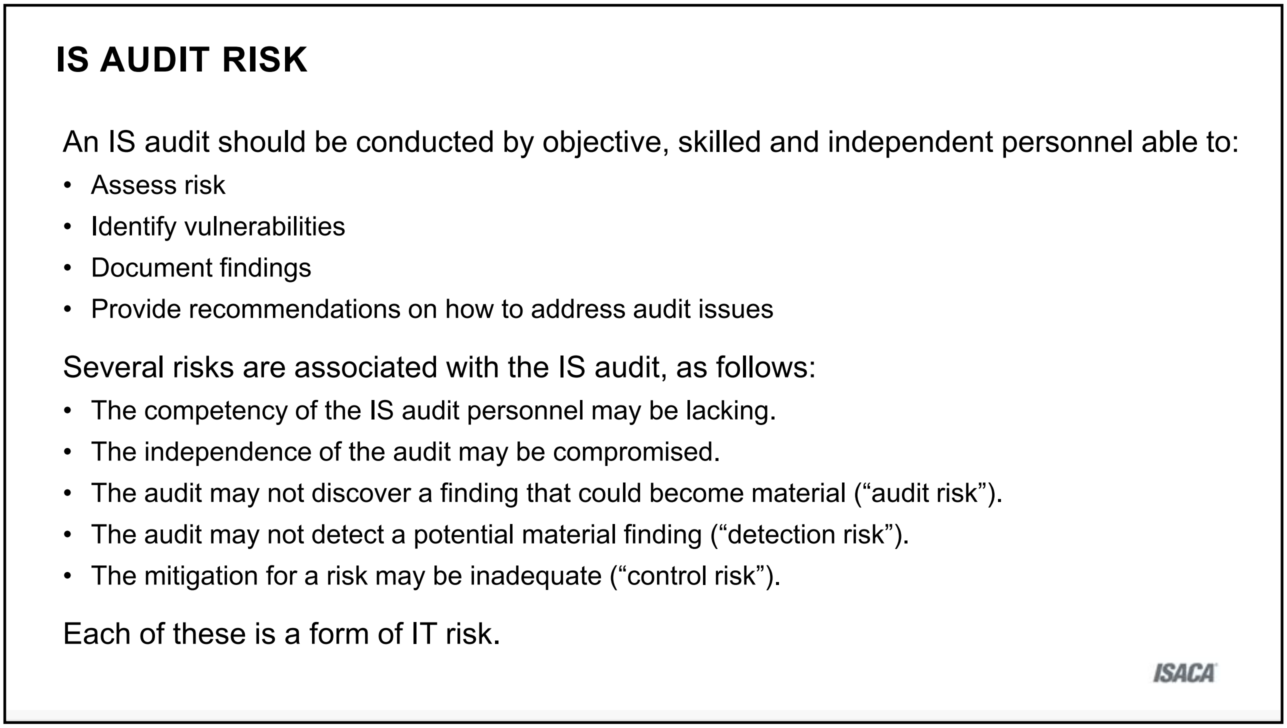


INFORMATION SYSTEM AUDIT

Information system (IS) audit is an important part of corporate governance.

Audit provides assurance to management regarding the effectiveness of IS control framework, IT risk management and compliance.

Due to increasing legislation, government oversight and media scrutiny, organizations must diligently demonstrate an adequate control environment and risk management.



IS AUDIT RISK

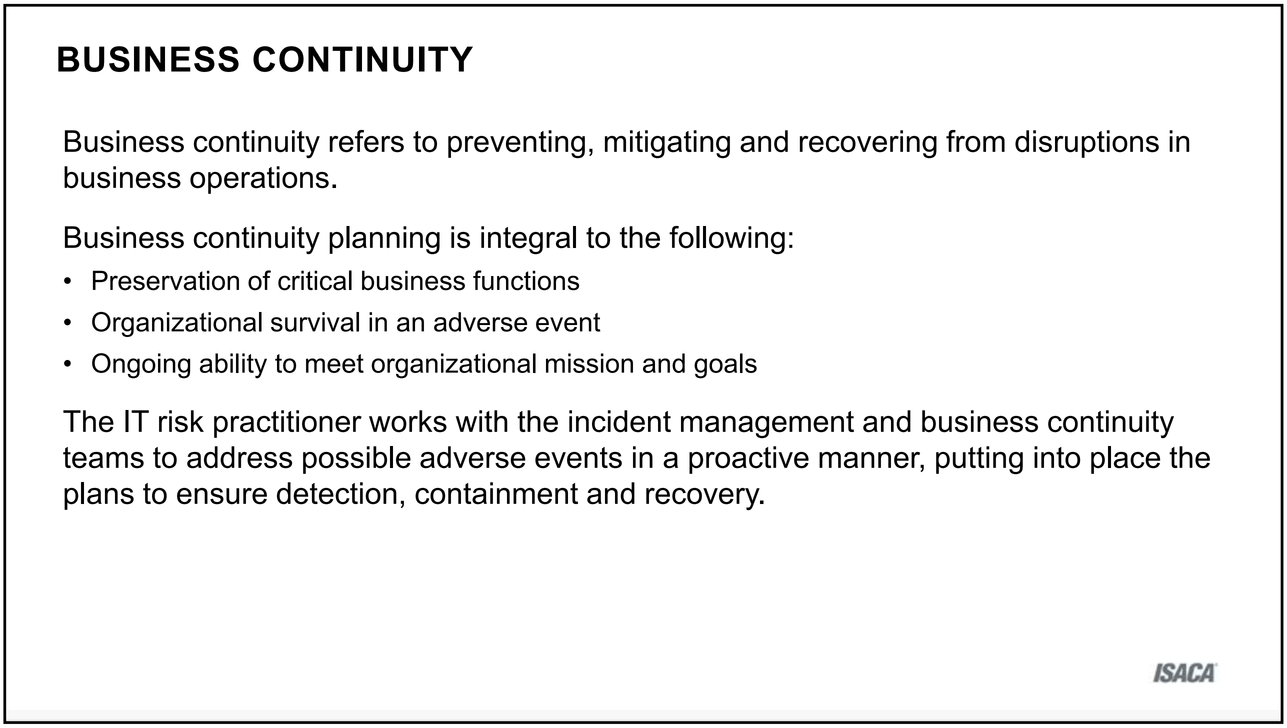
An IS audit should be conducted by objective, skilled and independent personnel able to:

- Assess risk
- Identify vulnerabilities
- Document findings
- Provide recommendations on how to address audit issues

Several risks are associated with the IS audit, as follows:

- The competency of the IS audit personnel may be lacking.
- The independence of the audit may be compromised.
- The audit may not discover a finding that could become material (“audit risk”).
- The audit may not detect a potential material finding (“detection risk”).
- The mitigation for a risk may be inadequate (“control risk”).

Each of these is a form of IT risk.



BUSINESS CONTINUITY

Business continuity refers to preventing, mitigating and recovering from disruptions in business operations.

Business continuity planning is integral to the following:

- Preservation of critical business functions
- Organizational survival in an adverse event
- Ongoing ability to meet organizational mission and goals

The IT risk practitioner works with the incident management and business continuity teams to address possible adverse events in a proactive manner, putting into place the plans to ensure detection, containment and recovery.

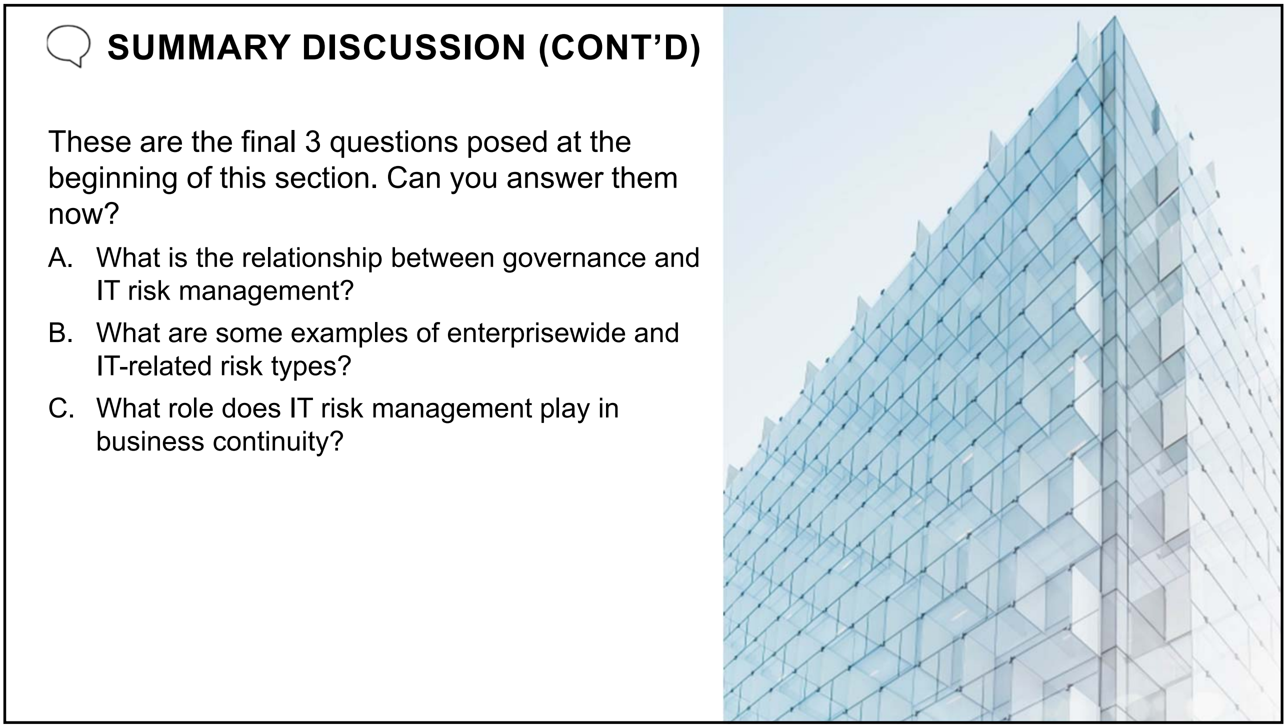
SUMMARY DISCUSSION

At the beginning of this section, the material to be covered was presented as a list of questions. How would you answer these questions now?

A. What is risk and risk management, especially in the context of information technology (IT)?

B. Why is IT risk management important to the enterprise?

C. What process is used to identify and address IT-related risk?



SUMMARY DISCUSSION (CONT’D)

These are the final 3 questions posed at the beginning of this section. Can you answer them now?

A. What is the relationship between governance and IT risk management?

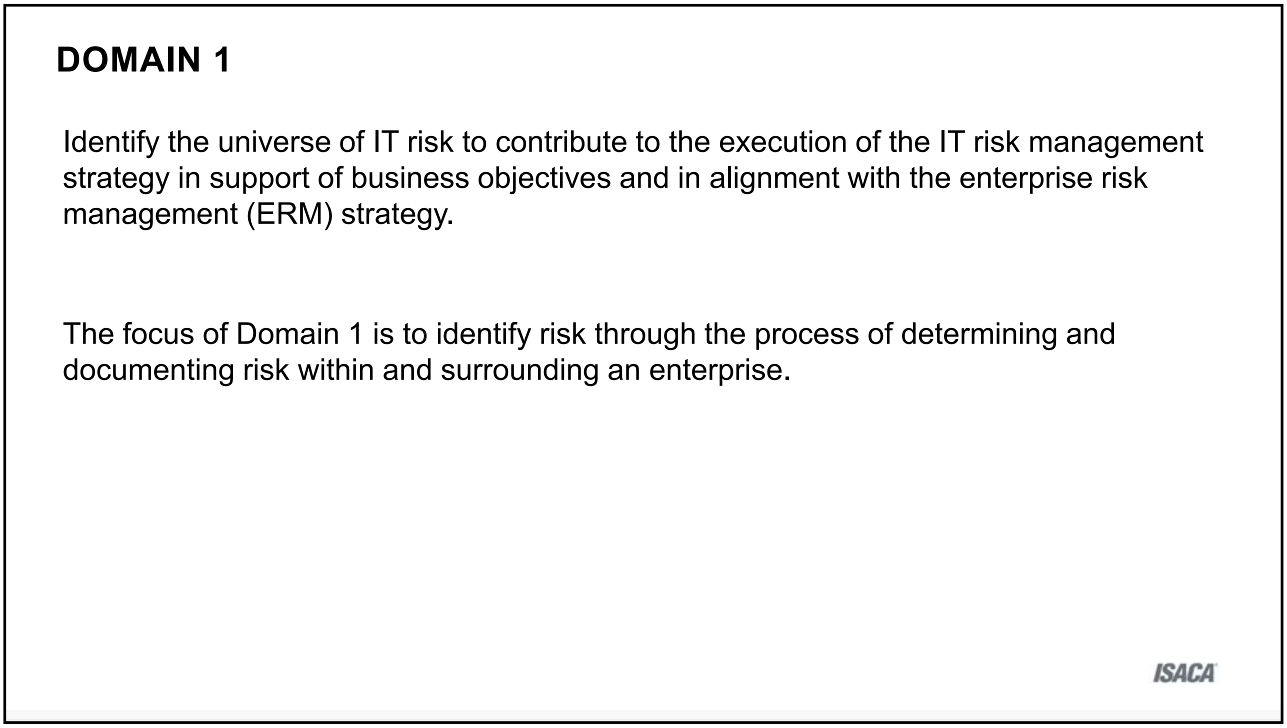
B. What are some examples of enterprisewide and IT-related risk types?

C. What role does IT risk management play in business continuity?

ISACA®

DOMAIN 1

IT RISK IDENTIFICATION



DOMAIN 1

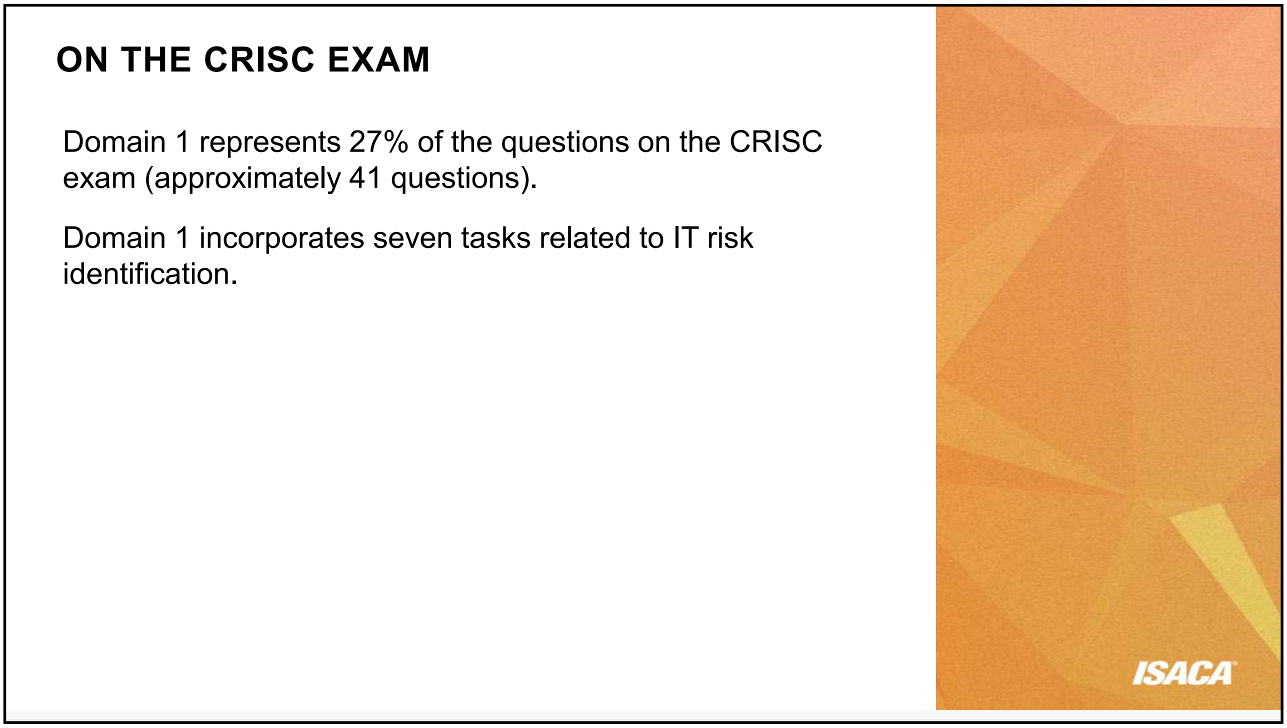
Identify the universe of IT risk to contribute to the execution of the IT risk management strategy in support of business objectives and in alignment with the enterprise risk management (ERM) strategy.

The focus of Domain 1 is to identify risk through the process of determining and documenting risk within and surrounding an enterprise.

LEARNING OBJECTIVES

The objective of this domain is to ensure that the CRISC candidate has the knowledge necessary to:

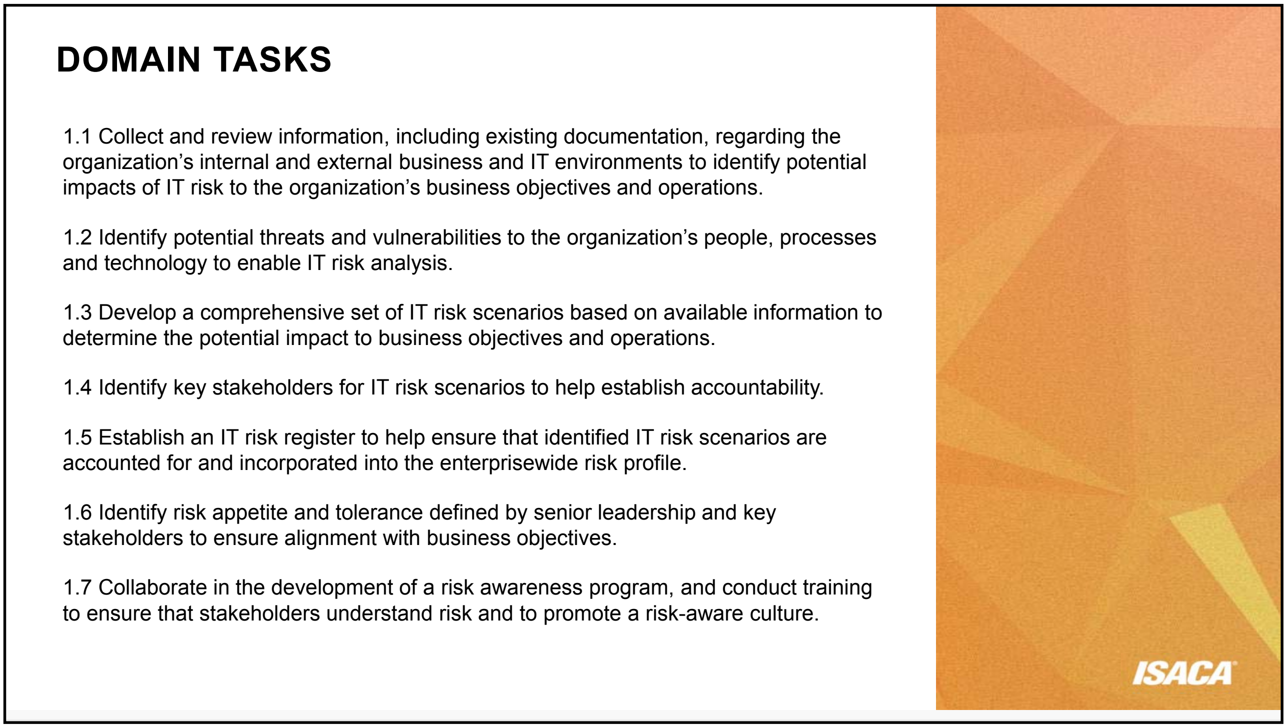
1. Identify relevant standards, frameworks and practices.
2. Apply risk identification techniques.
3. Distinguish between threats and vulnerabilities.
4. Identify relevant stakeholders.
5. Discuss risk scenario development tools and techniques.
6. Explain the meaning of key risk management concepts, including risk appetite and risk tolerance.
7. Describe the key elements of a risk register.
8. Contribute to the creation of a risk awareness program.



ON THE CRISC EXAM

Domain 1 represents 27% of the questions on the CRISC exam (approximately 41 questions).

Domain 1 incorporates seven tasks related to IT risk identification.



DOMAIN TASKS

1.1 Collect and review information, including existing documentation, regarding the organization’s internal and external business and IT environments to identify potential 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.

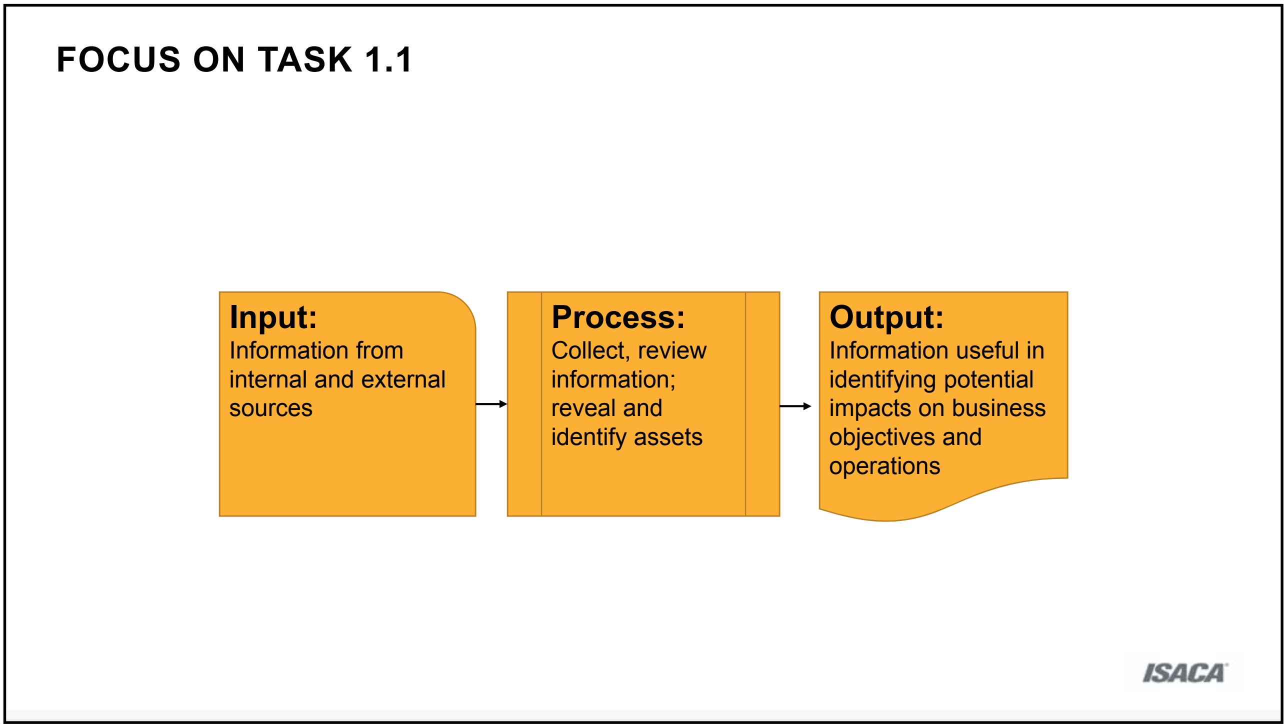
1.5 Establish an IT risk register to help ensure that identified IT risk scenarios are accounted for and incorporated into the enterprisewide risk profile.

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.

TASK 1.1

Collect and review information, including existing documentation, regarding the organization’s internal and external business and IT environments to identify potential impacts of IT risk to the organization’s business objectives and operations.

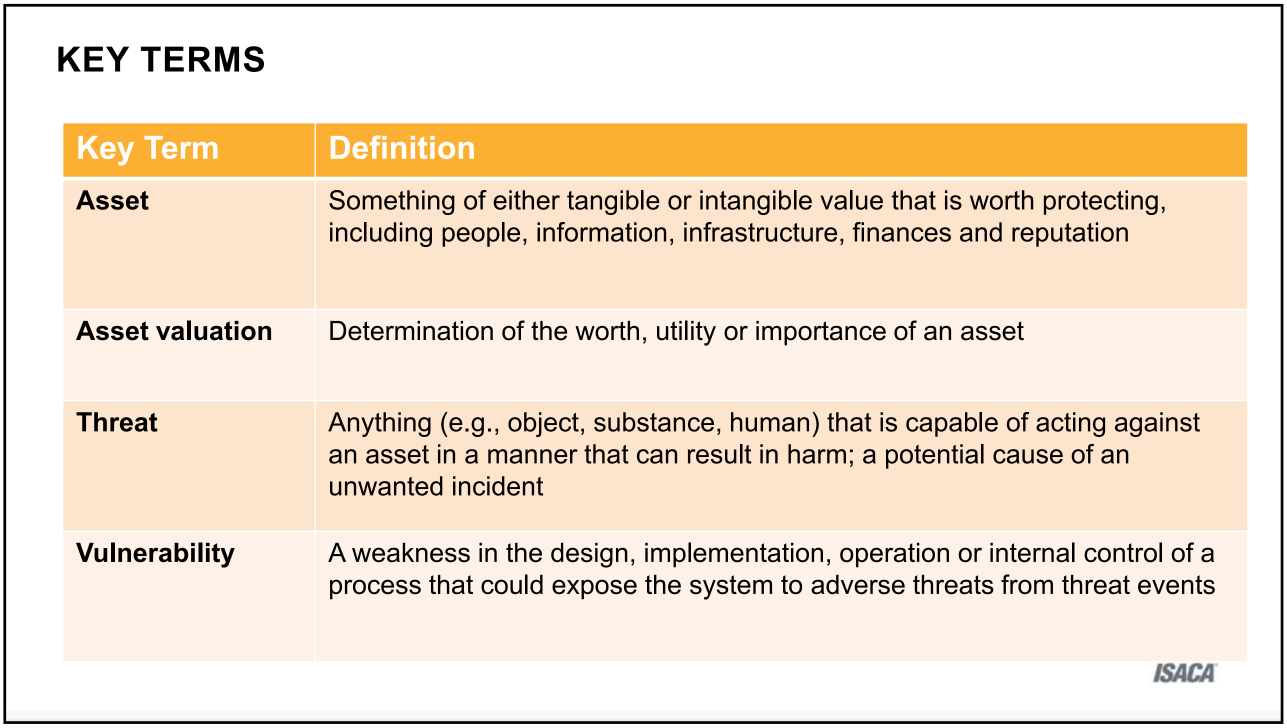


FOCUS ON TASK 1.1

Input:
Information from internal and external sources

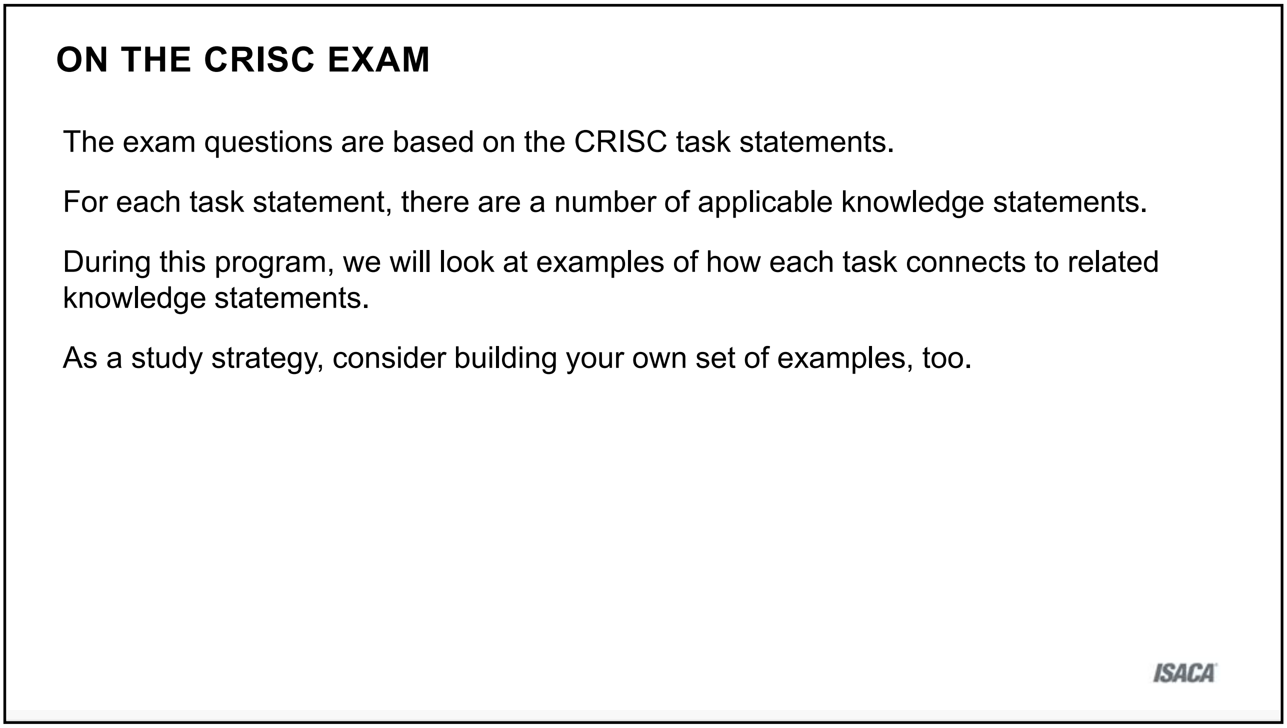
Process:
Collect, review information; reveal and identify assets

Output:
Information useful in identifying potential impacts on business objectives and operations



KEY TERMS

Key Term	Definition
Asset	Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation
Asset valuation	Determination of the worth, utility or importance of an asset
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
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



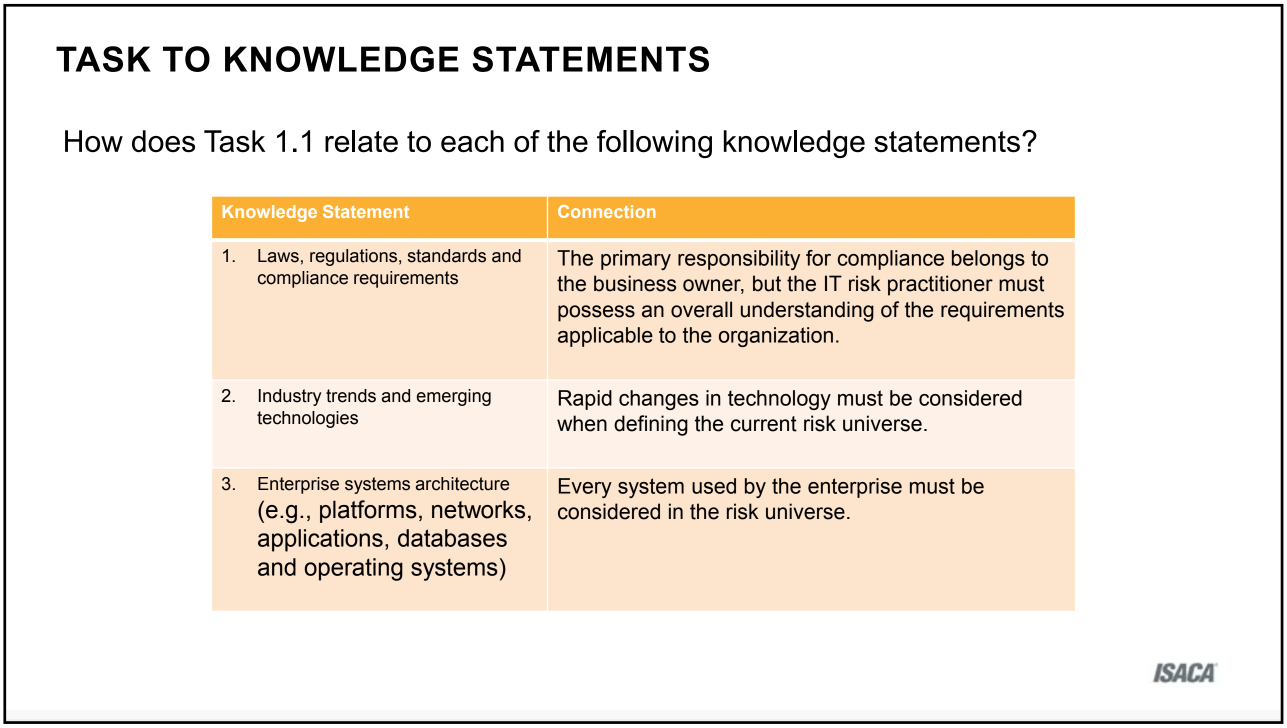
ON THE CRISC EXAM

The exam questions are based on the CRISC task statements.

For each task statement, there are a number of applicable knowledge statements.

During this program, we will look at examples of how each task connects to related knowledge statements.

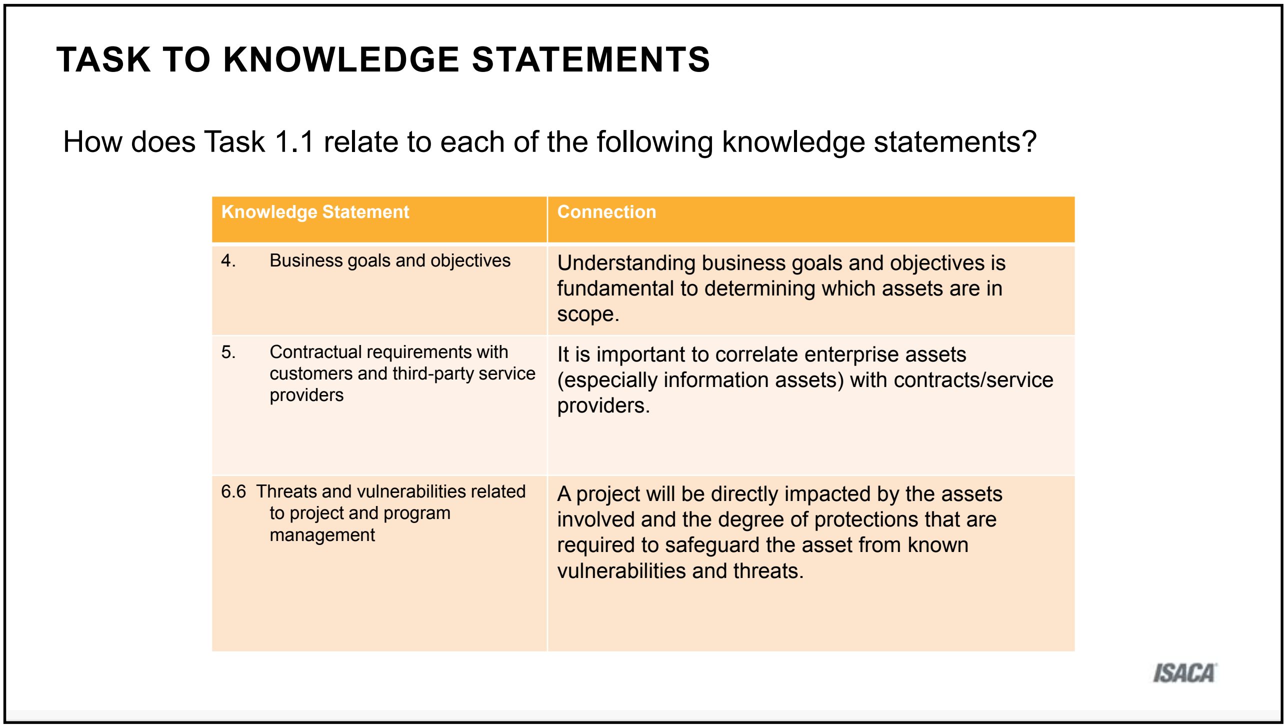
As a study strategy, consider building your own set of examples, too.



TASK TO KNOWLEDGE STATEMENTS

How does Task 1.1 relate to each of the following knowledge statements?

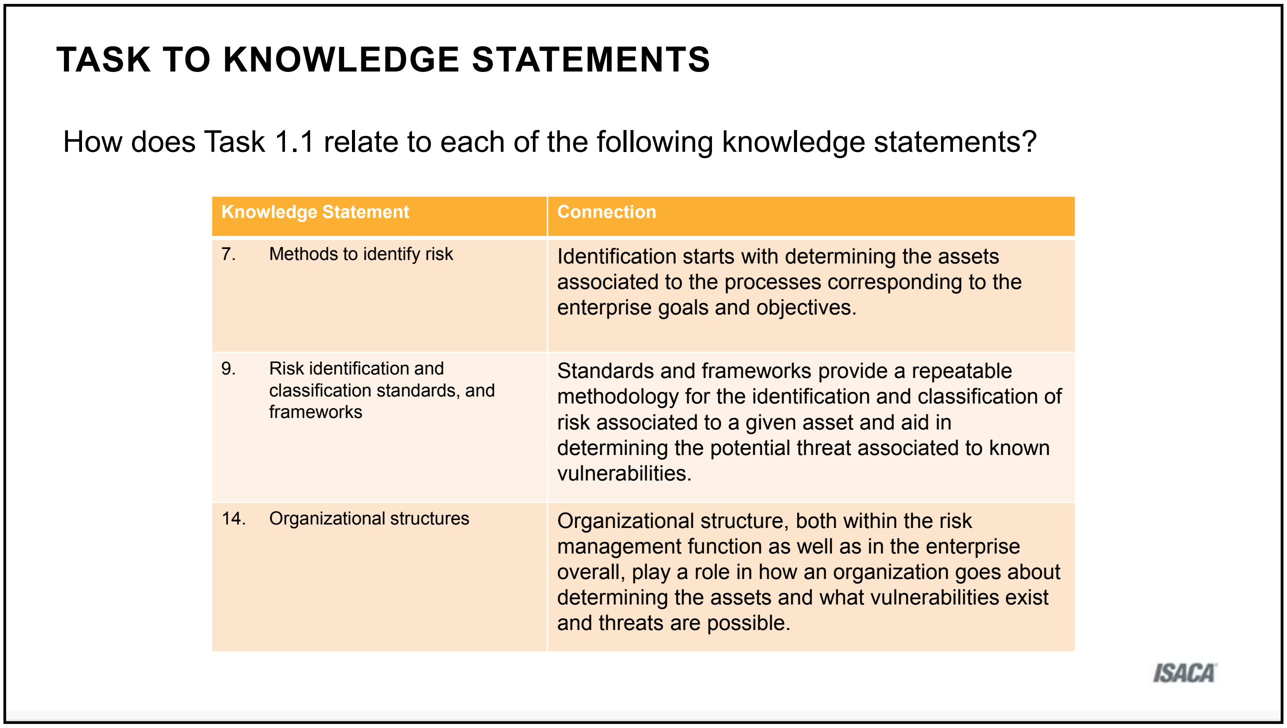
Knowledge Statement	Connection
1. Laws, regulations, standards and compliance requirements	The primary responsibility for compliance belongs to the business owner, but the IT risk practitioner must possess an overall understanding of the requirements applicable to the organization.
2. Industry trends and emerging technologies	Rapid changes in technology must be considered when defining the current risk universe.
3. Enterprise systems architecture (e.g., platforms, networks, applications, databases and operating systems)	Every system used by the enterprise must be considered in the risk universe.



TASK TO KNOWLEDGE STATEMENTS

How does Task 1.1 relate to each of the following knowledge statements?

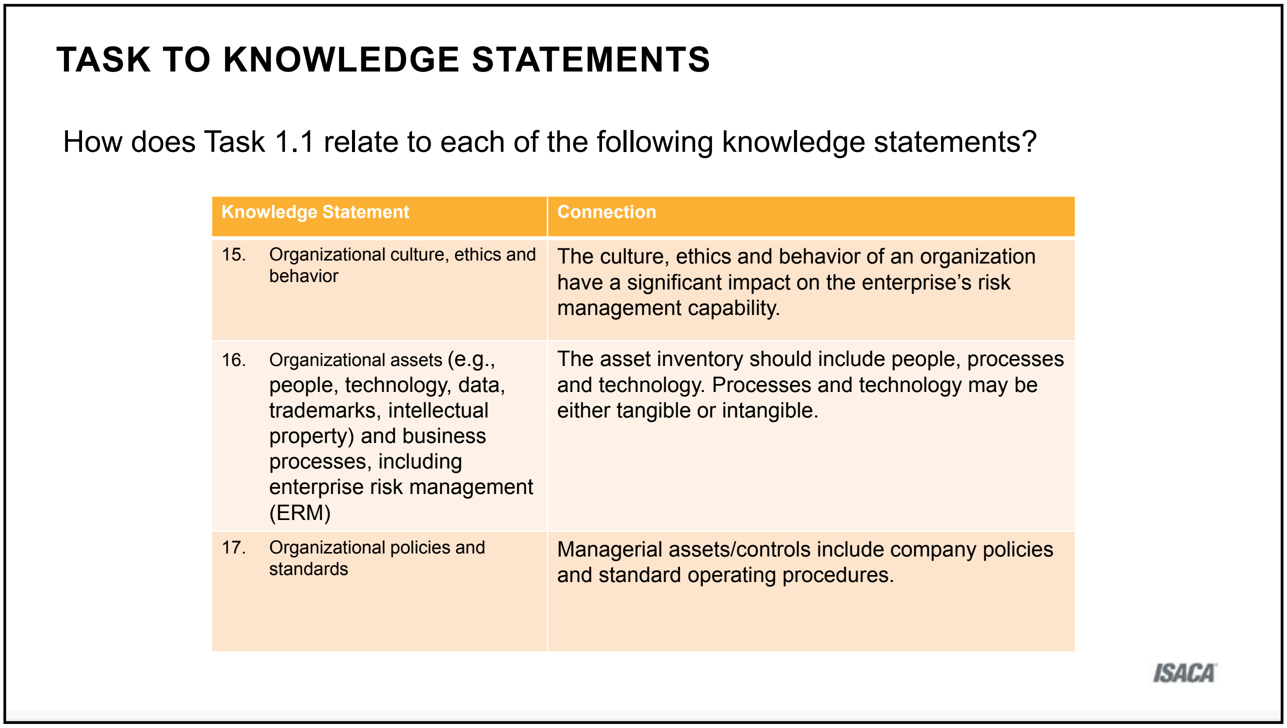
Knowledge Statement	Connection
4. Business goals and objectives	Understanding business goals and objectives is fundamental to determining which assets are in scope.
5. Contractual requirements with customers and third-party service providers	It is important to correlate enterprise assets (especially information assets) with contracts/service providers.
6.6 Threats and vulnerabilities related to project and program management	A project will be directly impacted by the assets involved and the degree of protections that are required to safeguard the asset from known vulnerabilities and threats.



TASK TO KNOWLEDGE STATEMENTS

How does Task 1.1 relate to each of the following knowledge statements?

Knowledge Statement	Connection
7. Methods to identify risk	Identification starts with determining the assets associated to the processes corresponding to the enterprise goals and objectives.
9. Risk identification and classification standards, and frameworks	Standards and frameworks provide a repeatable methodology for the identification and classification of risk associated to a given asset and aid in determining the potential threat associated to known vulnerabilities.
14. Organizational structures	Organizational structure, both within the risk management function as well as in the enterprise overall, play a role in how an organization goes about determining the assets and what vulnerabilities exist and threats are possible.

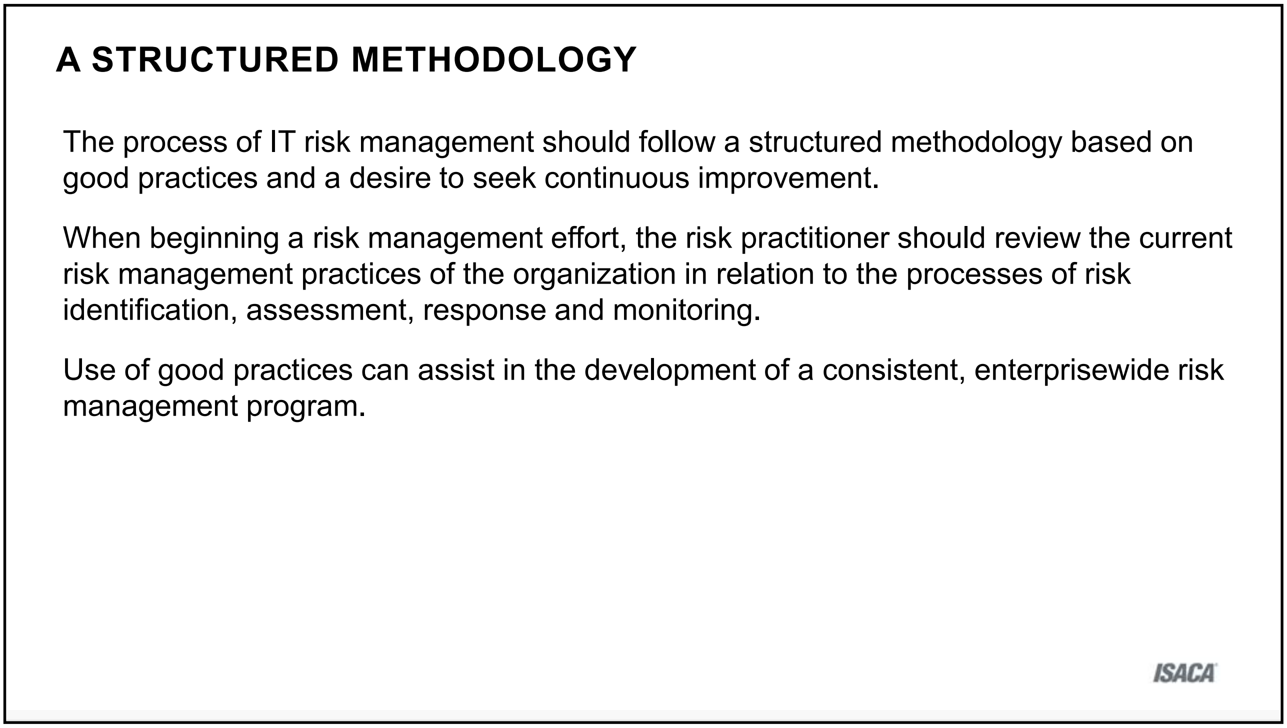


TASK TO KNOWLEDGE STATEMENTS

How does Task 1.1 relate to each of the following knowledge statements?

Knowledge Statement	Connection
15. Organizational culture, ethics and behavior	The culture, ethics and behavior of an organization have a significant impact on the enterprise's risk management capability.
16. Organizational assets (e.g., people, technology, data, trademarks, intellectual property) and business processes, including enterprise risk management (ERM)	The asset inventory should include people, processes and technology. Processes and technology may be either tangible or intangible.
17. Organizational policies and standards	Managerial assets/controls include company policies and standard operating procedures.

ISACA

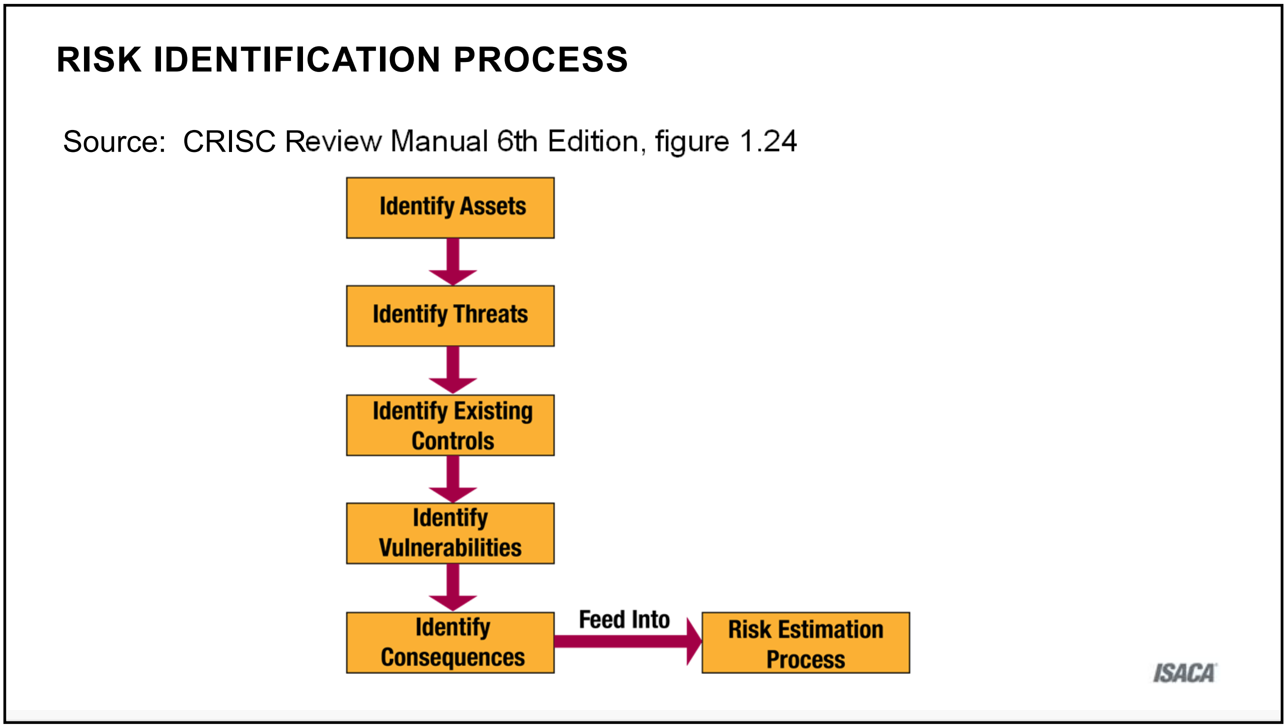


A STRUCTURED METHODOLOGY

The process of IT risk management should follow a structured methodology based on good practices and a desire to seek continuous improvement.

When beginning a risk management effort, the risk practitioner should review the current risk management practices of the organization in relation to the processes of risk identification, assessment, response and monitoring.

Use of good practices can assist in the development of a consistent, enterprisewide risk management program.



RISK IDENTIFICATION PROCESS

Source: CRISC Review Manual 6th Edition, figure 1.24

Identify Assets

Identify Threats

Identify Existing Controls

Identify Vulnerabilities

Identify Consequences

Feed Into

Risk Estimation Process

INFORMATION SOURCES

A variety of information sources aid in the identification of assets, vulnerabilities and threats, as follows:

Sources for Threat Information

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

Source: *CRISC Review Manual 6th Edition*, figure 1.11

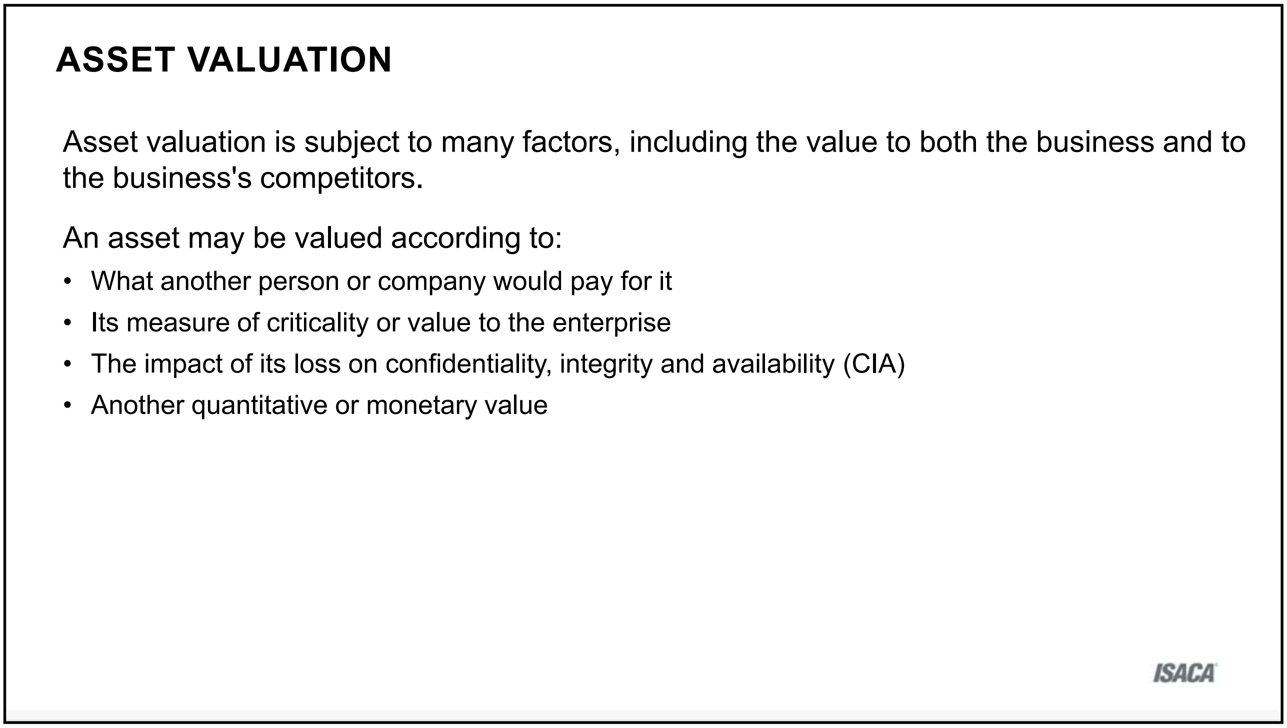
IDENTIFY ASSETS

IT risk management is concerned with the shielding of assets from threats.

An asset is something of either tangible or intangible value that is worth protecting.

Examples of assets include the following:

- Information
- Brand and reputation
- Intellectual property
- Facilities
- Equipment
- Cash and investments
- Customer lists
- Research
- People
- Service/ business processes

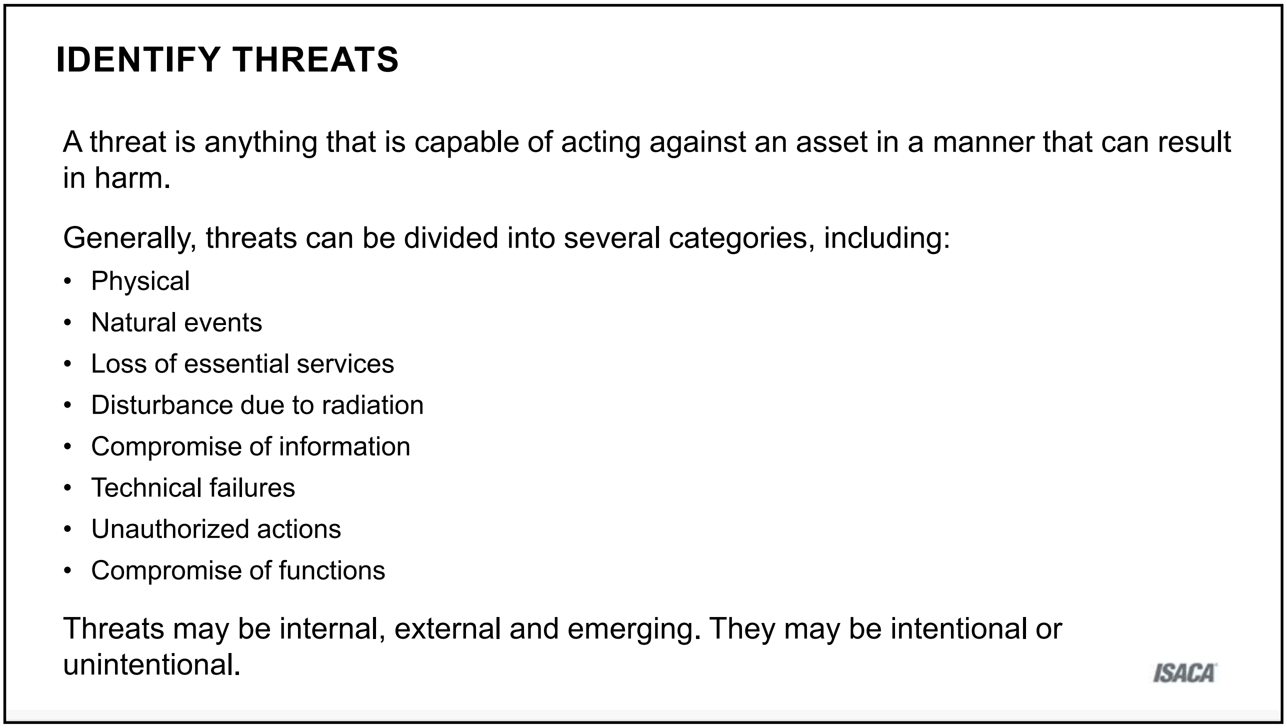


ASSET VALUATION

Asset valuation is subject to many factors, including the value to both the business and to the business's competitors.

An asset may be valued according to:

- What another person or company would pay for it
- Its measure of criticality or value to the enterprise
- The impact of its loss on confidentiality, integrity and availability (CIA)
- Another quantitative or monetary value



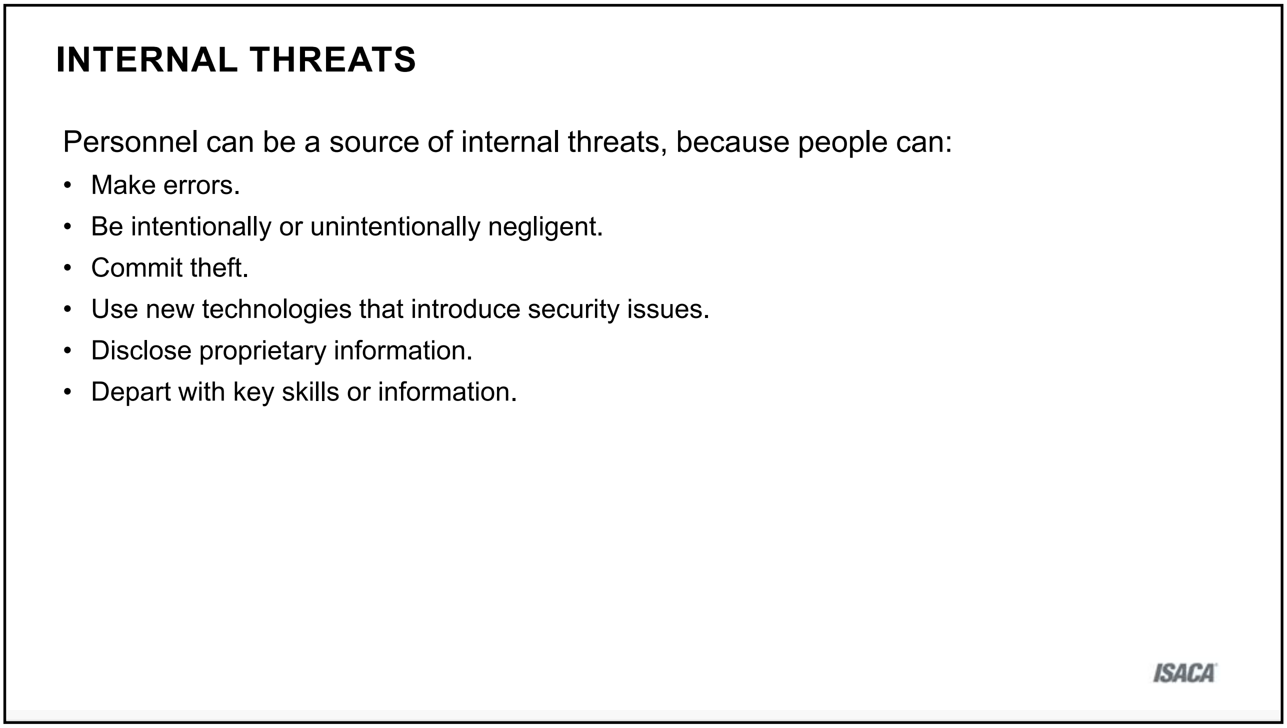
IDENTIFY THREATS

A threat is anything that is capable of acting against an asset in a manner that can result in harm.

Generally, threats can be divided into several categories, including:

- Physical
- Natural events
- Loss of essential services
- Disturbance due to radiation
- Compromise of information
- Technical failures
- Unauthorized actions
- Compromise of functions

Threats may be internal, external and emerging. They may be intentional or unintentional.



INTERNAL THREATS

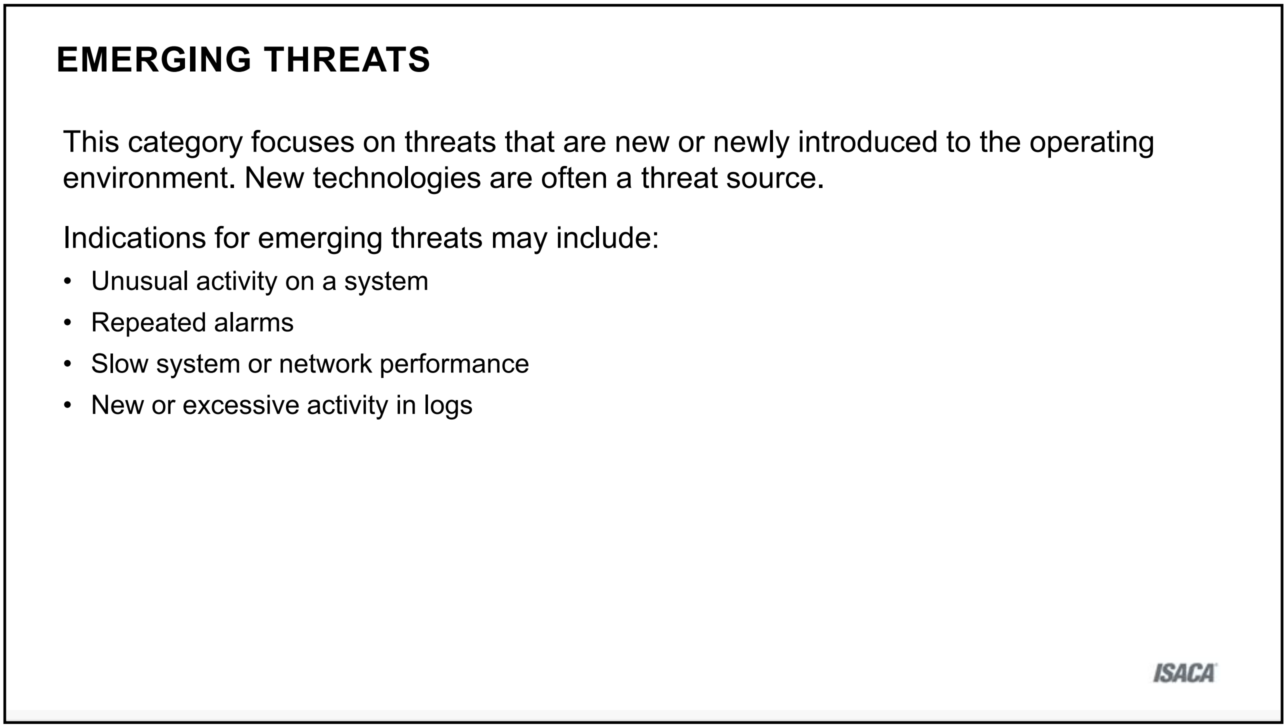
Personnel can be a source of internal threats, because people can:

- Make errors.
- Be intentionally or unintentionally negligent.
- Commit theft.
- Use new technologies that introduce security issues.
- Disclose proprietary information.
- Depart with key skills or information.

EXTERNAL THREATS

A wide range of external threats may present risk to an enterprise, including:

- Theft
- Sabotage
- Terrorism
- Espionage
- Criminal acts
- Software errors
- Hardware flaws
- Mechanical failures
- Lost assets
- Data corruption
- Facility breakdowns
- Fire or flooding
- Supply chain interruption
- Industrial accidents
- Disease (epidemic)
- Seismic activity
- Severe weather
- Power surge/utility failure

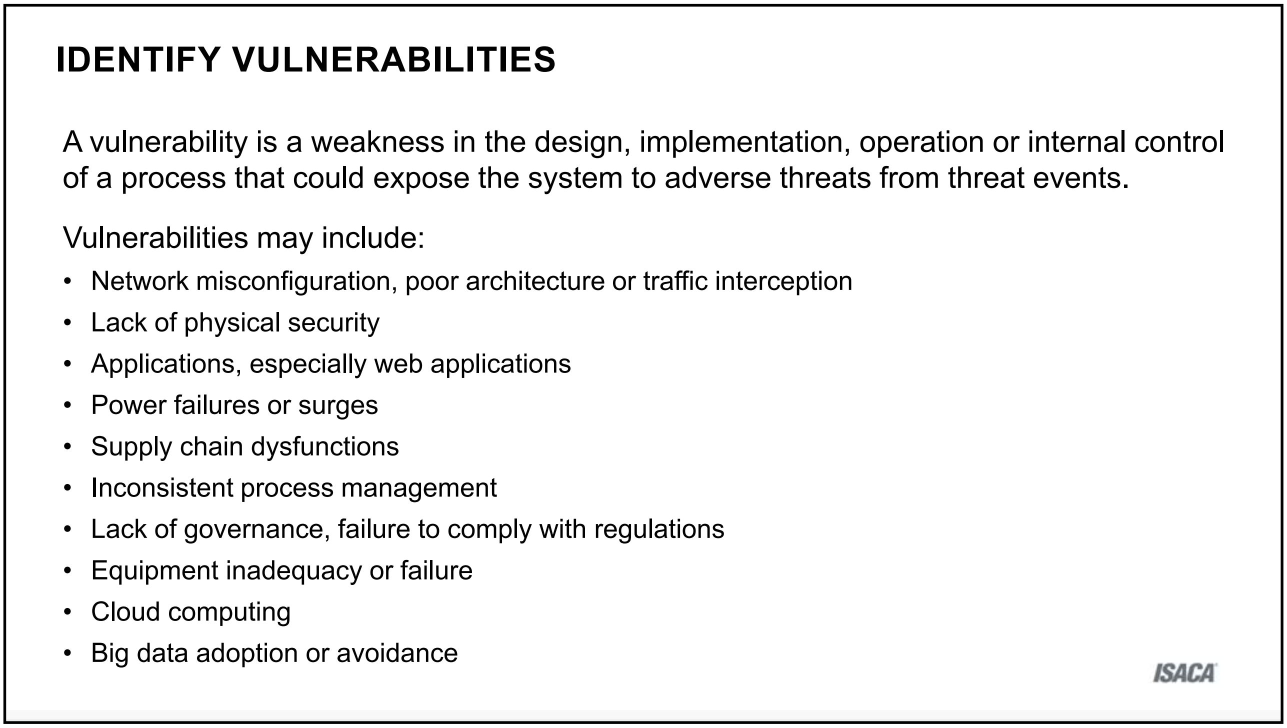


EMERGING THREATS

This category focuses on threats that are new or newly introduced to the operating environment. New technologies are often a threat source.

Indications for emerging threats may include:

- Unusual activity on a system
- Repeated alarms
- Slow system or network performance
- New or excessive activity in logs



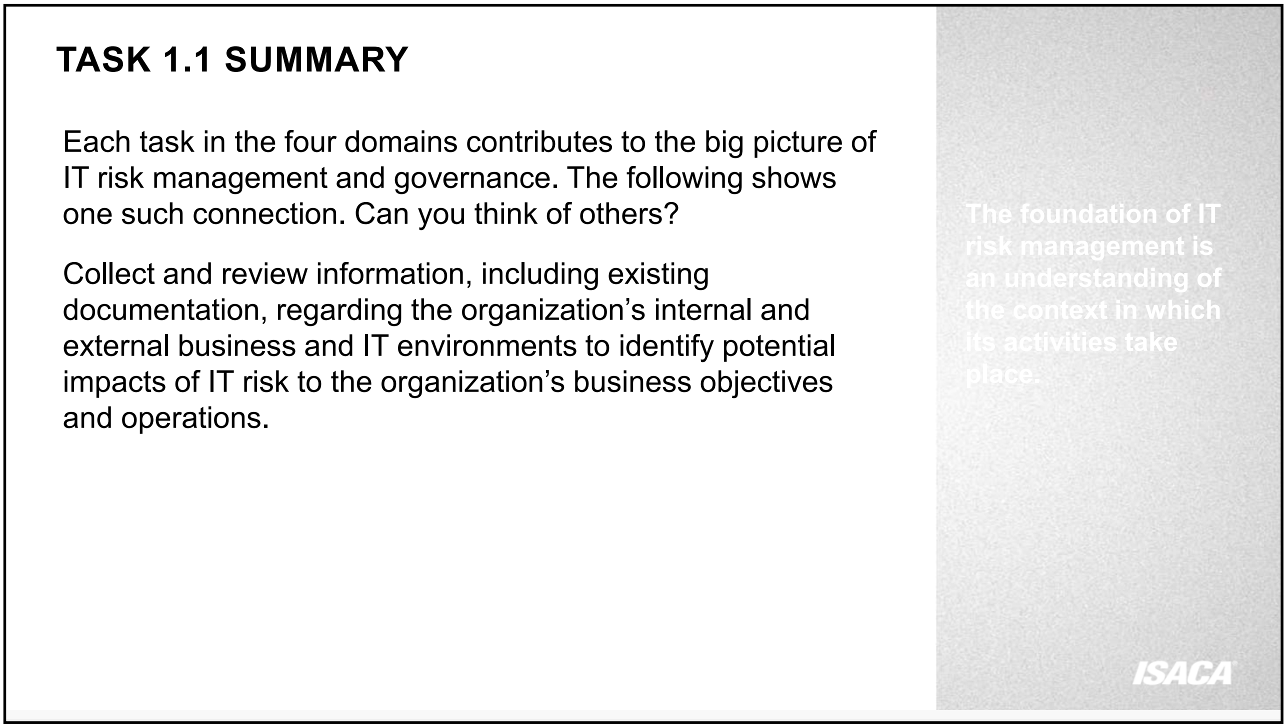
IDENTIFY VULNERABILITIES

A vulnerability is a weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events.

Vulnerabilities may include:

- Network misconfiguration, poor architecture or traffic interception
- Lack of physical security
- Applications, especially web applications
- Power failures or surges
- Supply chain dysfunctions
- Inconsistent process management
- Lack of governance, failure to comply with regulations
- Equipment inadequacy or failure
- Cloud computing
- Big data adoption or avoidance

ISACA



TASK 1.1 SUMMARY

Each task in the four domains contributes to the big picture of IT risk management and governance. The following shows one such connection. Can you think of others?

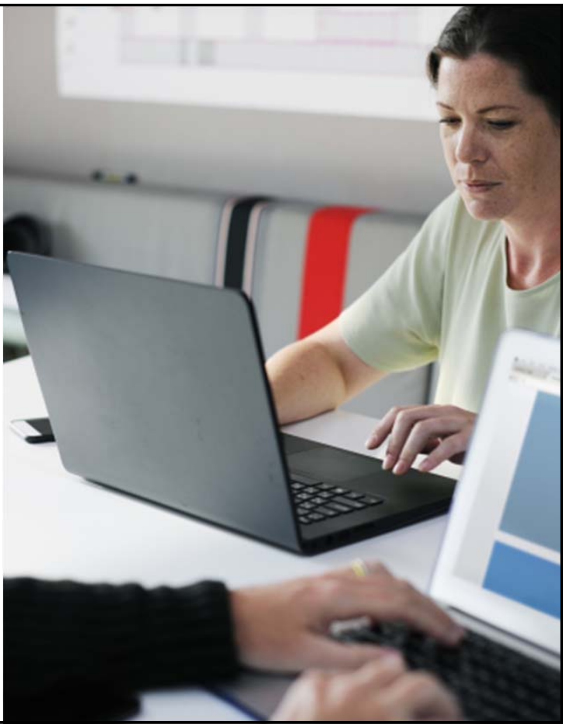
Collect and review information, including existing documentation, regarding the organization’s internal and external business and IT environments to identify potential impacts of IT risk to the organization’s business objectives and operations.

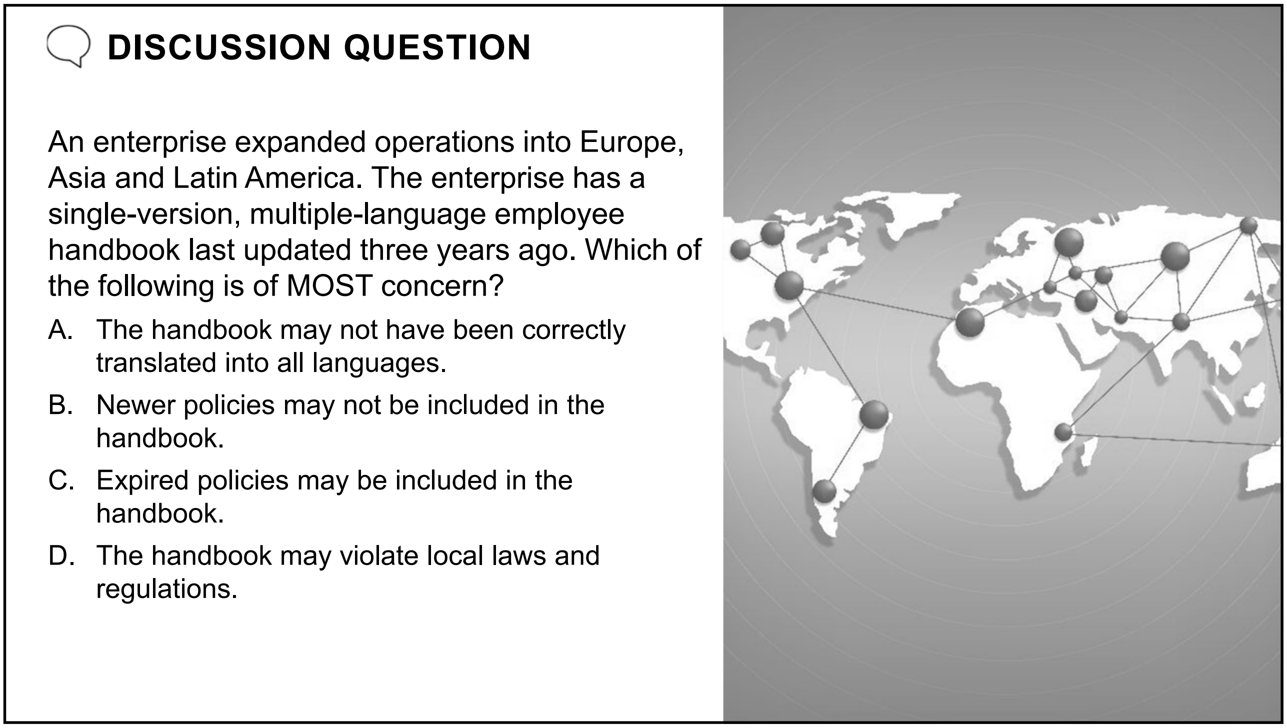
The foundation of IT risk management is an understanding of the context in which its activities take place.

TASK 1.1 ACTIVITY

Consider one critical business process with which you are familiar.

Write down the assets affiliated with this process.





DISCUSSION QUESTION

An enterprise expanded operations into Europe, Asia and Latin America. The enterprise has a single-version, multiple-language employee handbook last updated three years ago. Which of the following is of MOST concern?

A. The handbook may not have been correctly translated into all languages.

B. Newer policies may not be included in the handbook.

C. Expired policies may be included in the handbook.

D. The handbook may violate local laws and regulations.

🗨 DISCUSSION QUESTION

Which of the following is the BEST approach when conducting an IT risk awareness campaign?

A. Provide technical details on exploits.

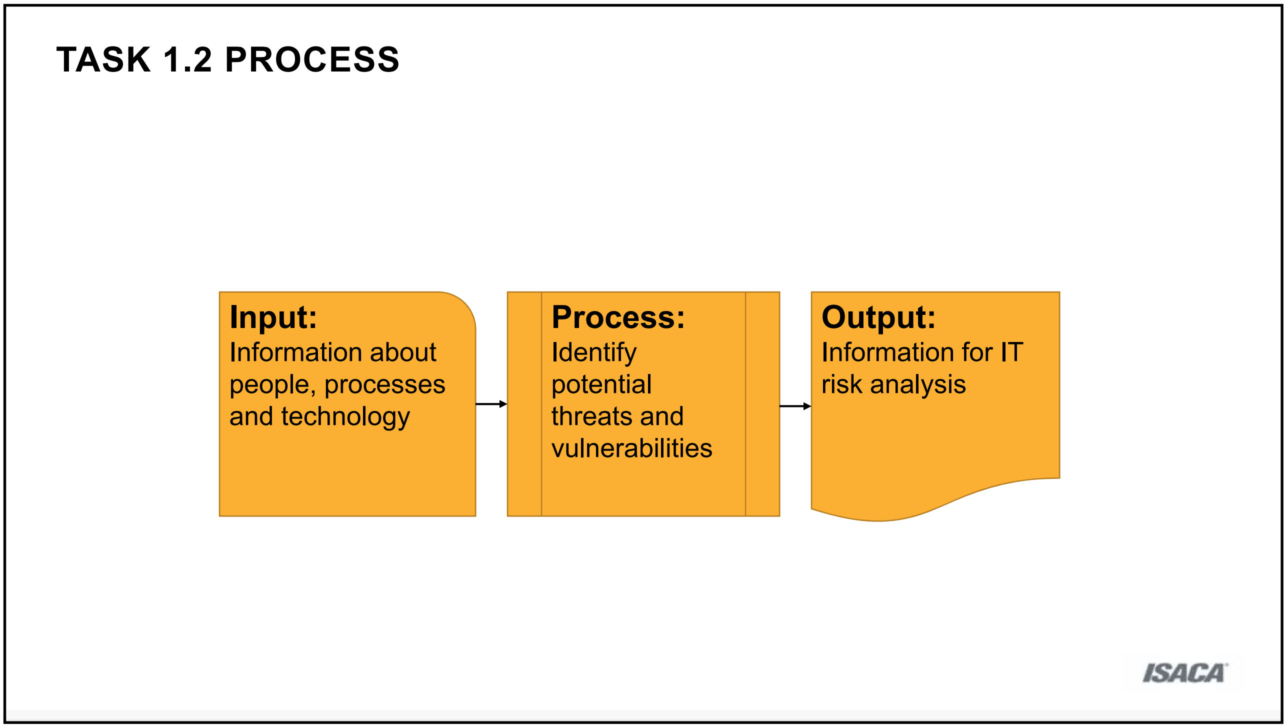
B. Provide common messages tailored for different groups.

C. Target system administrators and help desk staff.

D. Target senior managers and business process owners.

TASK 1.2

Identify potential threats and vulnerabilities to the organization’s people, processes and technology to enable IT risk analysis.

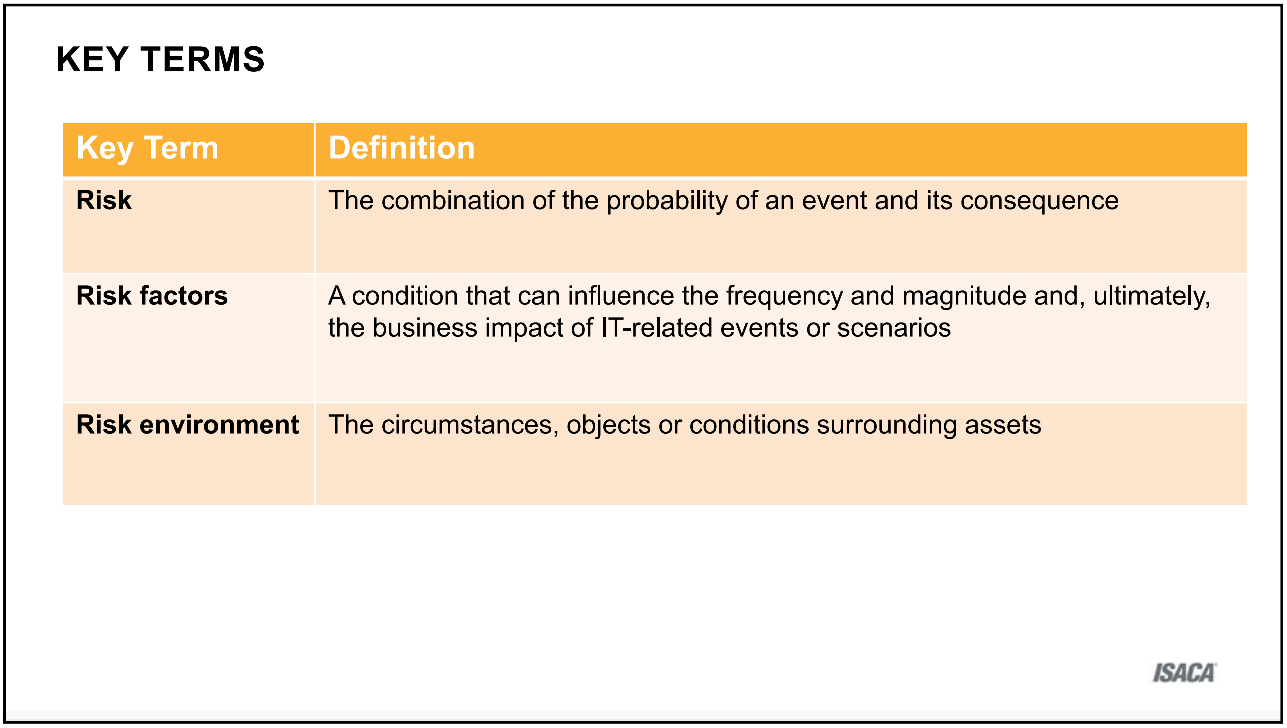


TASK 1.2 PROCESS

Input:
Information about people, processes and technology

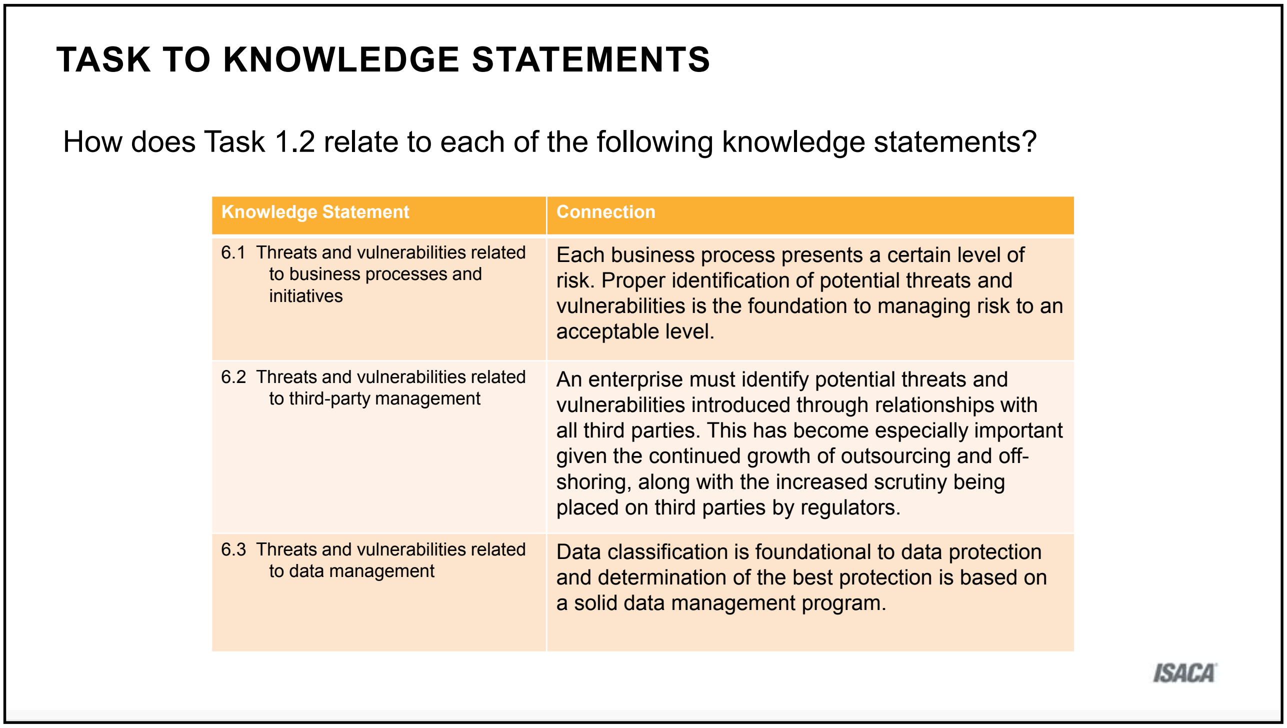
Process:
Identify potential threats and vulnerabilities

Output:
Information for IT risk analysis



KEY TERMS

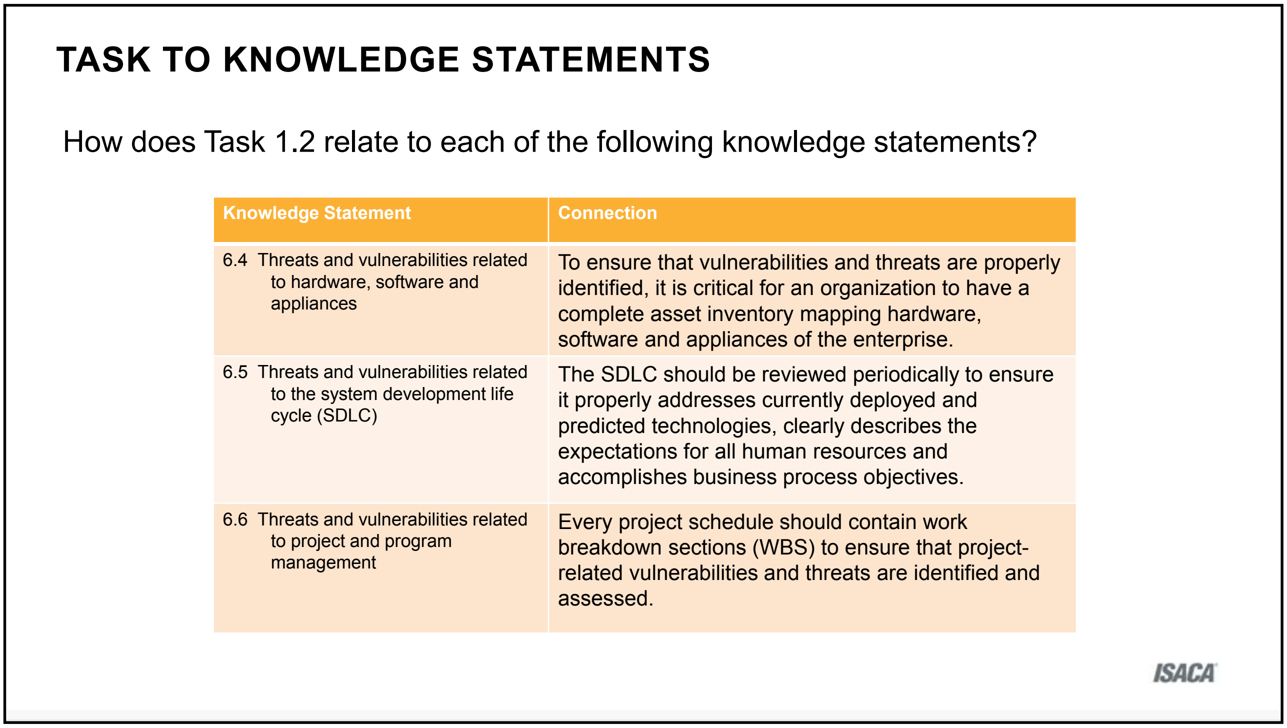
Key Term	Definition
Risk	The combination of the probability of an event and its consequence
Risk factors	A condition that can influence the frequency and magnitude and, ultimately, the business impact of IT-related events or scenarios
Risk environment	The circumstances, objects or conditions surrounding assets



TASK TO KNOWLEDGE STATEMENTS

How does Task 1.2 relate to each of the following knowledge statements?

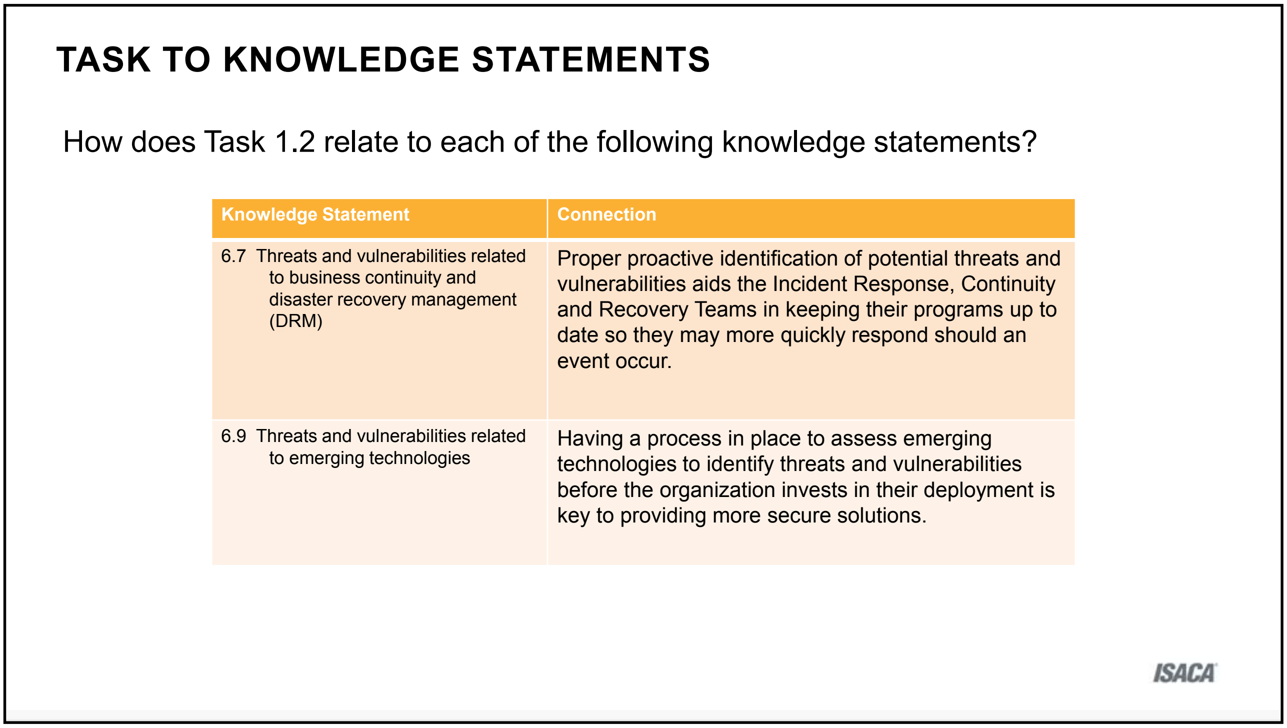
Knowledge Statement	Connection
6.1 Threats and vulnerabilities related to business processes and initiatives	Each business process presents a certain level of risk. Proper identification of potential threats and vulnerabilities is the foundation to managing risk to an acceptable level.
6.2 Threats and vulnerabilities related to third-party management	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 off-shoring, along with the increased scrutiny being placed on third parties by regulators.
6.3 Threats and vulnerabilities related to data management	Data classification is foundational to data protection and determination of the best protection is based on a solid data management program.



TASK TO KNOWLEDGE STATEMENTS

How does Task 1.2 relate to each of the following knowledge statements?

Knowledge Statement	Connection
6.4 Threats and vulnerabilities related to hardware, software and appliances	To ensure that vulnerabilities and threats are properly identified, it is critical for an organization to have a complete asset inventory mapping hardware, software and appliances of the enterprise.
6.5 Threats and vulnerabilities related to the system development life cycle (SDLC)	The SDLC should be reviewed periodically to ensure it properly addresses currently deployed and predicted technologies, clearly describes the expectations for all human resources and accomplishes business process objectives.
6.6 Threats and vulnerabilities related to project and program management	Every project schedule should contain work breakdown sections (WBS) to ensure that project-related vulnerabilities and threats are identified and assessed.

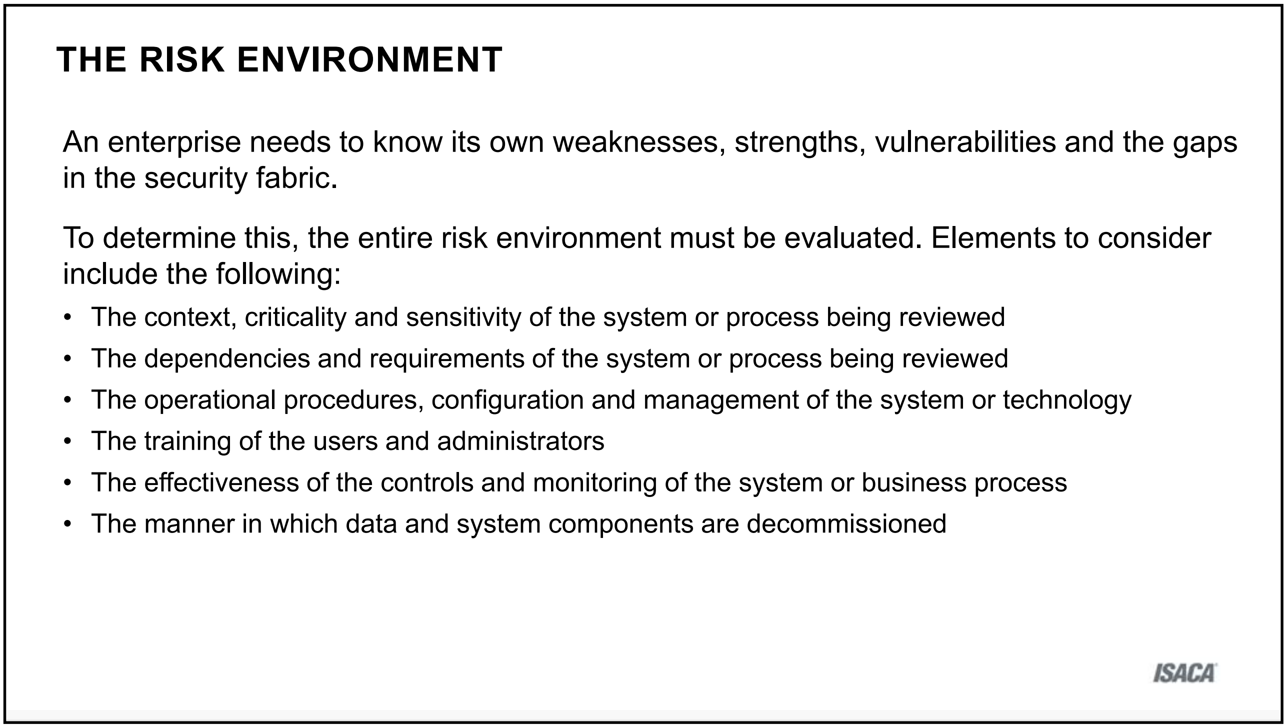


TASK TO KNOWLEDGE STATEMENTS

How does Task 1.2 relate to each of the following knowledge statements?

Knowledge Statement	Connection
6.7 Threats and vulnerabilities related to business continuity and disaster recovery management (DRM)	Proper proactive identification of potential threats and vulnerabilities aids the Incident Response, Continuity and Recovery Teams in keeping their programs up to date so they may more quickly respond should an event occur.
6.9 Threats and vulnerabilities related to emerging technologies	Having a process in place to assess emerging technologies to identify threats and vulnerabilities before the organization invests in their deployment is key to providing more secure solutions.

ISACA

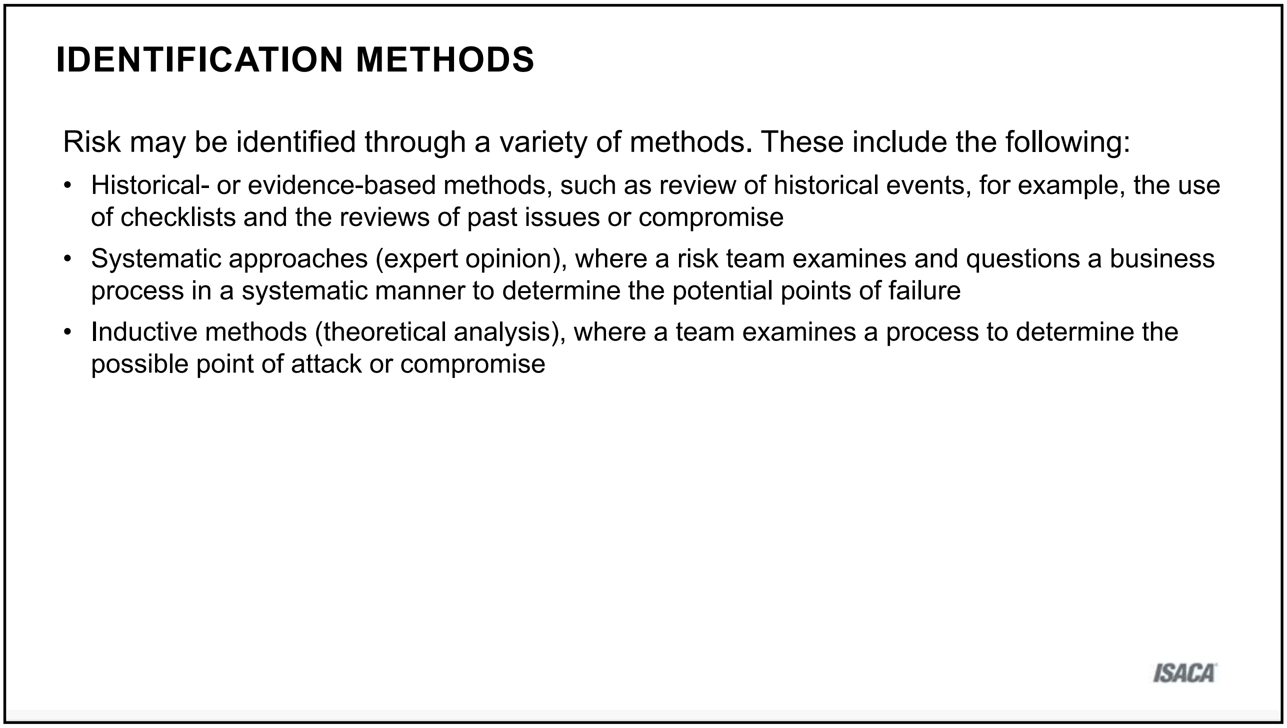


THE RISK ENVIRONMENT

An enterprise needs to know its own weaknesses, strengths, vulnerabilities and the gaps in the security fabric.

To determine this, the entire risk environment must be evaluated. Elements to consider include the following:

- The context, criticality and sensitivity of the system or process being reviewed
- The dependencies and requirements of the system or process being reviewed
- The operational procedures, configuration and management of the system or technology
- The training of the users and administrators
- The effectiveness of the controls and monitoring of the system or business process
- The manner in which data and system components are decommissioned

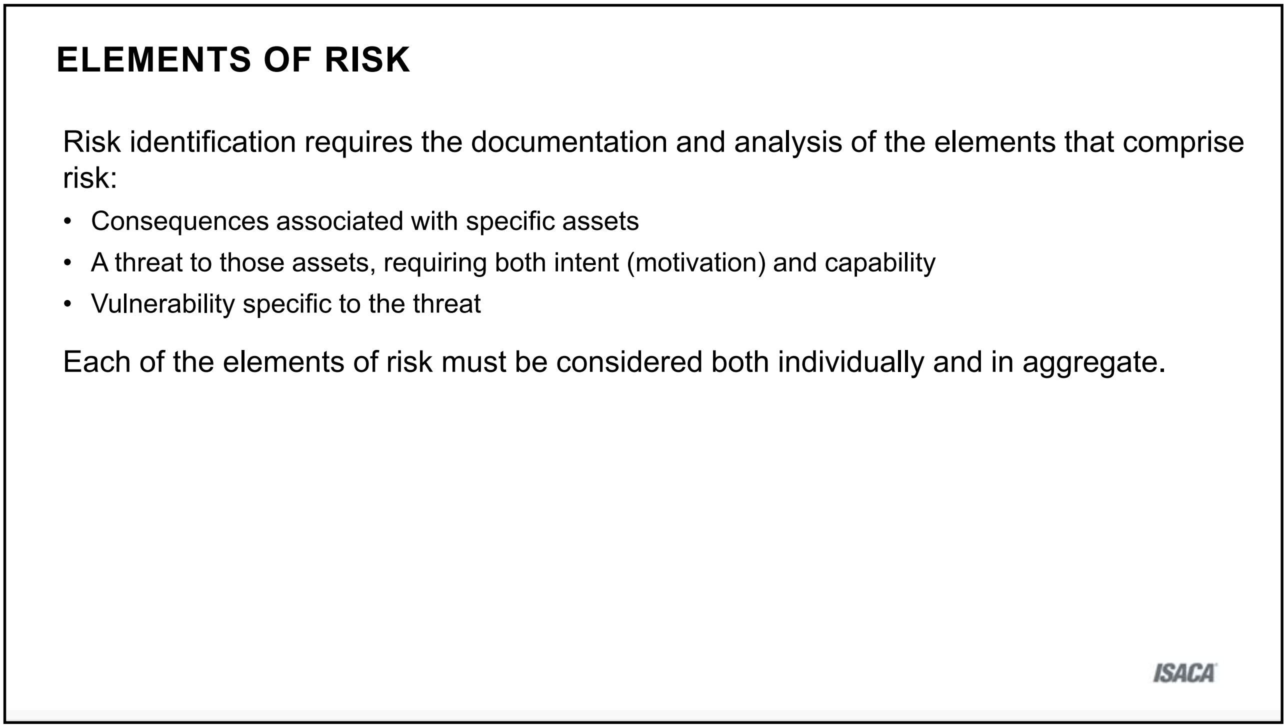


IDENTIFICATION METHODS

Risk may be identified through a variety of methods. These include the following:

- Historical- or evidence-based methods, such as review of historical events, for example, the use of checklists and the reviews of past issues or compromise
- Systematic approaches (expert opinion), where a risk team examines and questions a business process in a systematic manner to determine the potential points of failure
- Inductive methods (theoretical analysis), where a team examines a process to determine the possible point of attack or compromise

ISACA

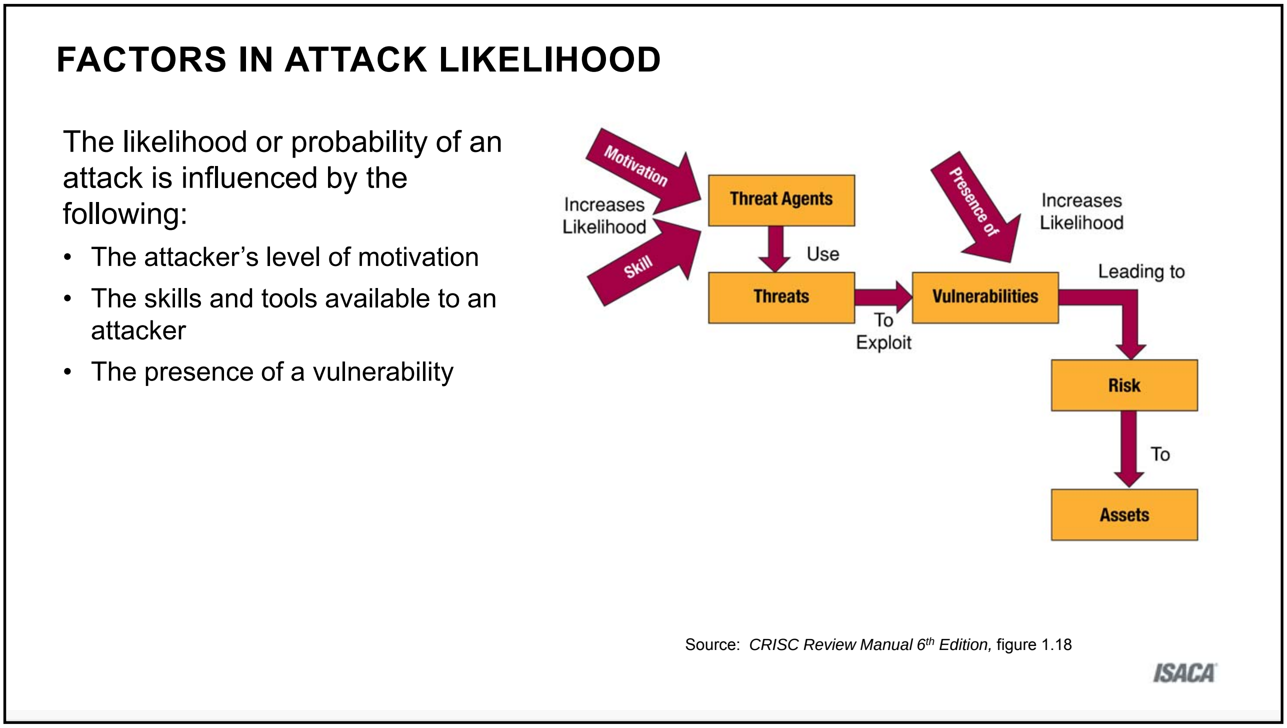


ELEMENTS OF RISK

Risk identification requires the documentation and analysis of the elements that comprise risk:

- Consequences associated with specific assets
- A threat to those assets, requiring both intent (motivation) and capability
- Vulnerability specific to the threat

Each of the elements of risk must be considered both individually and in aggregate.

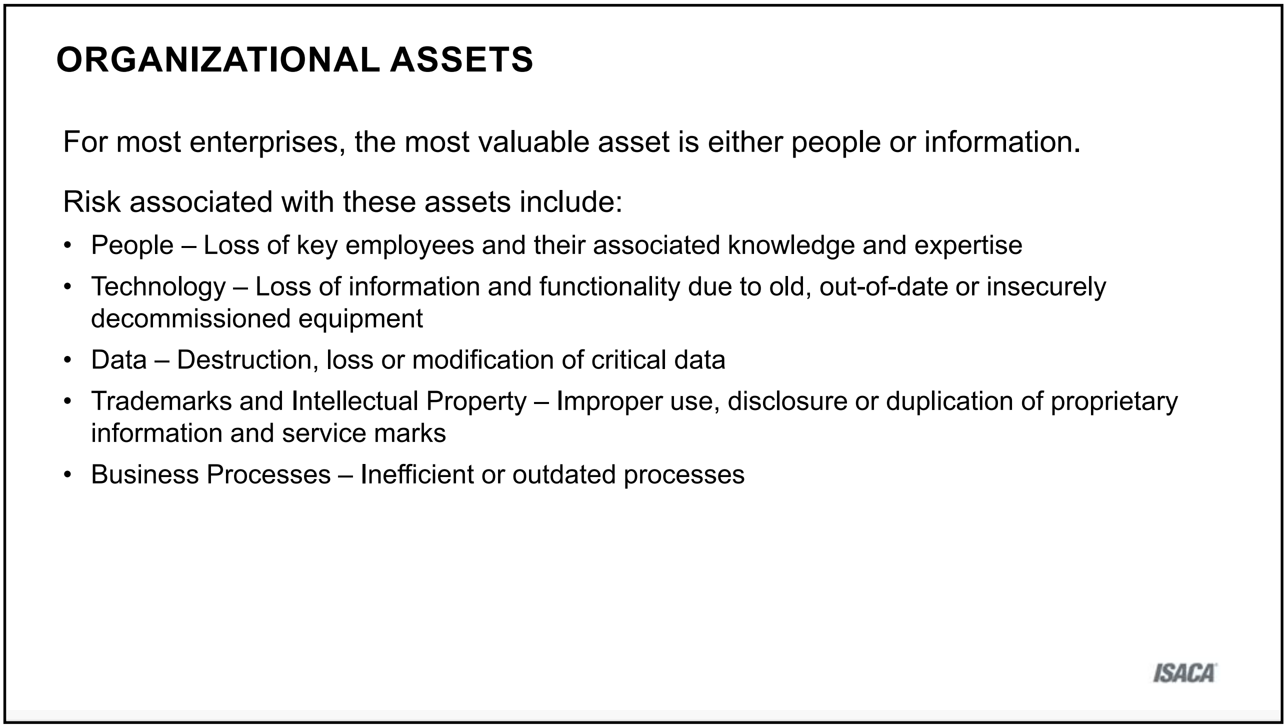


FACTORS IN ATTACK LIKELIHOOD

The likelihood or probability of an attack is influenced by the following:

- The attacker's level of motivation
- The skills and tools available to an attacker
- The presence of a vulnerability

Source: *CRISC Review Manual 6th Edition*, figure 1.18

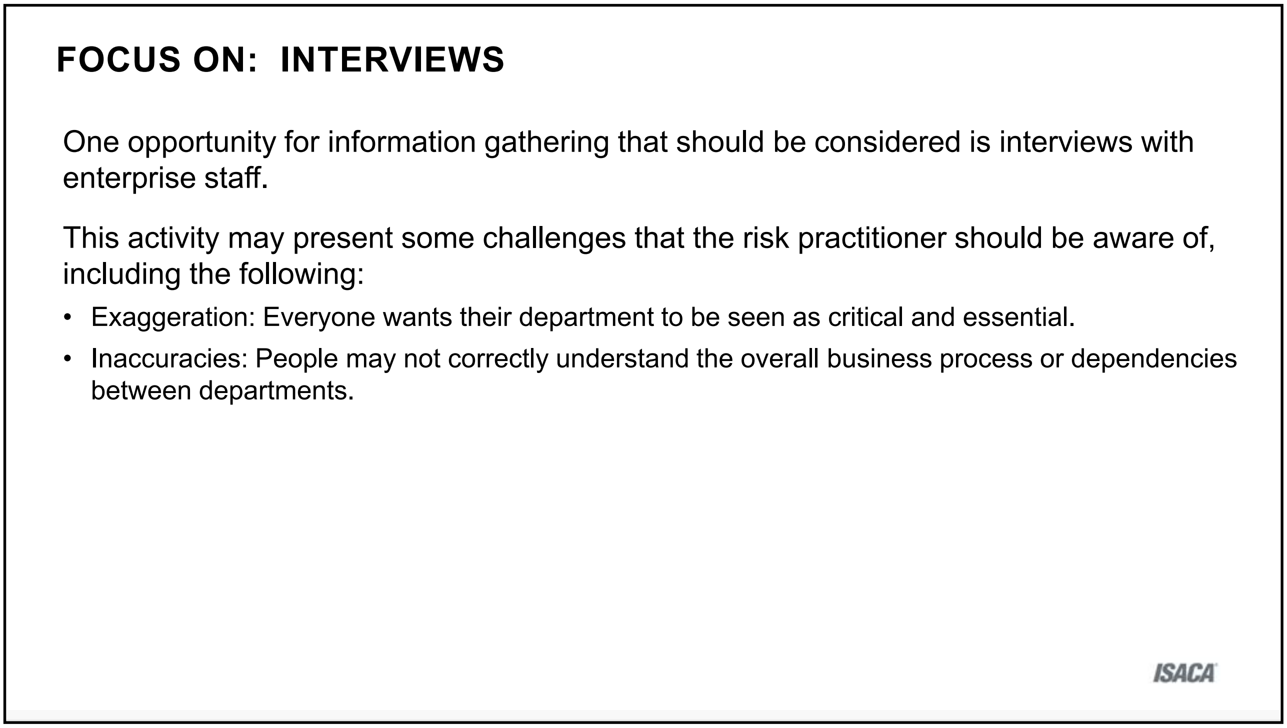


ORGANIZATIONAL ASSETS

For most enterprises, the most valuable asset is either people or information.

Risk associated with these assets include:

- People – Loss of key employees and their associated knowledge and expertise
- Technology – Loss of information and functionality due to old, out-of-date or insecurely decommissioned equipment
- Data – Destruction, loss or modification of critical data
- Trademarks and Intellectual Property – Improper use, disclosure or duplication of proprietary information and service marks
- Business Processes – Inefficient or outdated processes

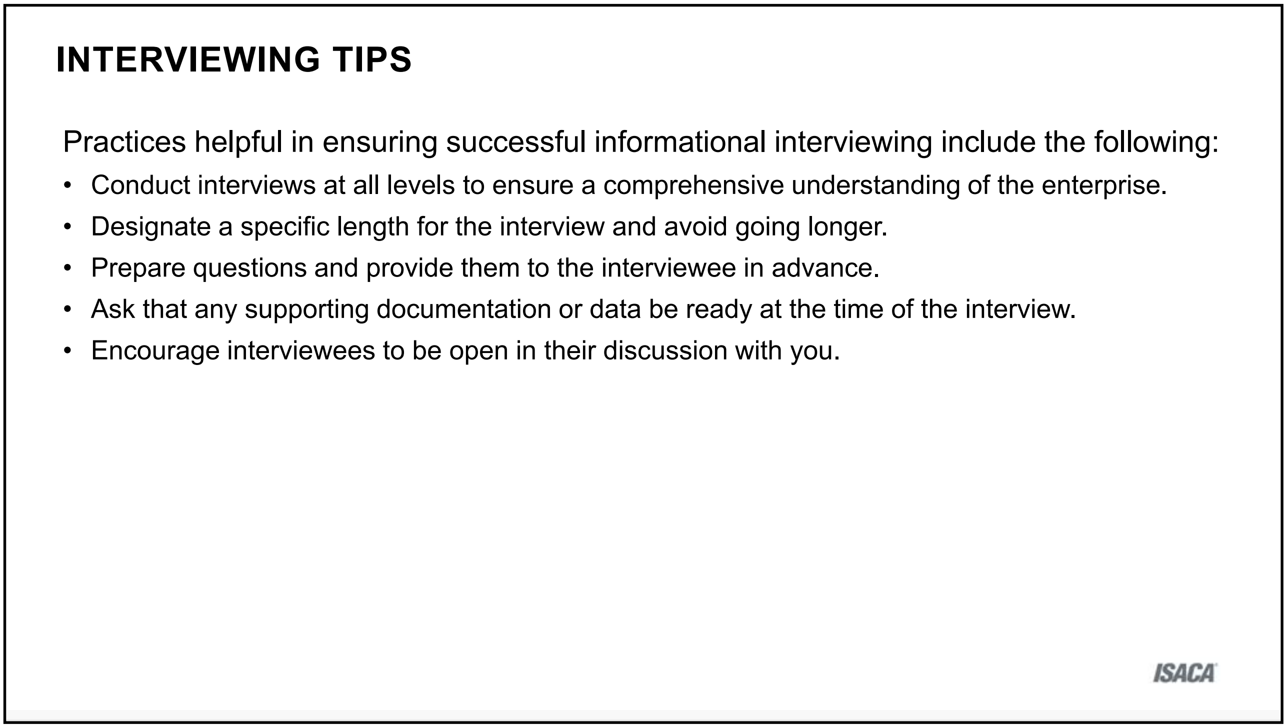


FOCUS ON: INTERVIEWS

One opportunity for information gathering that should be considered is interviews with enterprise staff.

This activity may present some challenges that the risk practitioner should be aware of, including the following:

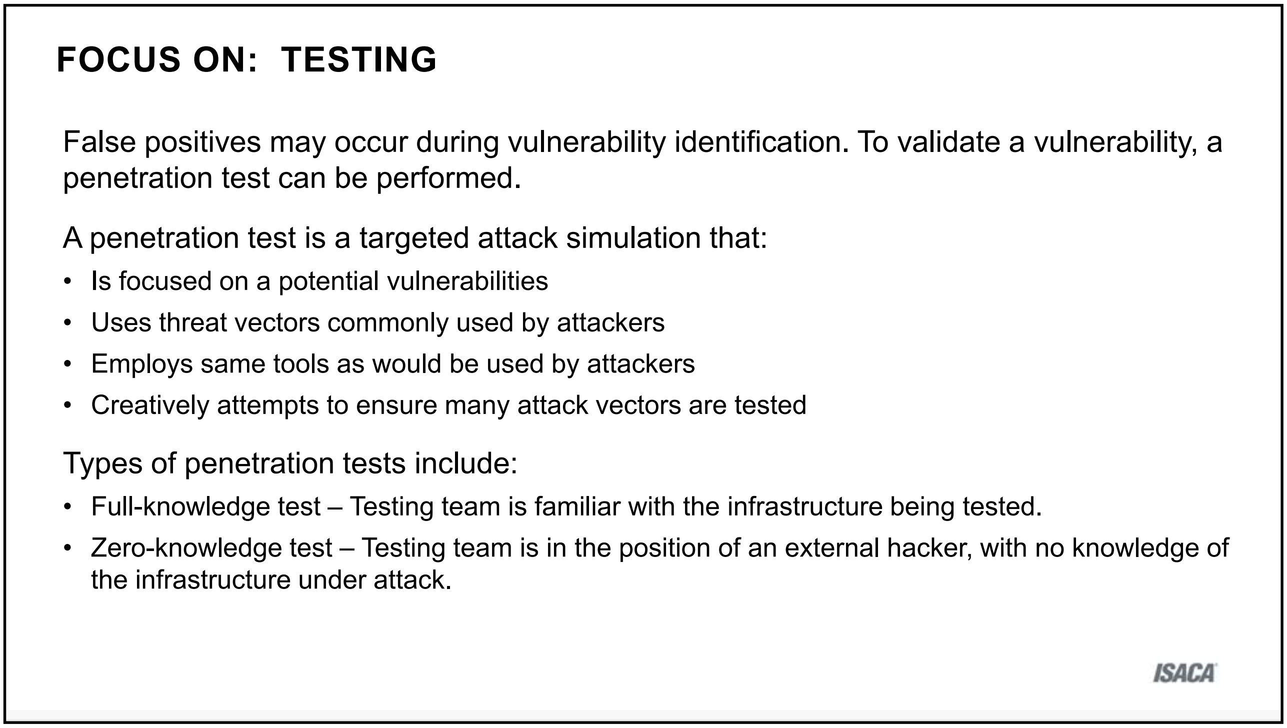
- Exaggeration: Everyone wants their department to be seen as critical and essential.
- Inaccuracies: People may not correctly understand the overall business process or dependencies between departments.



INTERVIEWING TIPS

Practices helpful in ensuring successful informational interviewing include the following:

- Conduct interviews at all levels to ensure a comprehensive understanding of the enterprise.
- Designate a specific length for the interview and avoid going longer.
- Prepare questions and provide them to the interviewee in advance.
- Ask that any supporting documentation or data be ready at the time of the interview.
- Encourage interviewees to be open in their discussion with you.



FOCUS ON: TESTING

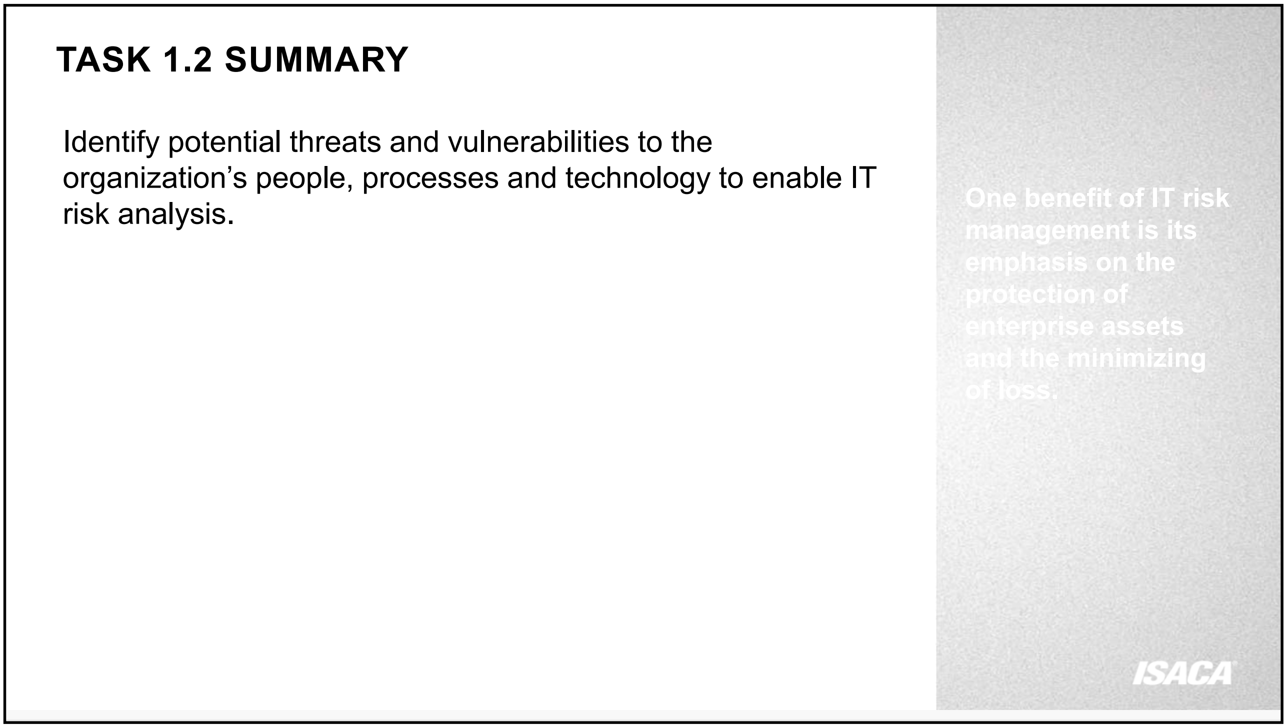
False positives may occur during vulnerability identification. To validate a vulnerability, a penetration test can be performed.

A penetration test is a targeted attack simulation that:

- Is focused on a potential vulnerabilities
- Uses threat vectors commonly used by attackers
- Employs same tools as would be used by attackers
- Creatively attempts to ensure many attack vectors are tested

Types of penetration tests include:

- Full-knowledge test – Testing team is familiar with the infrastructure being tested.
- Zero-knowledge test – Testing team is in the position of an external hacker, with no knowledge of the infrastructure under attack.



TASK 1.2 SUMMARY

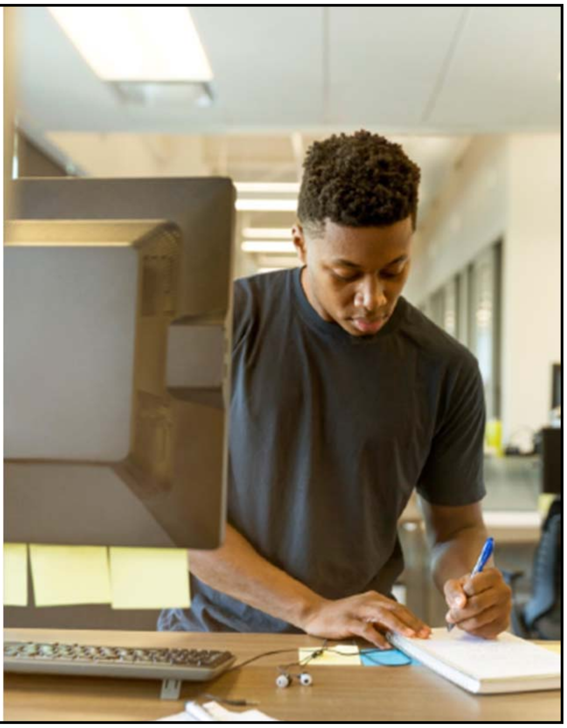
Identify potential threats and vulnerabilities to the organization’s people, processes and technology to enable IT risk analysis.

One benefit of IT risk management is its emphasis on the protection of enterprise assets and the minimizing of loss.

ISACA

TASK 1.2 ACTIVITY

Using the list you created in the previous task, add vulnerabilities. Include regulatory requirements on your list.



DISCUSSION QUESTION

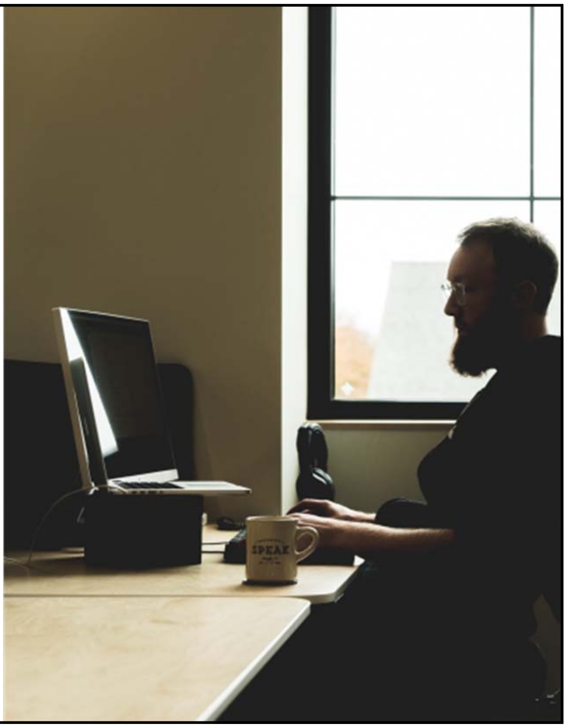
The likelihood of an attack being launched against an enterprise is MOST dependent upon:

A. The skill and motivation of the potential attacker.

B. The frequency that monitoring systems are reviewed.

C. The ability to respond quickly to any incident.

D. The effectiveness of the controls.



DISCUSSION QUESTION

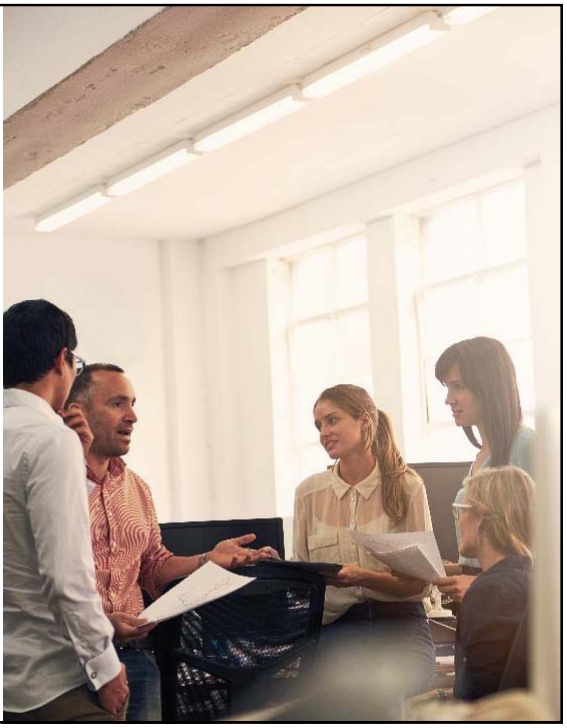
Risk scenarios should be created PRIMARILY based on which of the following?

A. Input from senior management

B. Previous security incidents

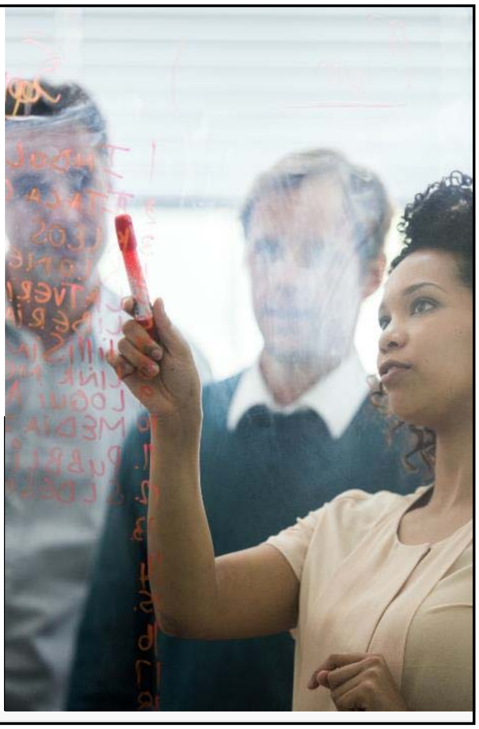
C. Threats that the enterprise faces

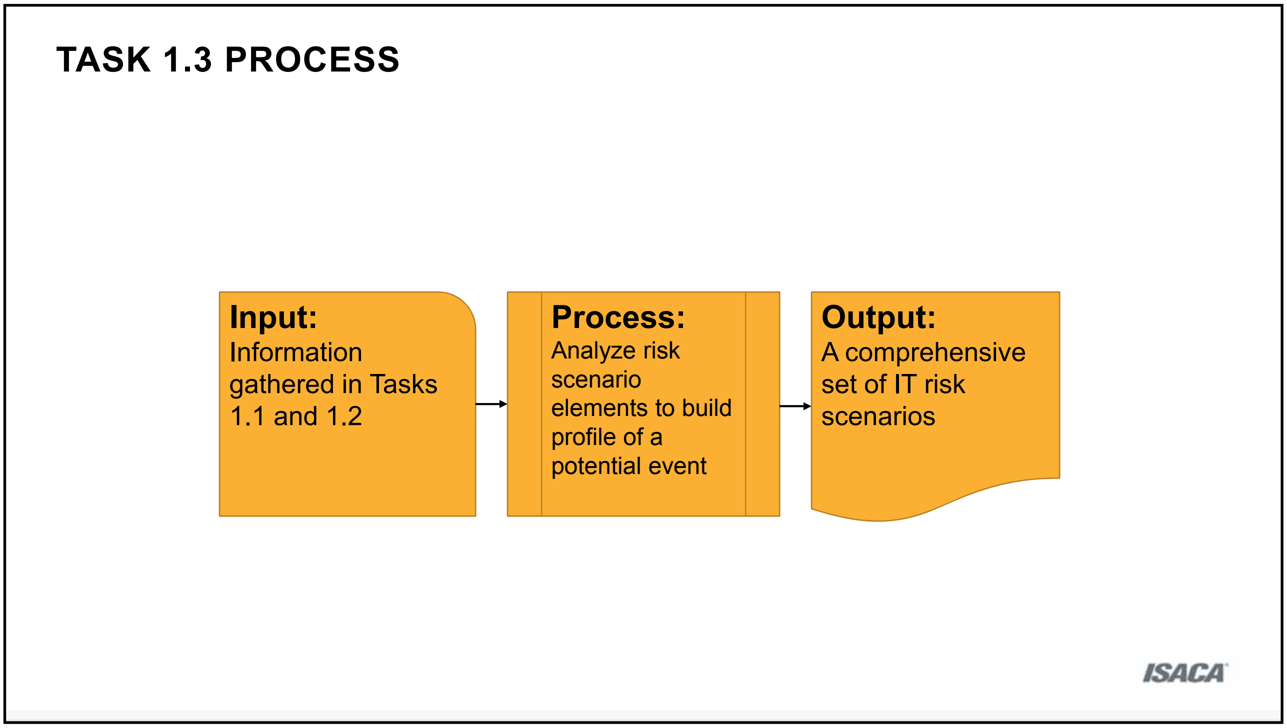
D. Results of the risk analysis



TASK 1.3

Develop a comprehensive set of IT risk scenarios based on available information to determine the potential impact to business objectives and operations.



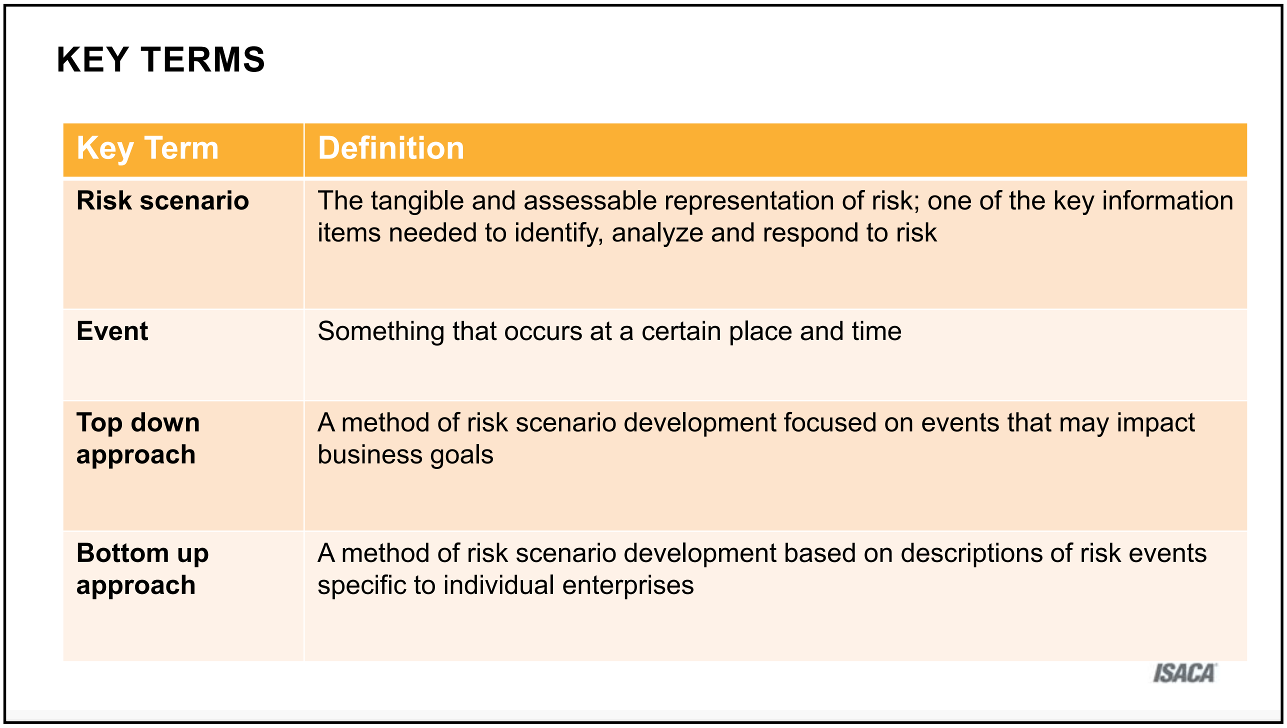


TASK 1.3 PROCESS

Input:
Information gathered in Tasks 1.1 and 1.2

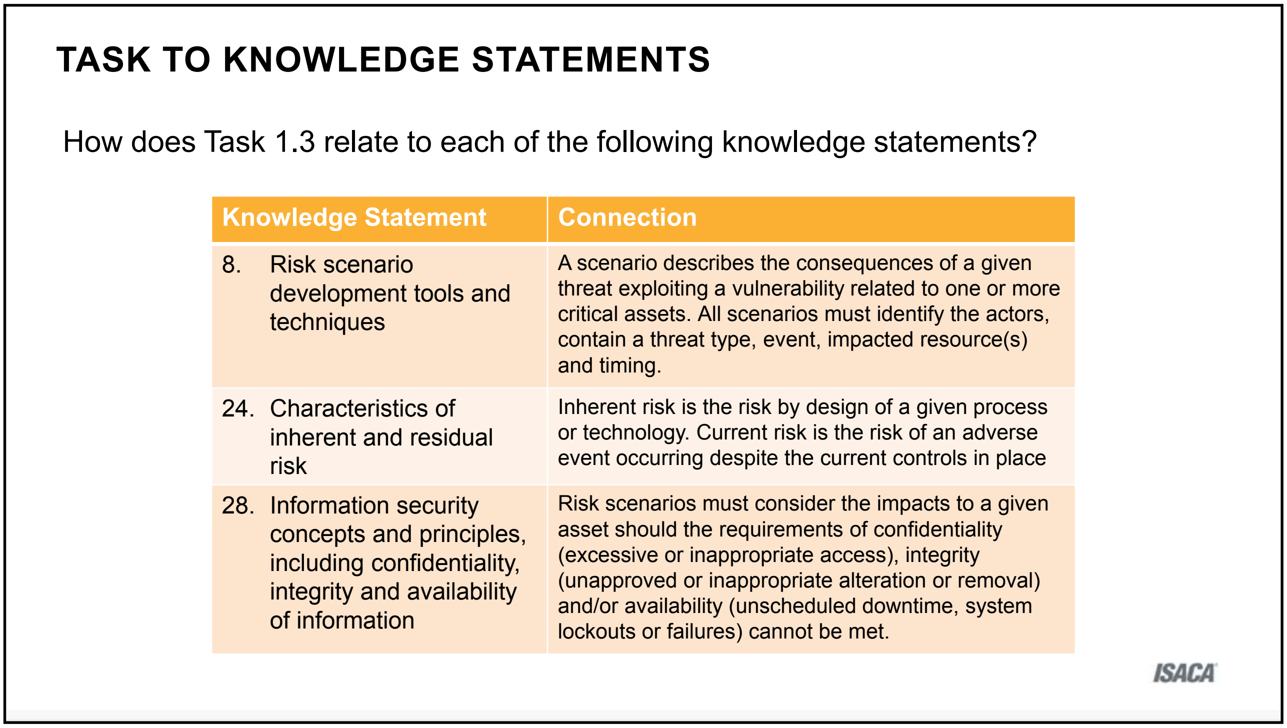
Process:
Analyze risk scenario elements to build profile of a potential event

Output:
A comprehensive set of IT risk scenarios



KEY TERMS

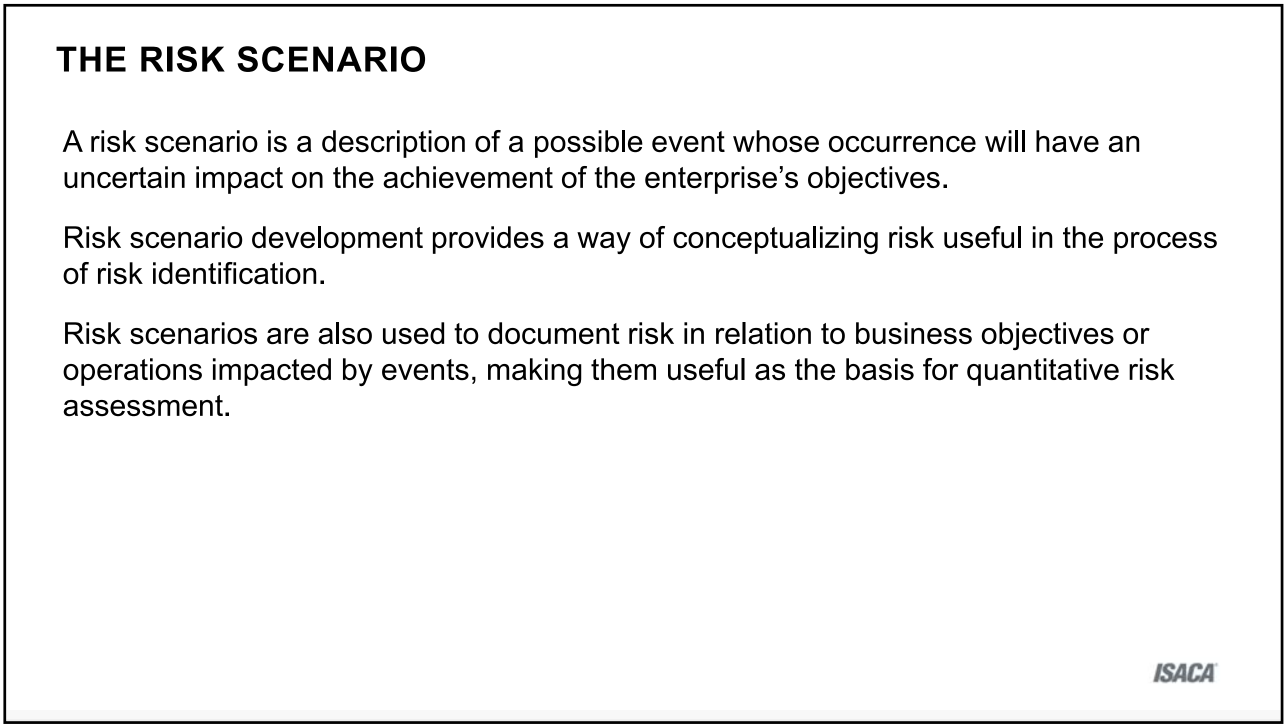
Key Term	Definition
Risk scenario	The tangible and assessable representation of risk; one of the key information items needed to identify, analyze and respond to risk
Event	Something that occurs at a certain place and time
Top down approach	A method of risk scenario development focused on events that may impact business goals
Bottom up approach	A method of risk scenario development based on descriptions of risk events specific to individual enterprises



TASK TO KNOWLEDGE STATEMENTS

How does Task 1.3 relate to each of the following knowledge statements?

Knowledge Statement	Connection
8. Risk scenario development tools and techniques	A scenario describes the consequences of a given threat exploiting a vulnerability related to one or more critical assets. All scenarios must identify the actors, contain a threat type, event, impacted resource(s) and timing.
24. Characteristics of inherent and residual risk	Inherent risk is the risk by design of a given process or technology. Current risk is the risk of an adverse event occurring despite the current controls in place
28. Information security concepts and principles, including confidentiality, integrity and availability of information	Risk scenarios must consider the impacts to a given asset should the requirements of confidentiality (excessive or inappropriate access), integrity (unapproved or inappropriate alteration or removal) and/or availability (unscheduled downtime, system lockouts or failures) cannot be met.

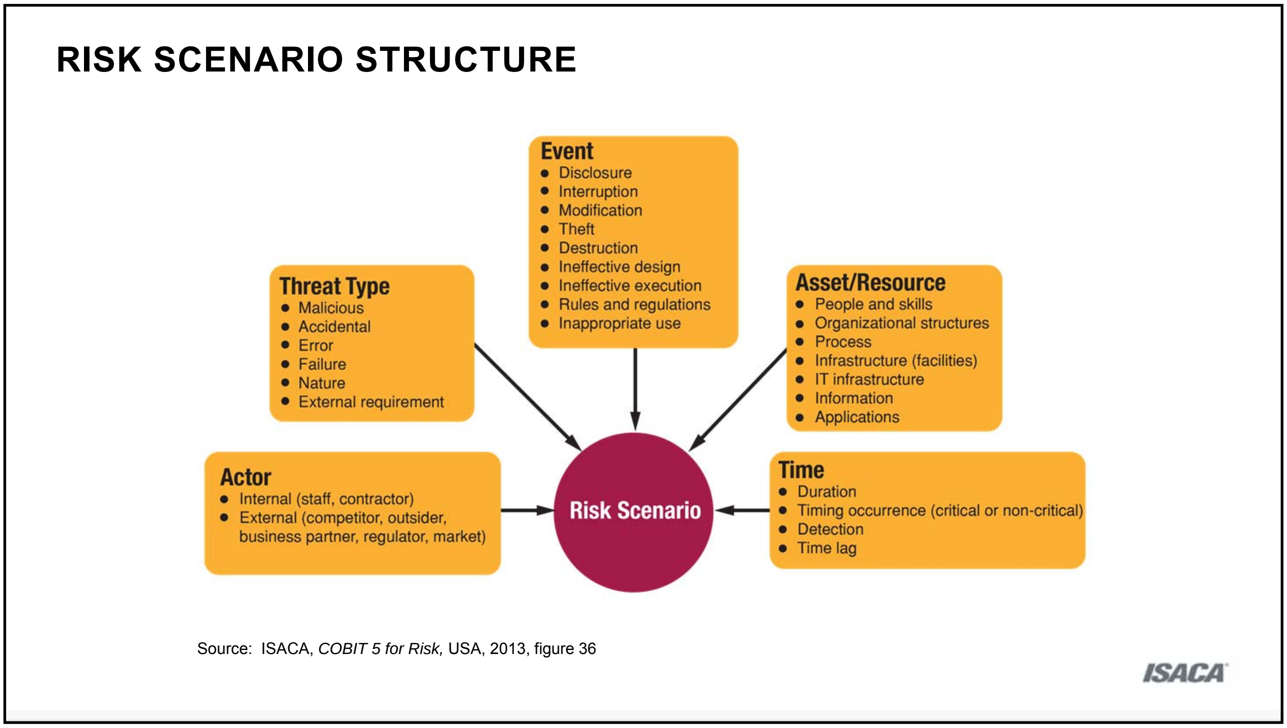


THE RISK SCENARIO

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 STRUCTURE

Event
- Disclosure
- Interruption
- Modification
- Theft
- Destruction
- Ineffective design
- Ineffective execution
- Rules and regulations
- Inappropriate use

Threat Type
- Malicious
- Accidental
- Error
- Failure
- Nature
- External requirement

Asset/Resource
- People and skills
- Organizational structures
- Process
- Infrastructure (facilities)
- IT infrastructure
- Information
- Applications

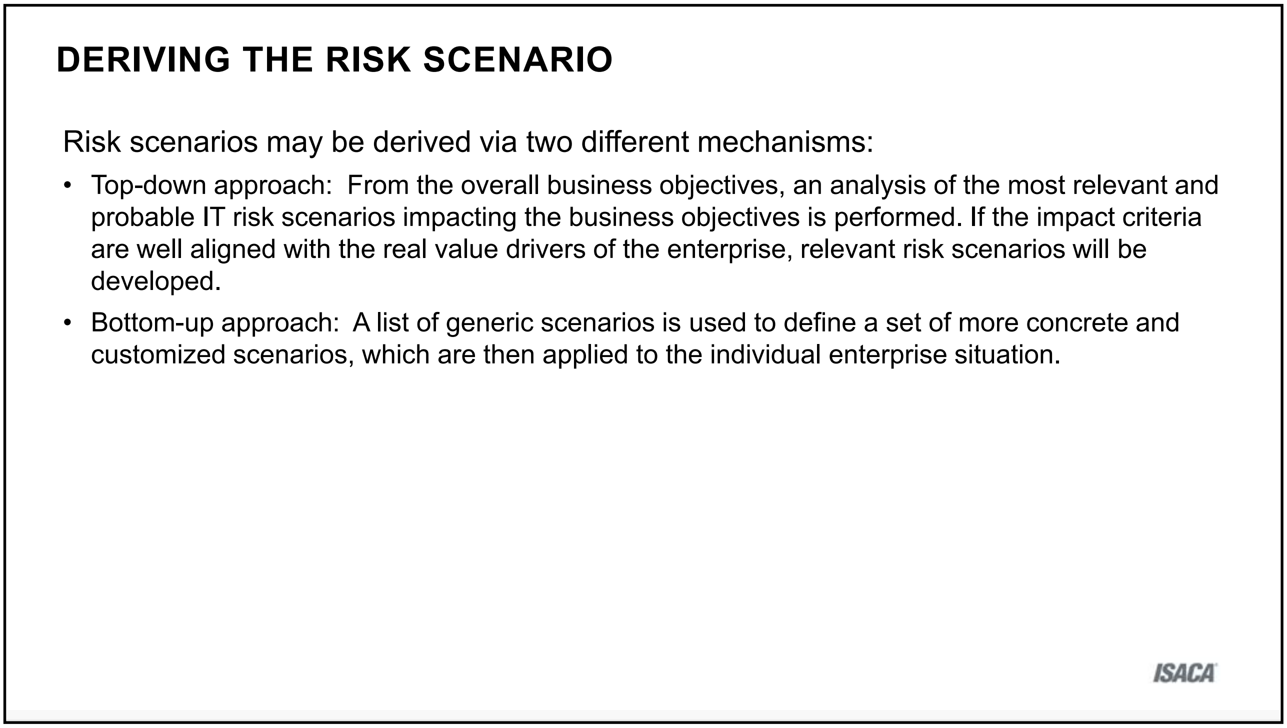
Actor
- Internal (staff, contractor)
- External (competitor, outsider, business partner, regulator, market)

Risk Scenario

Time
- Duration
- Timing occurrence (critical or non-critical)
- Detection
- Time lag

Source: ISACA, *COBIT 5 for Risk,* USA, 2013, figure 36

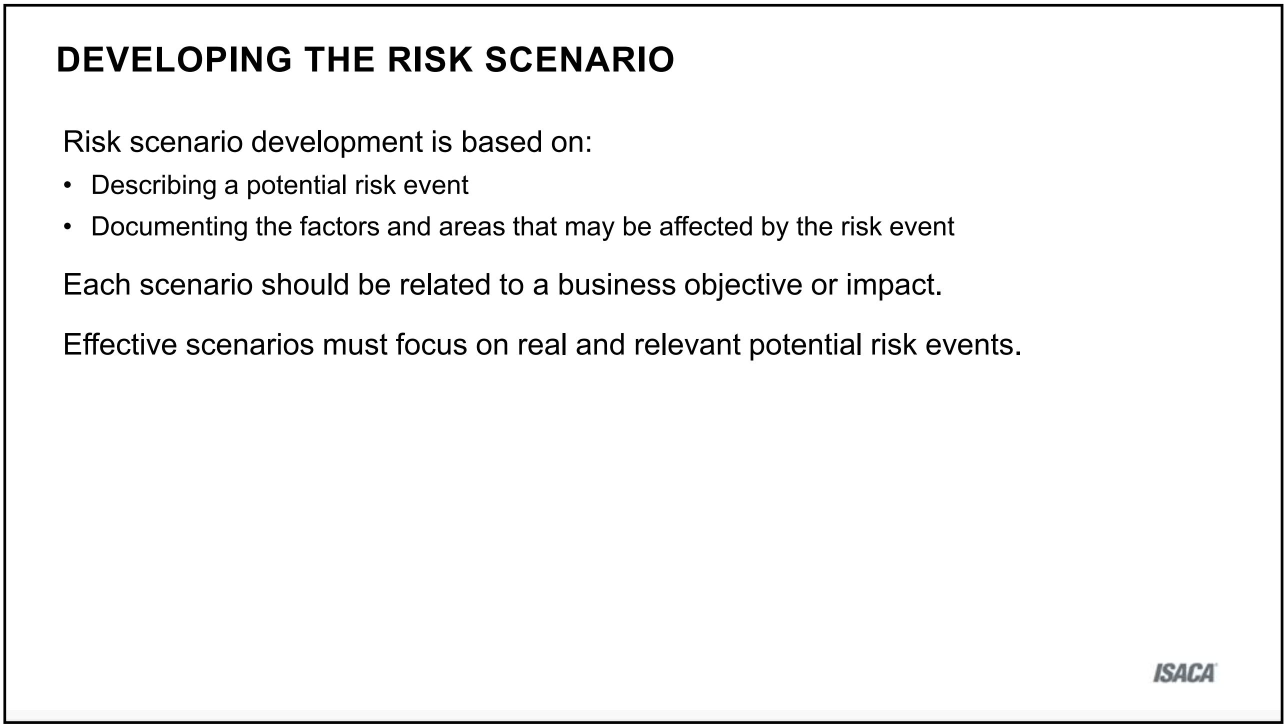
ISACA



DERIVING THE RISK SCENARIO

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.



DEVELOPING THE RISK SCENARIO

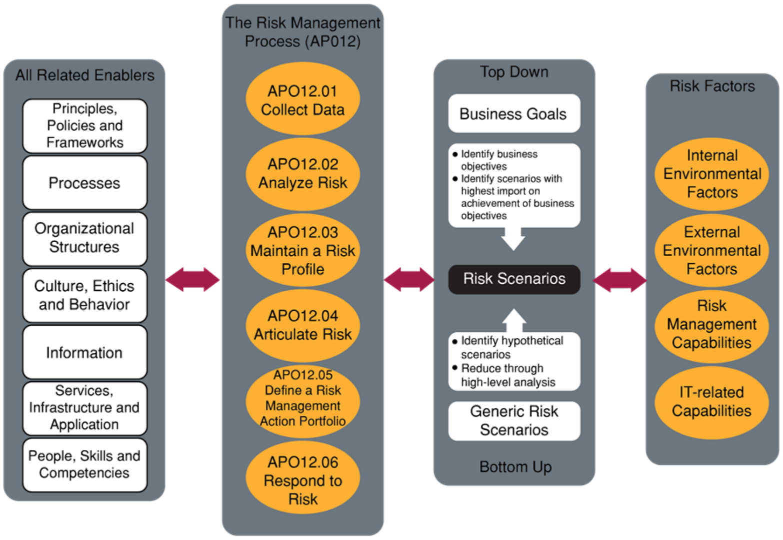
Risk scenario development is based on:

- 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.

RISK SCENARIO OVERVIEW



All Related Enablers

- Principles, Policies and Frameworks
- Processes
- Organizational Structures
- Culture, Ethics and Behavior
- Information
- Services, Infrastructure and Application
- People, Skills and Competencies

The Risk Management Process (AP012)

- APO12.01 Collect Data
- APO12.02 Analyze Risk
- APO12.03 Maintain a Risk Profile
- APO12.04 Articulate Risk
- APO12.05 Define a Risk Management Action Portfolio
- APO12.06 Respond to Risk

Top Down

Business Goals

- Identify business objectives
- Identify scenarios with highest import on achievement of business objectives

Risk Scenarios

- Identify hypothetical scenarios
- Reduce through high-level analysis

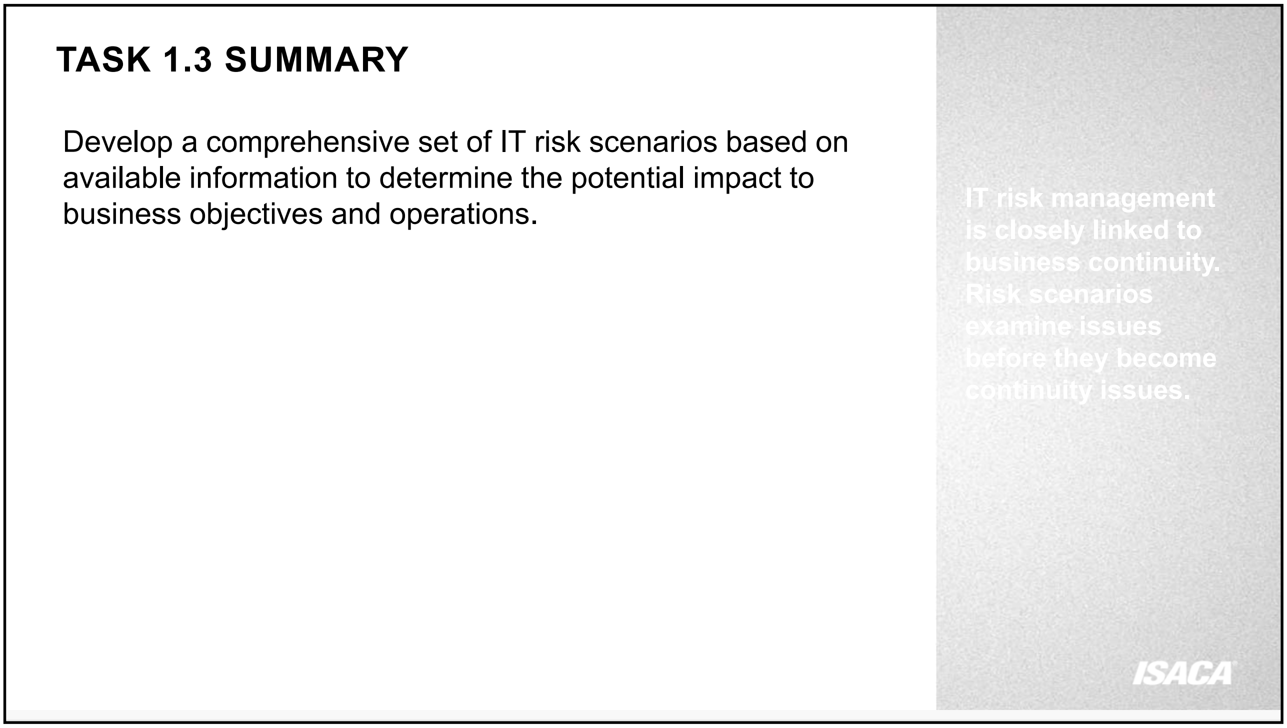
Generic Risk Scenarios

Bottom Up

Risk Factors

- Internal Environmental Factors
- External Environmental Factors
- Risk Management Capabilities
- IT-related Capabilities

Source: ISACA, *COBIT 5 for Risk,* USA, 2013, figure 34



TASK 1.3 SUMMARY

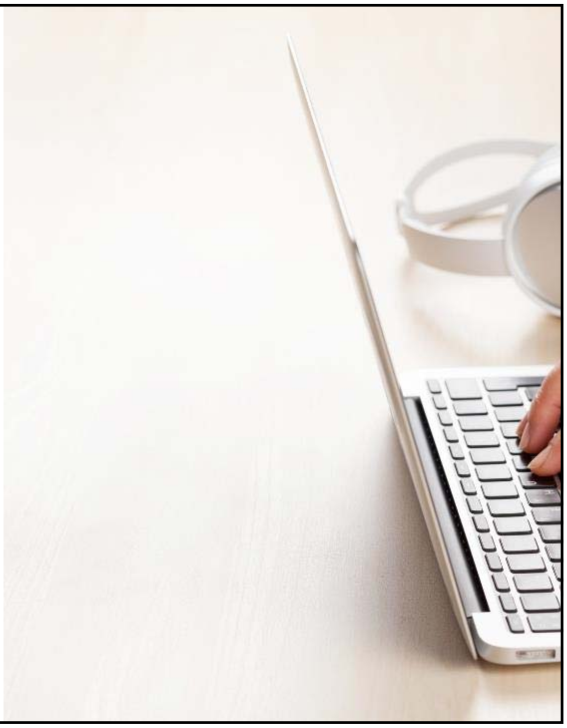
Develop a comprehensive set of IT risk scenarios based on available information to determine the potential impact to business objectives and operations.

IT risk management is closely linked to business continuity. Risk scenarios examine issues before they become continuity issues.

ISACA

TASK 1.3 ACTIVITY

Build a risk scenario associated with the process you developed in the previous two tasks.



DISCUSSION QUESTION

When developing IT-related risk scenarios with a top-down approach, it is MOST important to identify the:

A. Information system environment
B. Business objectives
C. Hypothetical risk scenarios
D. External risk scenarios

DISCUSSION QUESTION

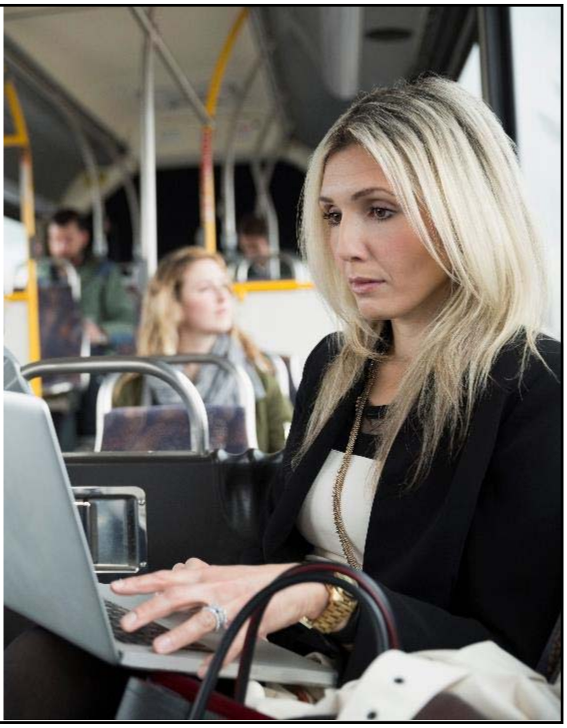
Risk scenarios enable the risk assessment process because they:

A. cover a wide range of potential risk.

B. minimize the need for quantitative risk analysis techniques.

C. segregate IT risk from business risk for easier risk analysis.

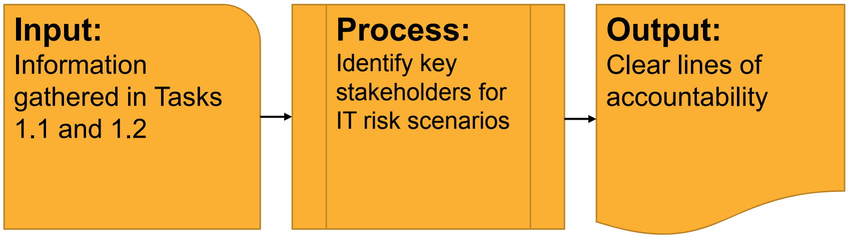
D. help estimate the frequency and impact of risk.



TASK 1.4

Identify key stakeholders for IT risk scenarios to help establish accountability.

FOCUS ON TASK 1.4

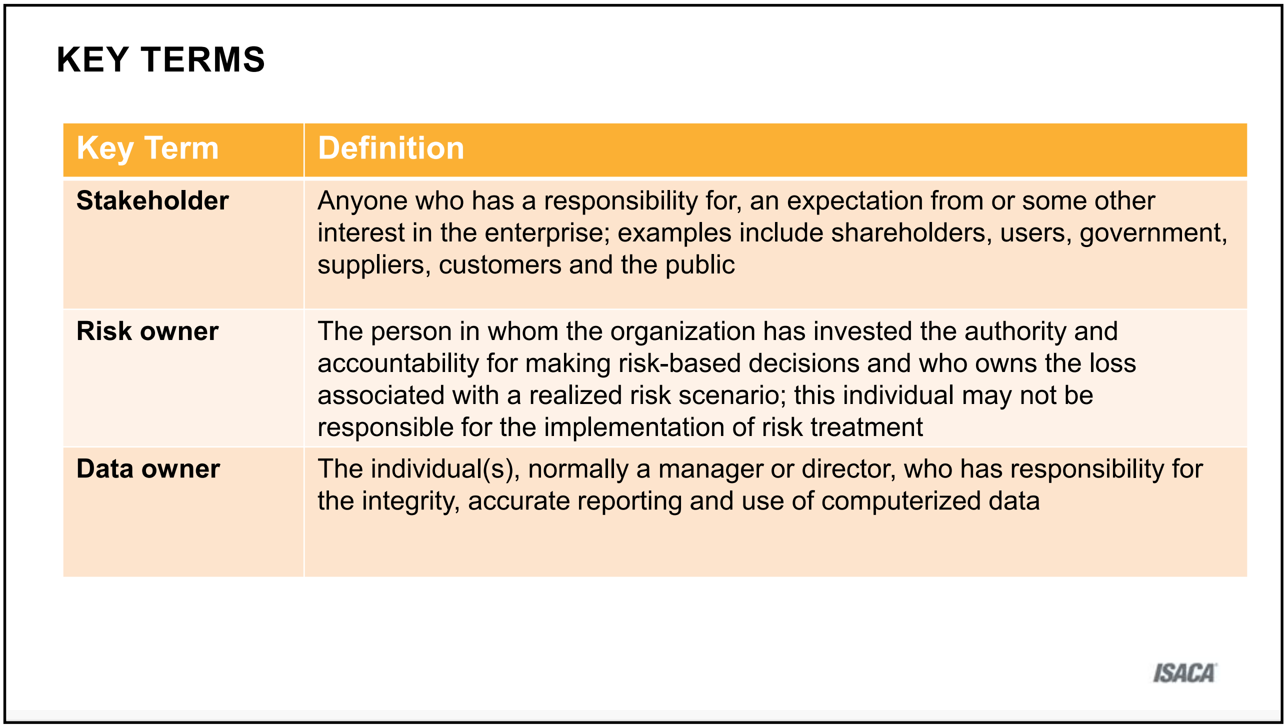


Input: Information gathered in Tasks 1.1 and 1.2

Process: Identify key stakeholders for IT risk scenarios

Output: Clear lines of accountability

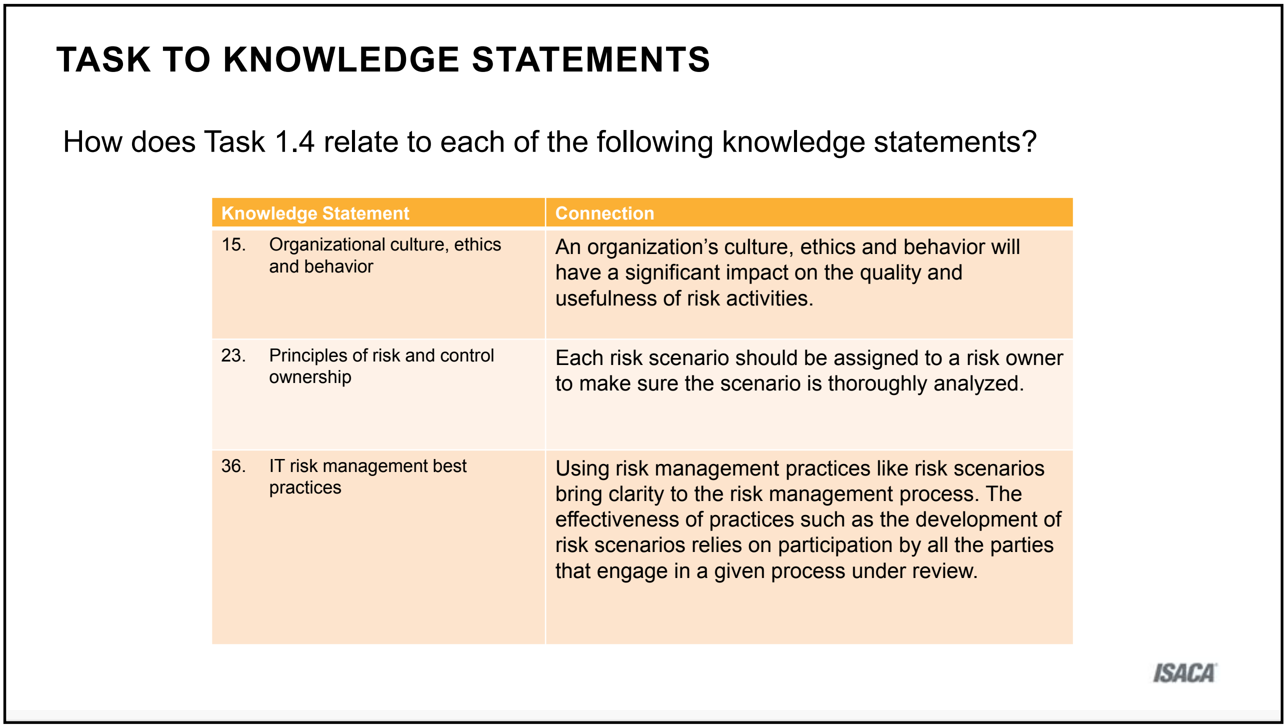
ISACA



KEY TERMS

Key Term	Definition
Stakeholder	Anyone who has a responsibility for, an expectation from or some other interest in the enterprise; examples include shareholders, users, government, suppliers, customers and the public
Risk owner	The person in whom the organization has invested the authority and accountability for making risk-based decisions and who owns the loss associated with a realized risk scenario; this individual may not be responsible for the implementation of risk treatment
Data owner	The individual(s), normally a manager or director, who has responsibility for the integrity, accurate reporting and use of computerized data

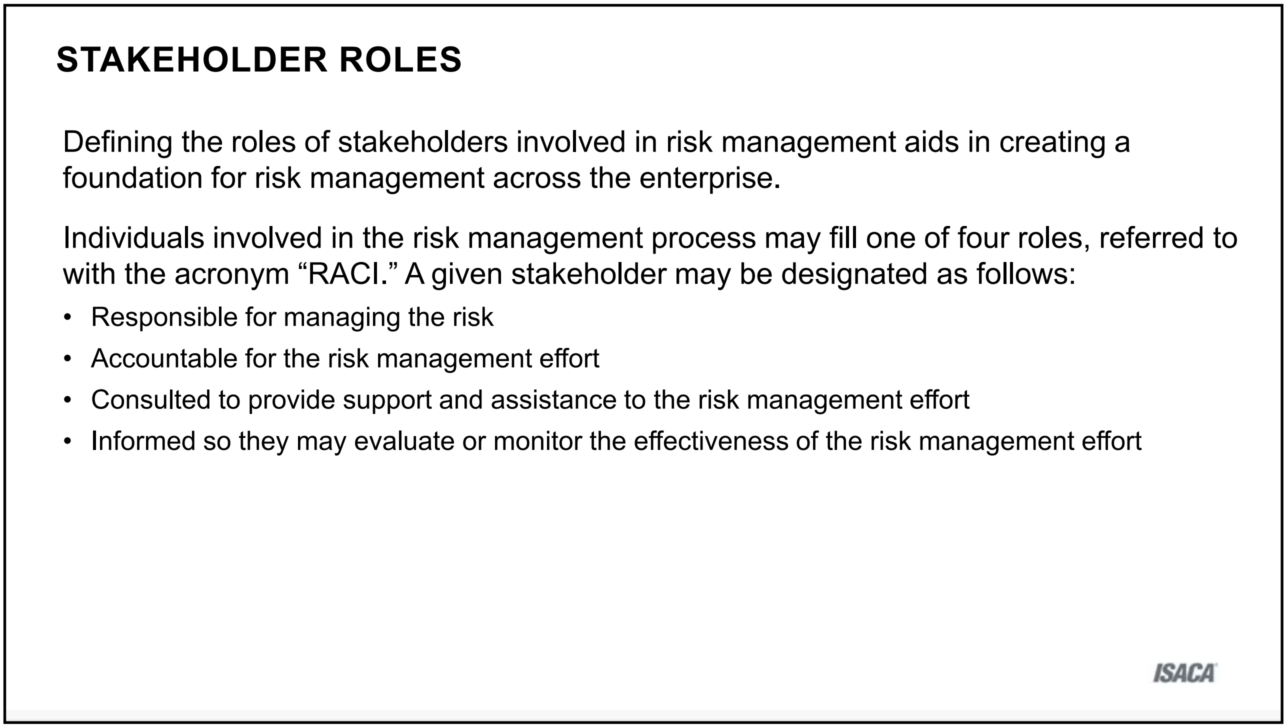
ISACA



TASK TO KNOWLEDGE STATEMENTS

How does Task 1.4 relate to each of the following knowledge statements?

Knowledge Statement	Connection
15. Organizational culture, ethics and behavior	An organization’s culture, ethics and behavior will have a significant impact on the quality and usefulness of risk activities.
23. Principles of risk and control ownership	Each risk scenario should be assigned to a risk owner to make sure the scenario is thoroughly analyzed.
36. IT risk management best practices	Using risk management practices like risk scenarios bring clarity to the risk management process. The effectiveness of practices such as the development of risk scenarios relies on participation by all the parties that engage in a given process under review.

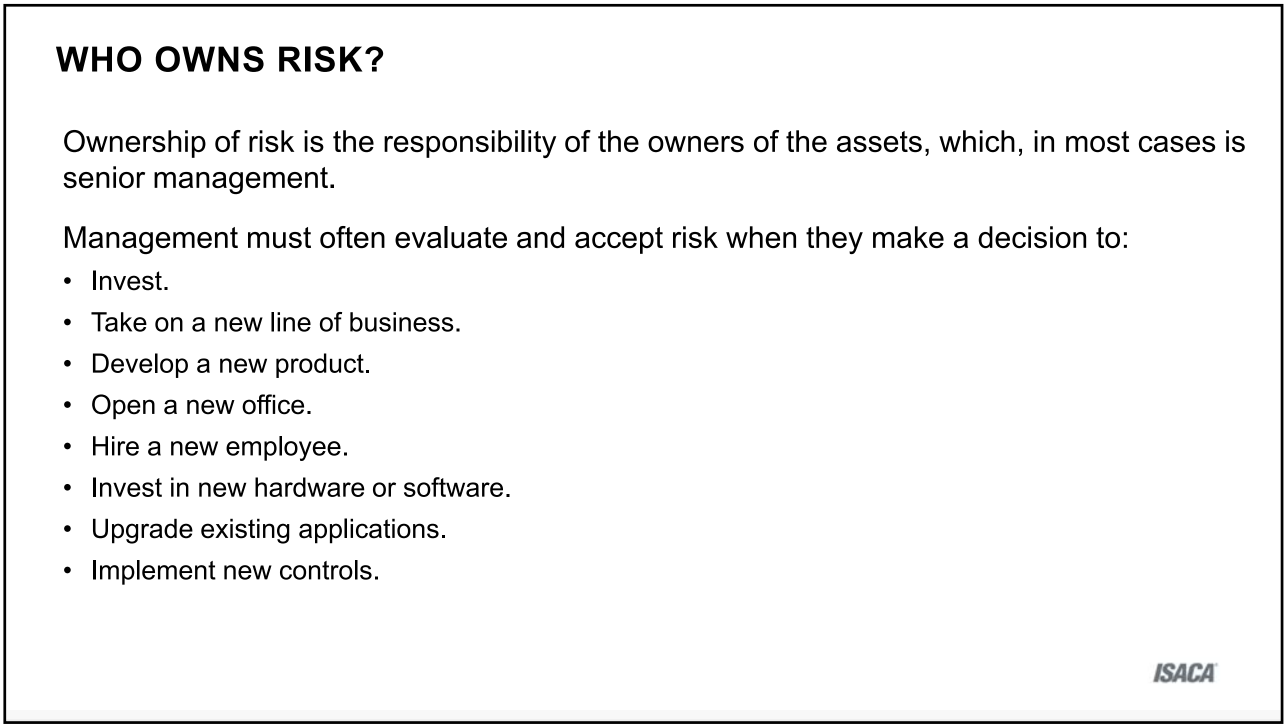


STAKEHOLDER ROLES

Defining the roles of stakeholders involved in risk management aids in creating a foundation for risk management across the enterprise.

Individuals involved in the risk management process may fill one of four roles, referred to with the acronym “RACI.” A given stakeholder may be designated as follows:

- Responsible for managing the risk
- Accountable for the risk management effort
- Consulted to provide support and assistance to the risk management effort
- Informed so they may evaluate or monitor the effectiveness of the risk management effort

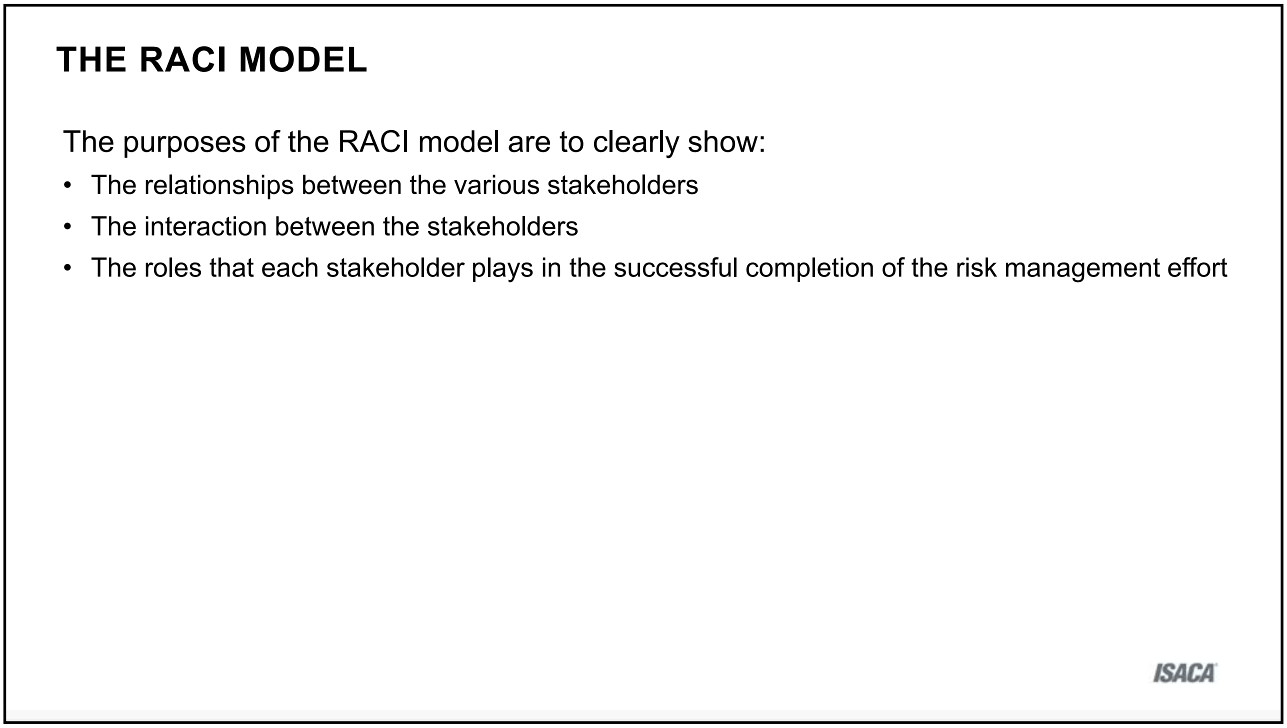


WHO OWNS RISK?

Ownership of risk is the responsibility of the owners of the assets, which, in most cases is senior management.

Management must often evaluate and accept risk when they make a decision to:

- Invest.
- Take on a new line of business.
- Develop a new product.
- Open a new office.
- Hire a new employee.
- Invest in new hardware or software.
- Upgrade existing applications.
- Implement new controls.

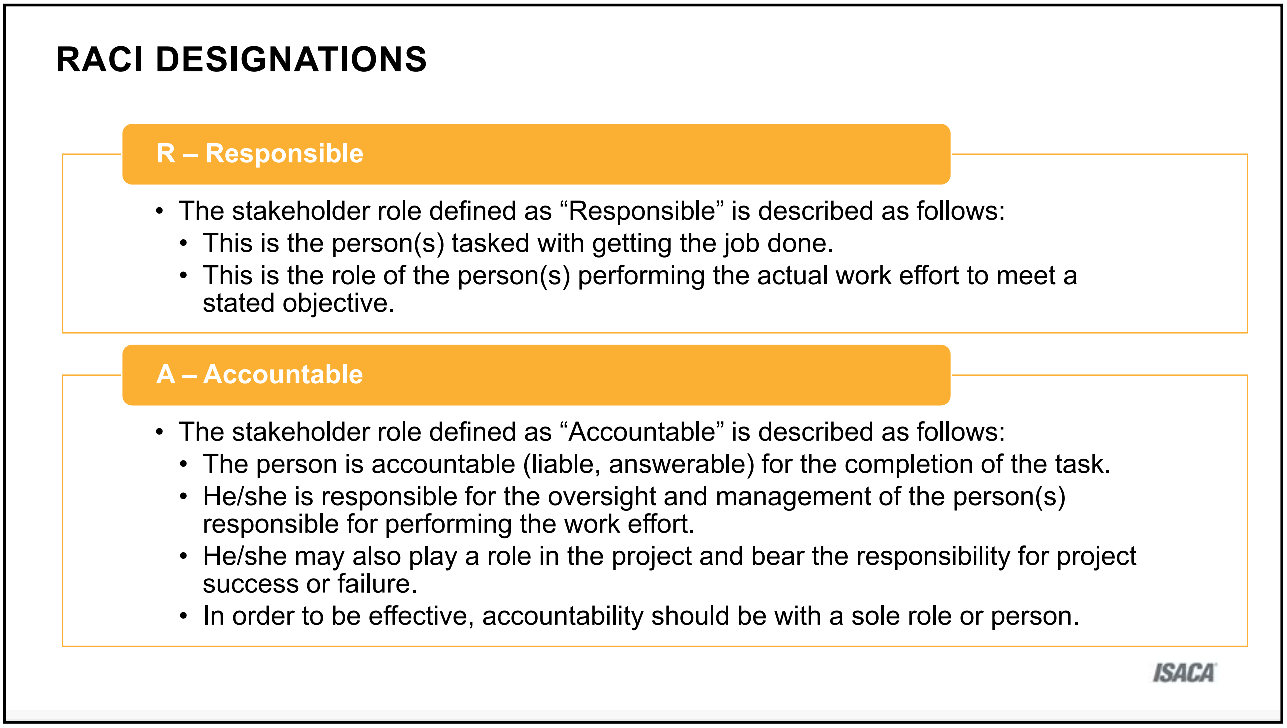


THE RACI MODEL

The purposes of the RACI model are to clearly show:

- The relationships between the various stakeholders
- The interaction between the stakeholders
- The roles that each stakeholder plays in the successful completion of the risk management effort

ISACA



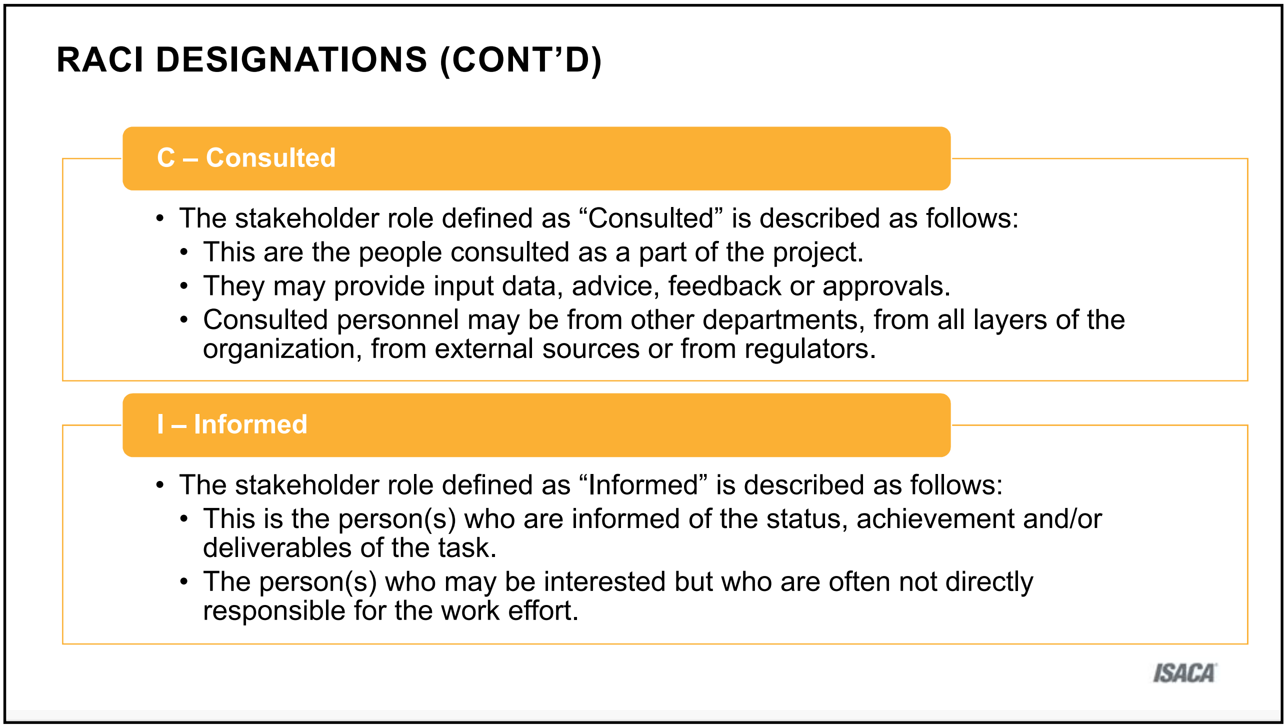
RACI DESIGNATIONS

R – Responsible

- The stakeholder role defined as “Responsible” is described as follows:
  - This is the person(s) tasked with getting the job done.
  - This is the role of the person(s) performing the actual work effort to meet a stated objective.

A – Accountable

- The stakeholder role defined as “Accountable” is described as follows:
  - The person is accountable (liable, answerable) for the completion of the task.
  - He/she is responsible for the oversight and management of the person(s) responsible for performing the work effort.
  - He/she may also play a role in the project and bear the responsibility for project success or failure.
  - In order to be effective, accountability should be with a sole role or person.



RACI DESIGNATIONS (CONT’D)

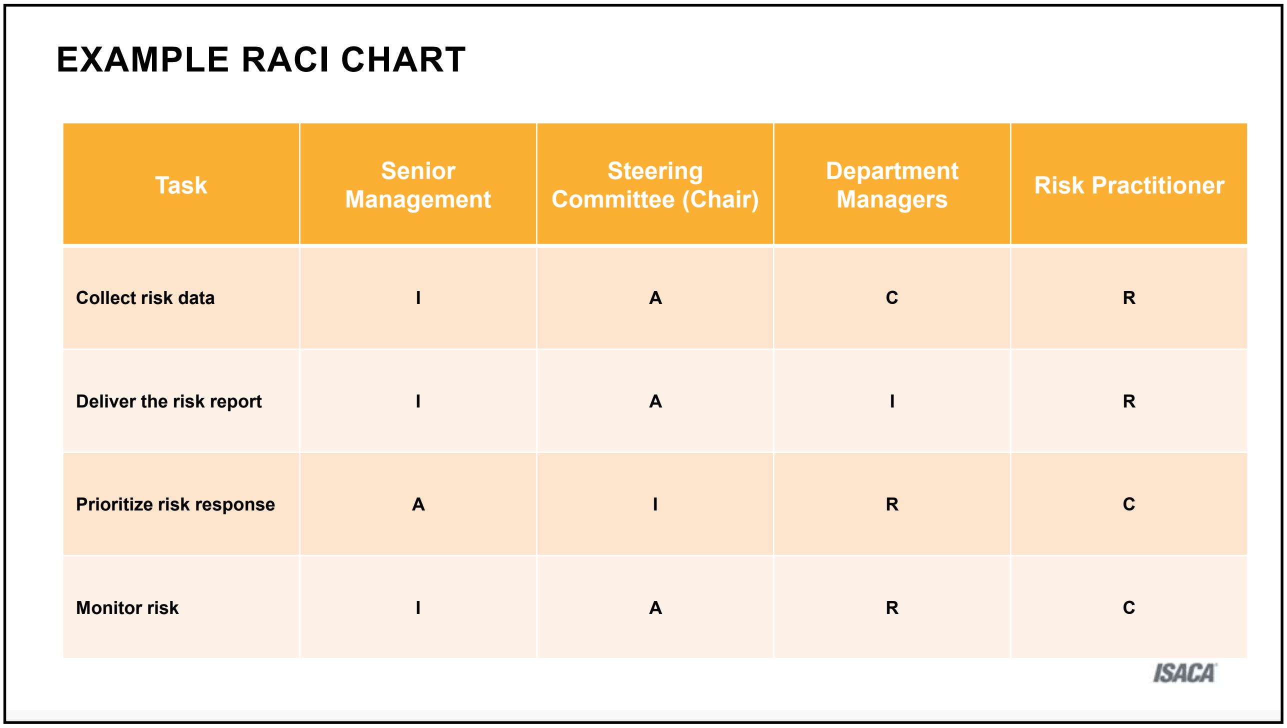
C – Consulted

- The stakeholder role defined as “Consulted” is described as follows:
  - This are the people consulted as a part of the project.
  - They may provide input data, advice, feedback or approvals.
  - Consulted personnel may be from other departments, from all layers of the organization, from external sources or from regulators.

I – Informed

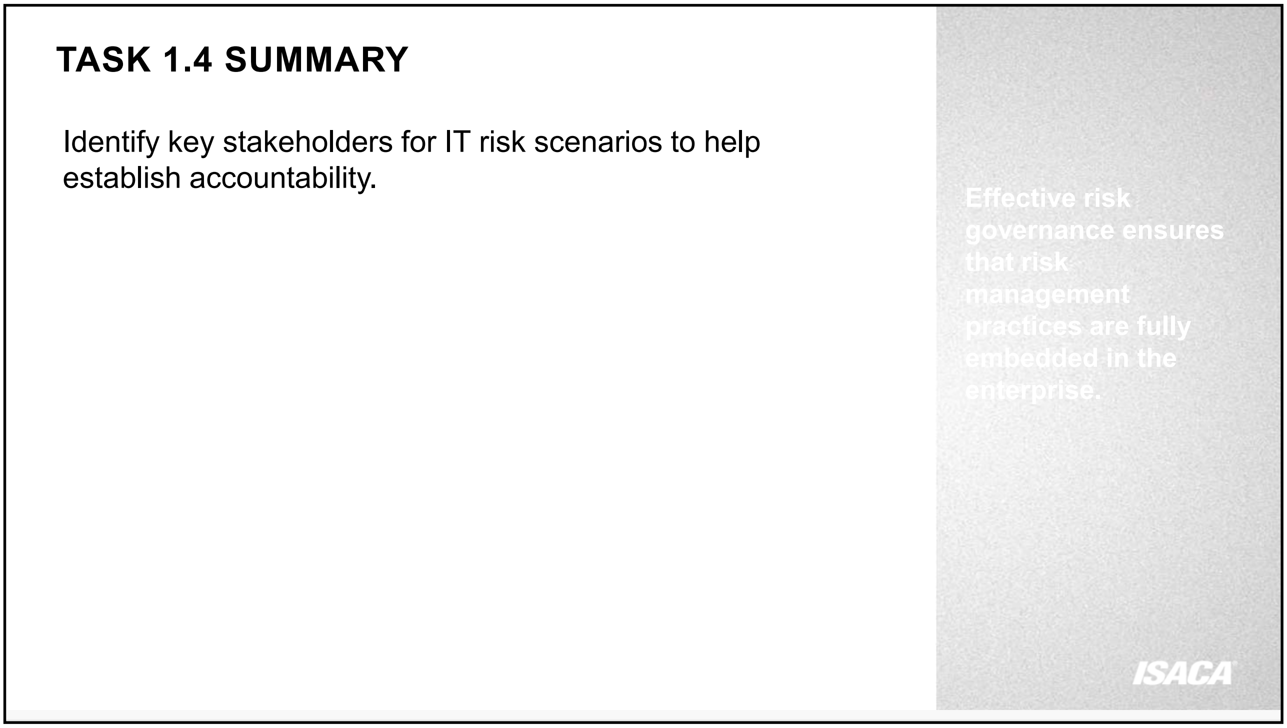
- The stakeholder role defined as “Informed” is described as follows:
  - This is the person(s) who are informed of the status, achievement and/or deliverables of the task.
  - The person(s) who may be interested but who are often not directly responsible for the work effort.

ISACA



EXAMPLE RACI CHART

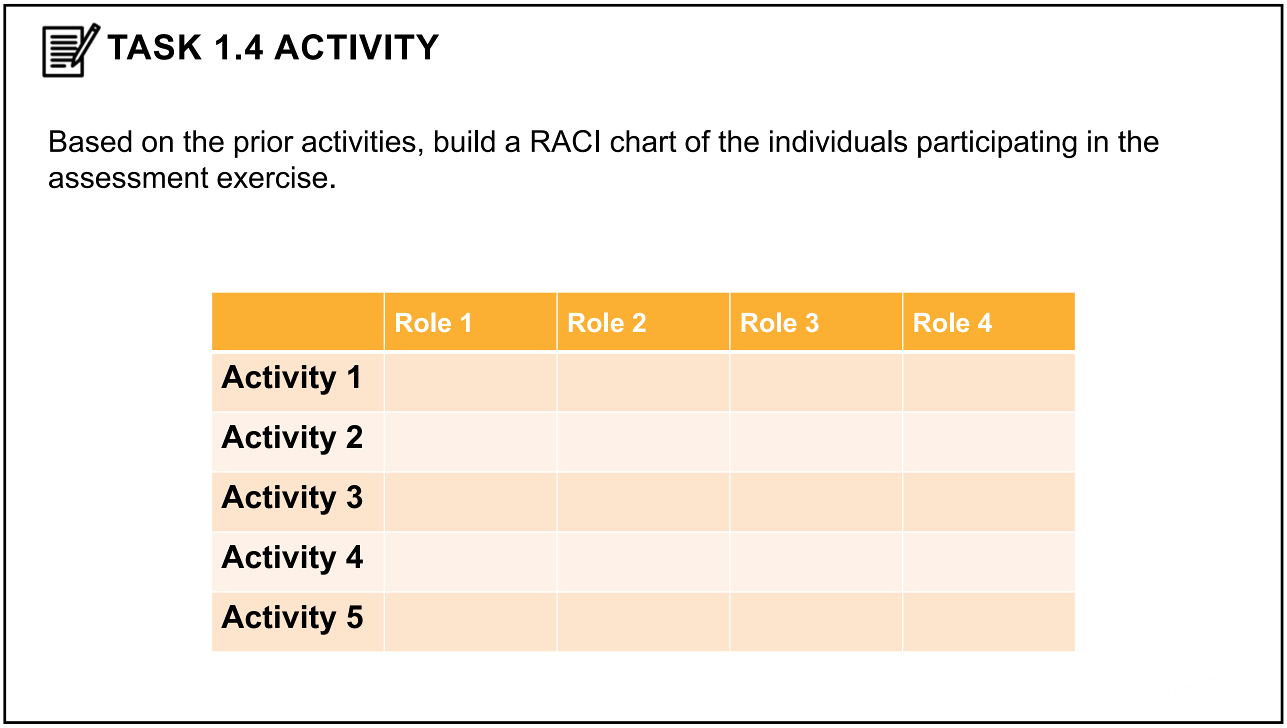
Task	Senior Management	Steering Committee (Chair)	Department Managers	Risk Practitioner
Collect risk data	I	A	C	R
Deliver the risk report	I	A	I	R
Prioritize risk response	A	I	R	C
Monitor risk	I	A	R	C



TASK 1.4 SUMMARY

Identify key stakeholders for IT risk scenarios to help establish accountability.

Effective risk governance ensures that risk management practices are fully embedded in the enterprise.



TASK 1.4 ACTIVITY

Based on the prior activities, build a RACI chart of the individuals participating in the assessment exercise.

	Role 1	Role 2	Role 3	Role 4
Activity 1				
Activity 2				
Activity 3				
Activity 4				
Activity 5				

DISCUSSION QUESTION

Which of the following activities provides the BEST basis for establishing risk ownership?

A. Documenting interdependencies between departments

B. Mapping identified risk to a specific business process

C. Referring to available RACI charts

D. Distributing risk equally among all asset owners

DISCUSSION QUESTION

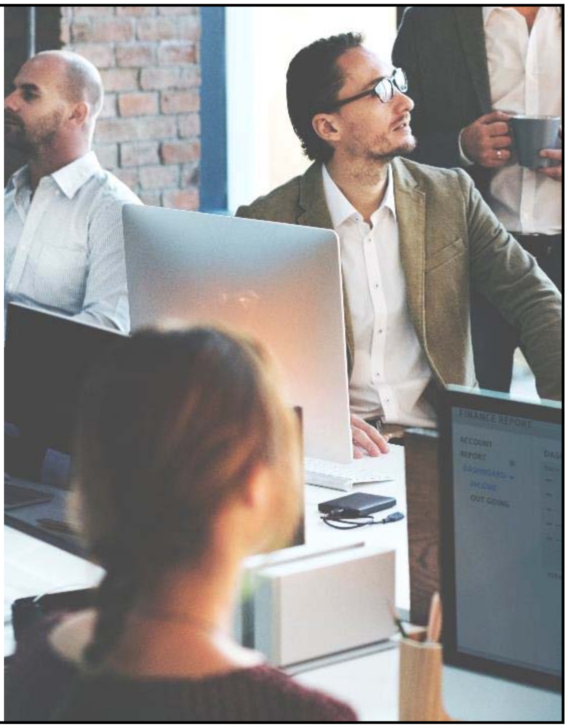
Which of the following is MOST important for effective risk management?

A. Assignment of risk owners to identified risk

B. Ensuring compliance with regulatory requirements

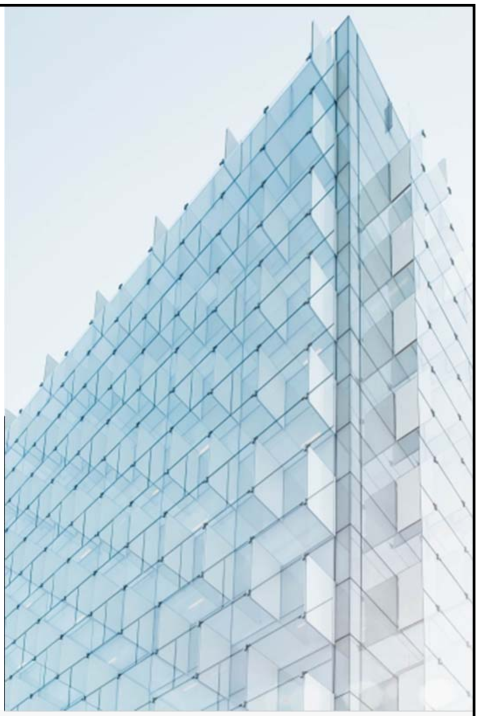
C. Integration of risk management into operational processes

D. Implementation of a risk avoidance strategy

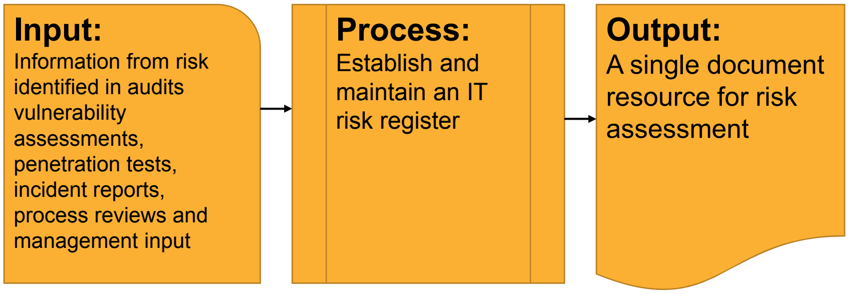


TASK 1.5

Establish an IT risk register to help ensure that identified IT risk scenarios are accounted for and incorporated into the enterprisewide risk profile.



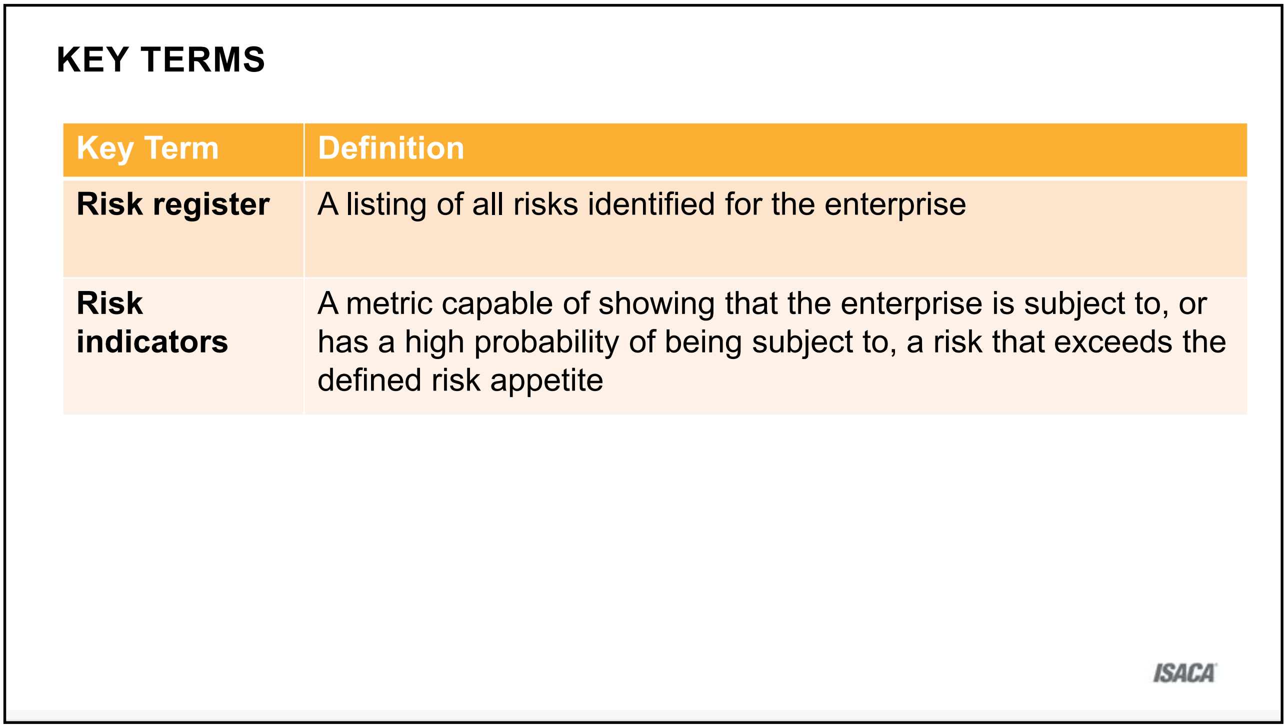
FOCUS ON TASK 1.5



Input:
Information from risk identified in audits vulnerability assessments, penetration tests, incident reports, process reviews and management input

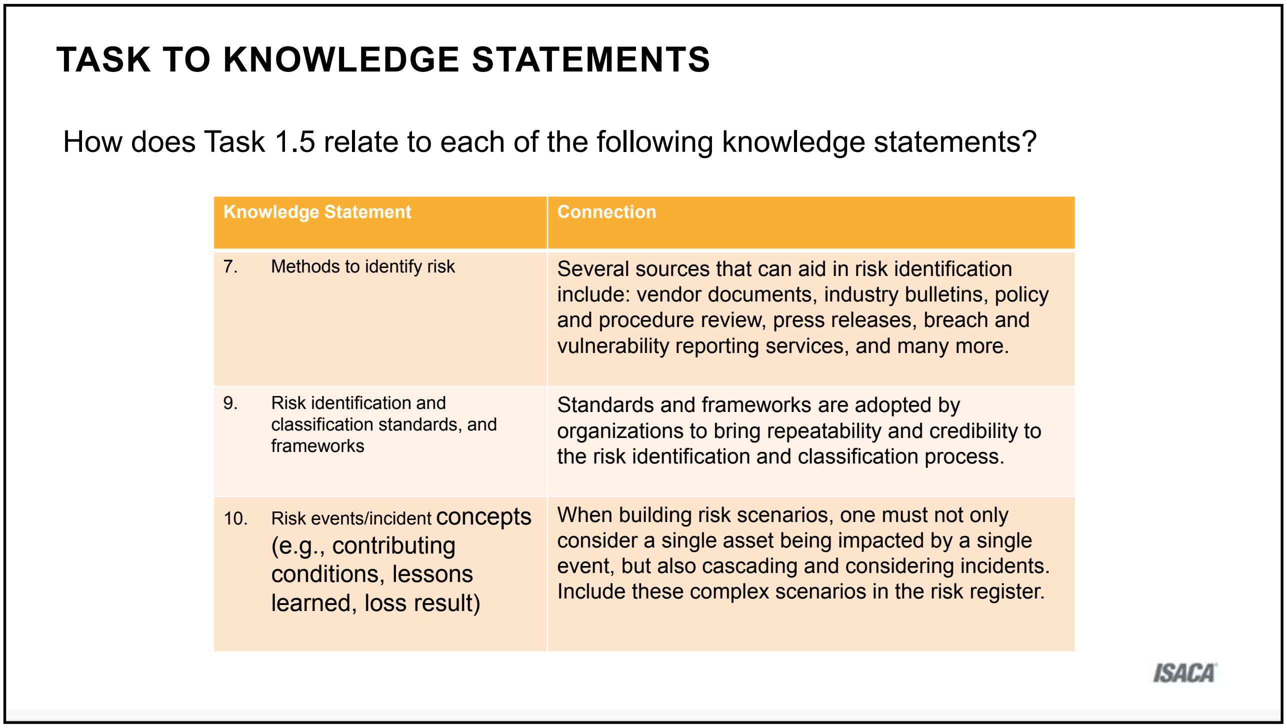
Process:
Establish and maintain an IT risk register

Output:
A single document resource for risk assessment



KEY TERMS

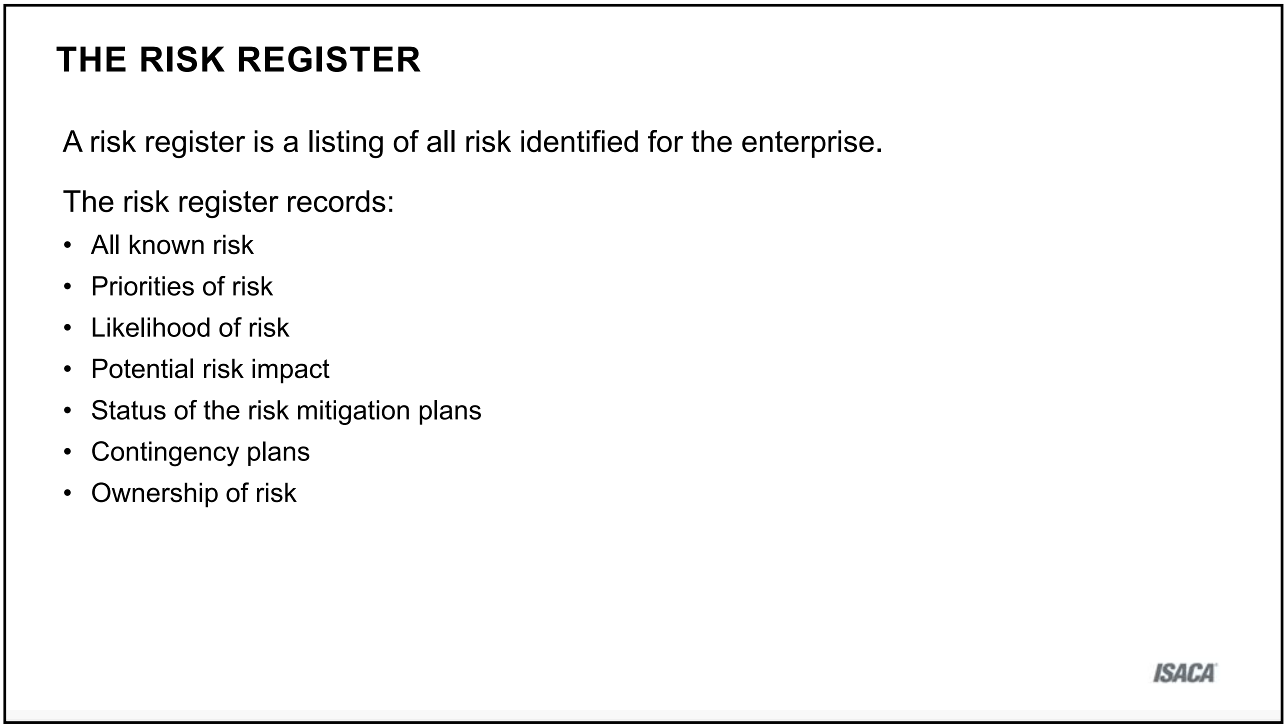
Key Term	Definition
Risk register	A listing of all risks identified for the enterprise
Risk indicators	A metric capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite



TASK TO KNOWLEDGE STATEMENTS

How does Task 1.5 relate to each of the following knowledge statements?

Knowledge Statement	Connection
7. Methods to identify risk	Several sources that can aid in risk identification include: vendor documents, industry bulletins, policy and procedure review, press releases, breach and vulnerability reporting services, and many more.
9. Risk identification and classification standards, and frameworks	Standards and frameworks are adopted by organizations to bring repeatability and credibility to the risk identification and classification process.
10. Risk events/incident concepts (e.g., contributing conditions, lessons learned, loss result)	When building risk scenarios, one must not only consider a single asset being impacted by a single event, but also cascading and considering incidents. Include these complex scenarios in the risk register.



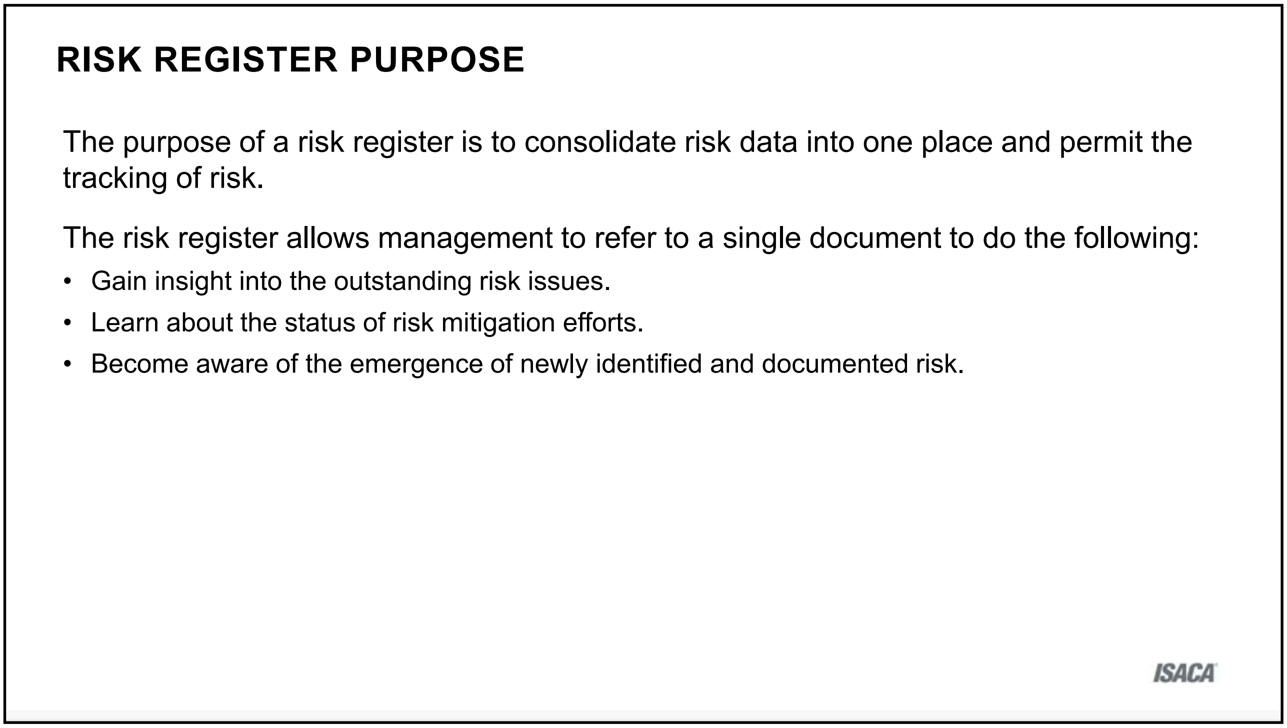
THE RISK REGISTER

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

ISACA

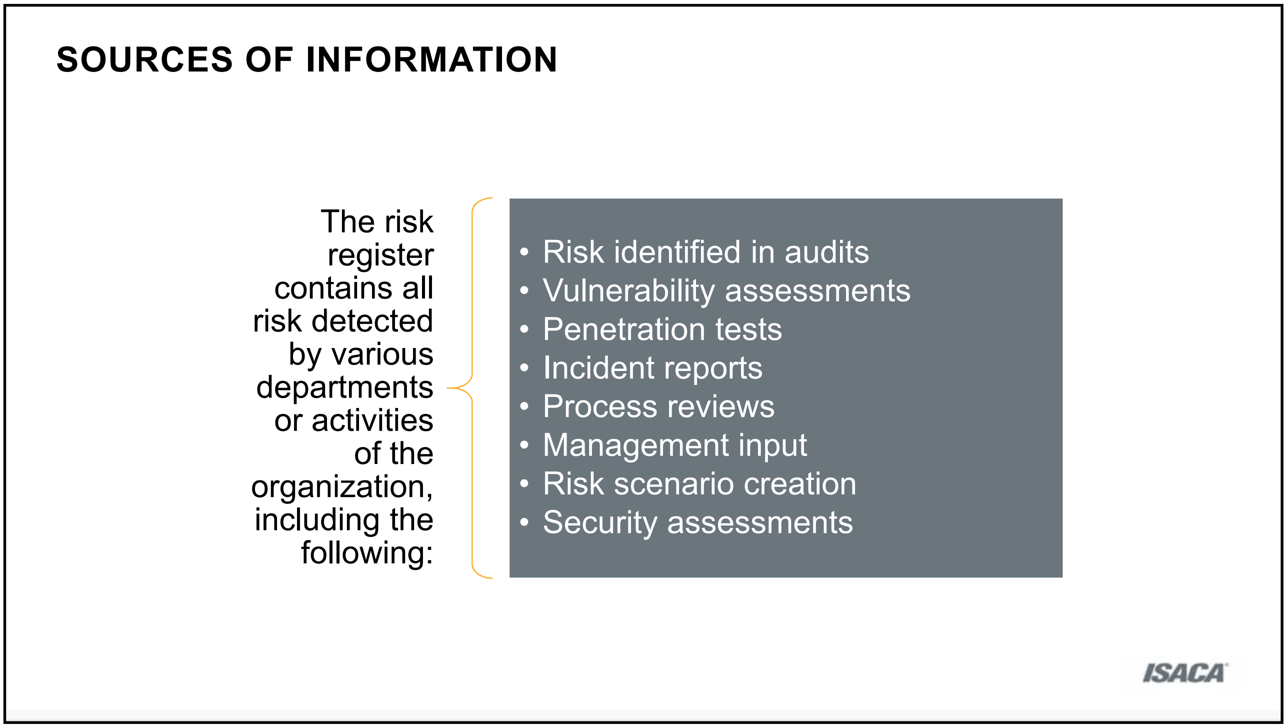


RISK REGISTER PURPOSE

The purpose of a risk register is to consolidate risk data into one place and permit the tracking of risk.

The risk register allows management to refer to a single document to do the following:

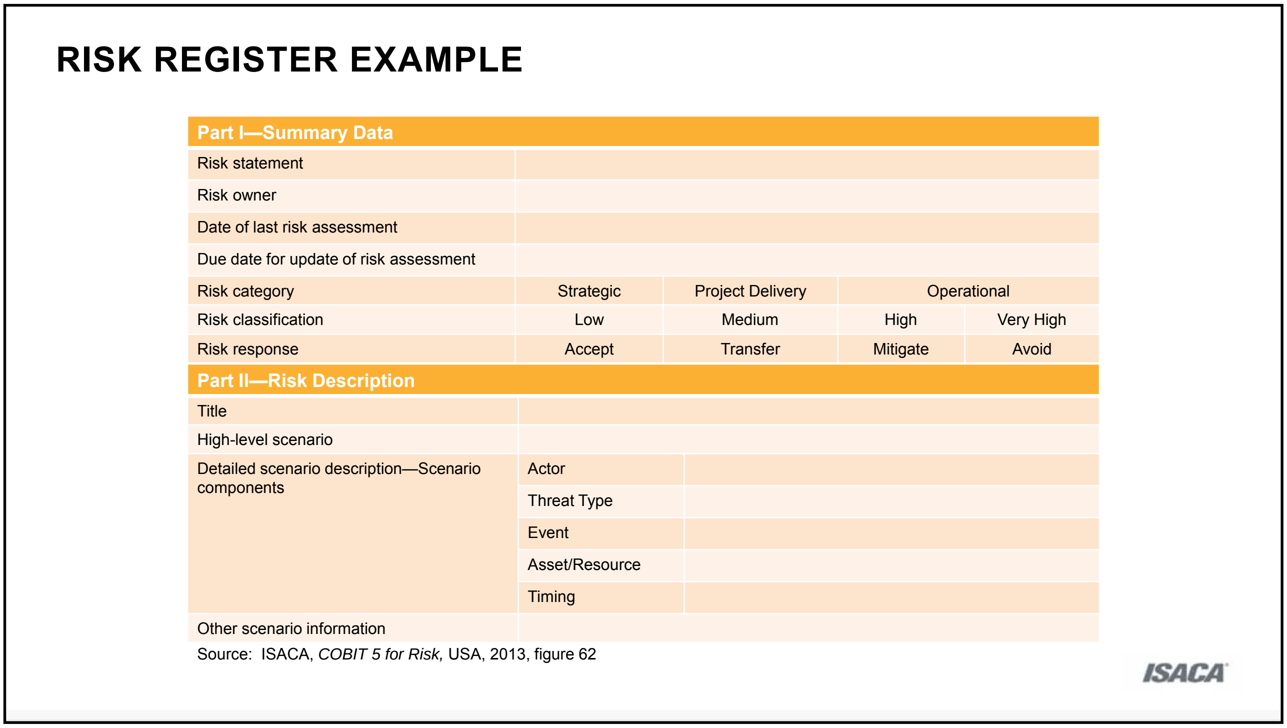
- Gain insight into the outstanding risk issues.
- Learn about the status of risk mitigation efforts.
- Become aware of the emergence of newly identified and documented risk.



SOURCES OF INFORMATION

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

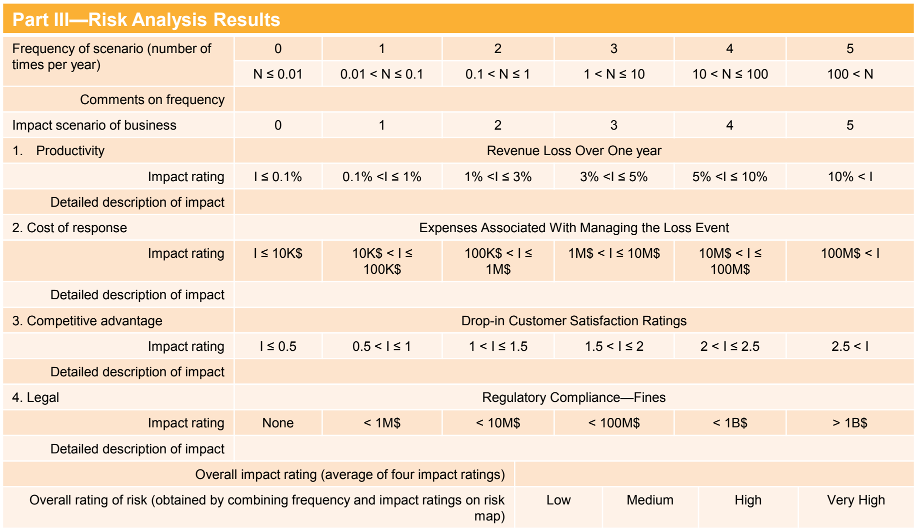


RISK REGISTER EXAMPLE

Part I—Summary Data				
Risk statement				
Risk owner				
Date of last risk assessment				
Due date for update of risk assessment				
Risk category	Strategic	Project Delivery	Operational	
Risk classification	Low	Medium	High	Very High
Risk response	Accept	Transfer	Mitigate	Avoid
Part II—Risk Description				
Title				
High-level scenario				
Detailed scenario description—Scenario components	Actor			
	Threat Type			
	Event			
	Asset/Resource			
	Timing			
Other scenario information				

Source: ISACA, *COBIT 5 for Risk,* USA, 2013, figure 62

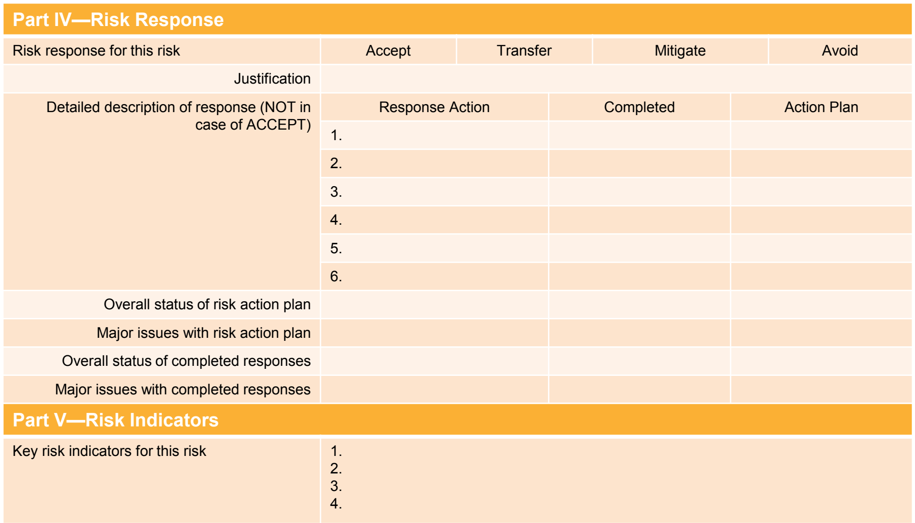
RISK REGISTER EXAMPLE (CONT'D)



Part III—Risk Analysis Results						
Frequency of scenario (number of times per year)	0	1	2	3	4	5
	N ≤ 0.01	0.01 < N ≤ 0.1	0.1 < N ≤ 1	1 < N ≤ 10	10 < N ≤ 100	100 < N
Comments on frequency						
Impact scenario of business	0	1	2	3	4	5
1. Productivity	Revenue Loss Over One year					
Impact rating	I ≤ 0.1%	0.1% <I ≤ 1%	1% <I ≤ 3%	3% <I ≤ 5%	5% <I ≤ 10%	10% < I
Detailed description of impact						
2. Cost of response	Expenses Associated With Managing the Loss Event					
Impact rating	I ≤ 10K$	10K$ < I ≤ 100K$	100K$ < I ≤ 1M$	1M$ < I ≤ 10M$	10M$ < I ≤ 100M$	100M$ < I
Detailed description of impact						
3. Competitive advantage	Drop-in Customer Satisfaction Ratings					
Impact rating	I ≤ 0.5	0.5 < I ≤ 1	1 < I ≤ 1.5	1.5 < I ≤ 2	2 < I ≤ 2.5	2.5 < I
Detailed description of impact						
4. Legal	Regulatory Compliance—Fines					
Impact rating	None	< 1M$	< 10M$	< 100M$	< 1B$	> 1B$
Detailed description of impact						
Overall impact rating (average of four impact ratings)						
Overall rating of risk (obtained by combining frequency and impact ratings on risk map)			Low	Medium	High	Very High

Source: ISACA, *COBIT 5 for Risk,* USA, 2013, figure 62

RISK REGISTER EXAMPLE (CONT'D)



Part IV—Risk Response

Risk response for this risk	Accept	Transfer	Mitigate	Avoid
Justification				

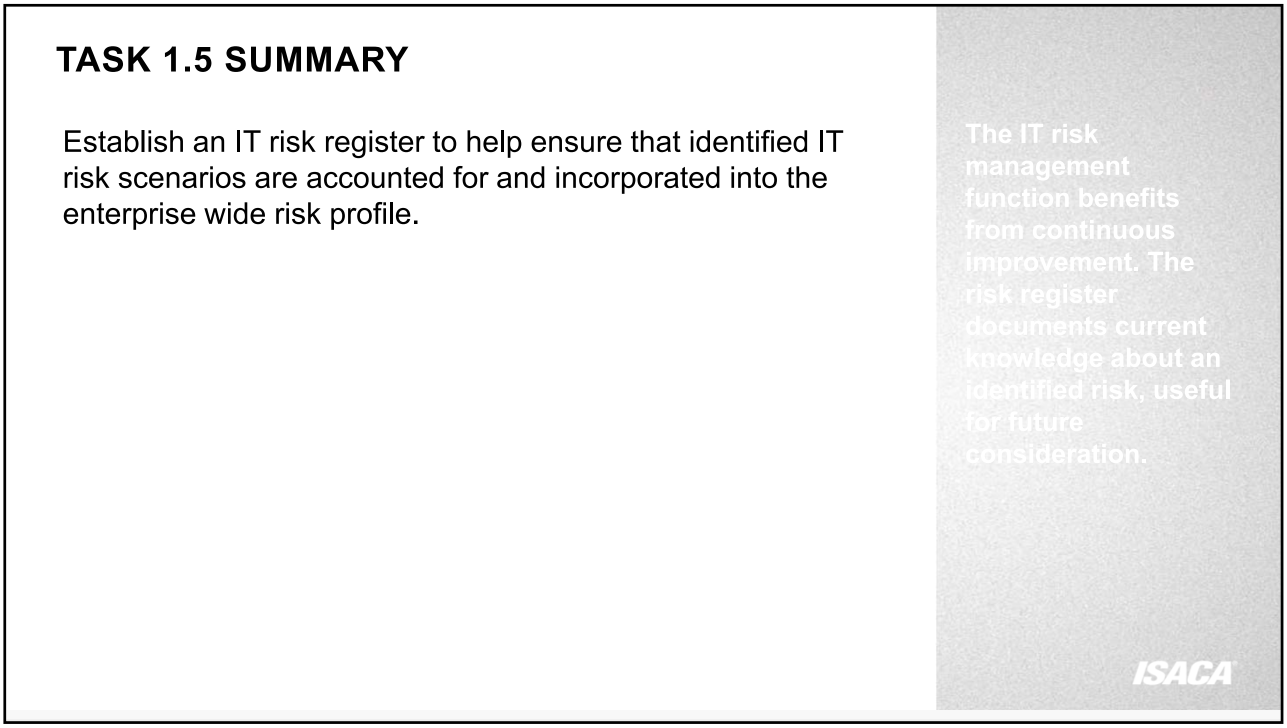
Detailed description of response (NOT in case of ACCEPT)	Response Action	Completed	Action Plan
	1.		
	2.		
	3.		
	4.		
	5.		
	6.		
Overall status of risk action plan			
Major issues with risk action plan			
Overall status of completed responses			
Major issues with completed responses			

Part V—Risk Indicators

Key risk indicators for this risk	1. 2. 3. 4.

Source: ISACA, *COBIT 5 for Risk,* USA, 2013, figure 62

ISACA



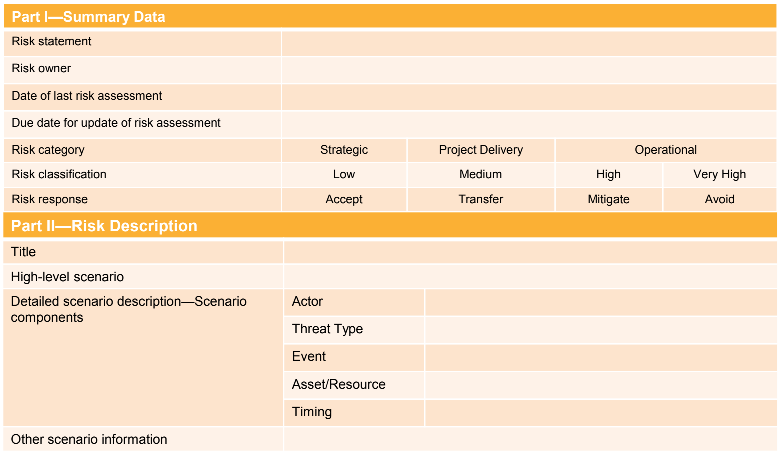
TASK 1.5 SUMMARY

Establish an IT risk register to help ensure that identified IT risk scenarios are accounted for and incorporated into the enterprise wide risk profile.

The IT risk management function benefits from continuous improvement. The risk register documents current knowledge about an identified risk, useful for future consideration.

TASK 1.5 ACTIVITY

Based on information from earlier activities, complete Parts I and II of the risk register.



Part I—Summary Data				
Risk statement				
Risk owner				
Date of last risk assessment				
Due date for update of risk assessment				
Risk category	Strategic	Project Delivery	Operational	
Risk classification	Low	Medium	High	Very High
Risk response	Accept	Transfer	Mitigate	Avoid

Part II—Risk Description		
Title		
High-level scenario		
Detailed scenario description—Scenario components	Actor	
	Threat Type	
	Event	
	Asset/Resource	
	Timing	
Other scenario information		

DISCUSSION QUESTION

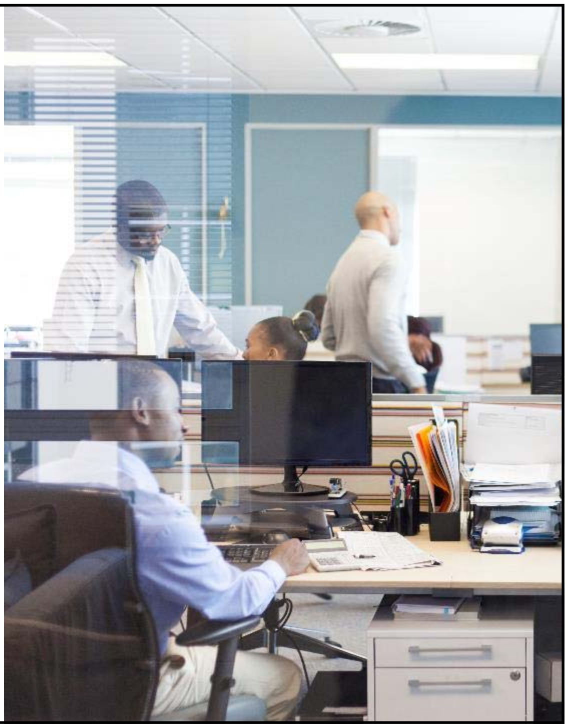
Which of the following statements BEST describes the value of a risk register?

A. It captures the risk inventory.

B. It drives the risk response plan.

C. It is a risk reporting tool.

D. It lists internal risk and external risk.



DISCUSSION QUESTION

Which of the following information in the risk register BEST helps in developing proper risk scenarios? A list of:

A. potential threats to assets.

B. residual risk on individual assets.

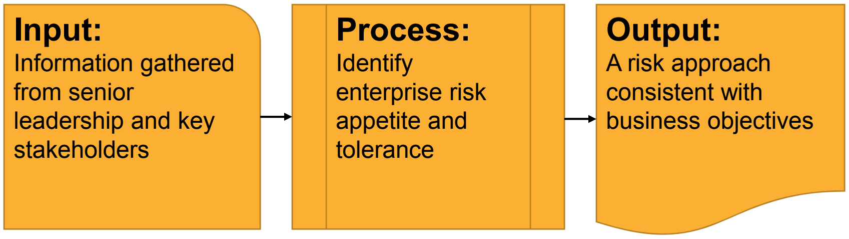
C. accepted risk.

D. security incidents.

TASK 1.6

Identify risk appetite and tolerance defined by senior leadership and key stakeholders to ensure alignment with business objectives.

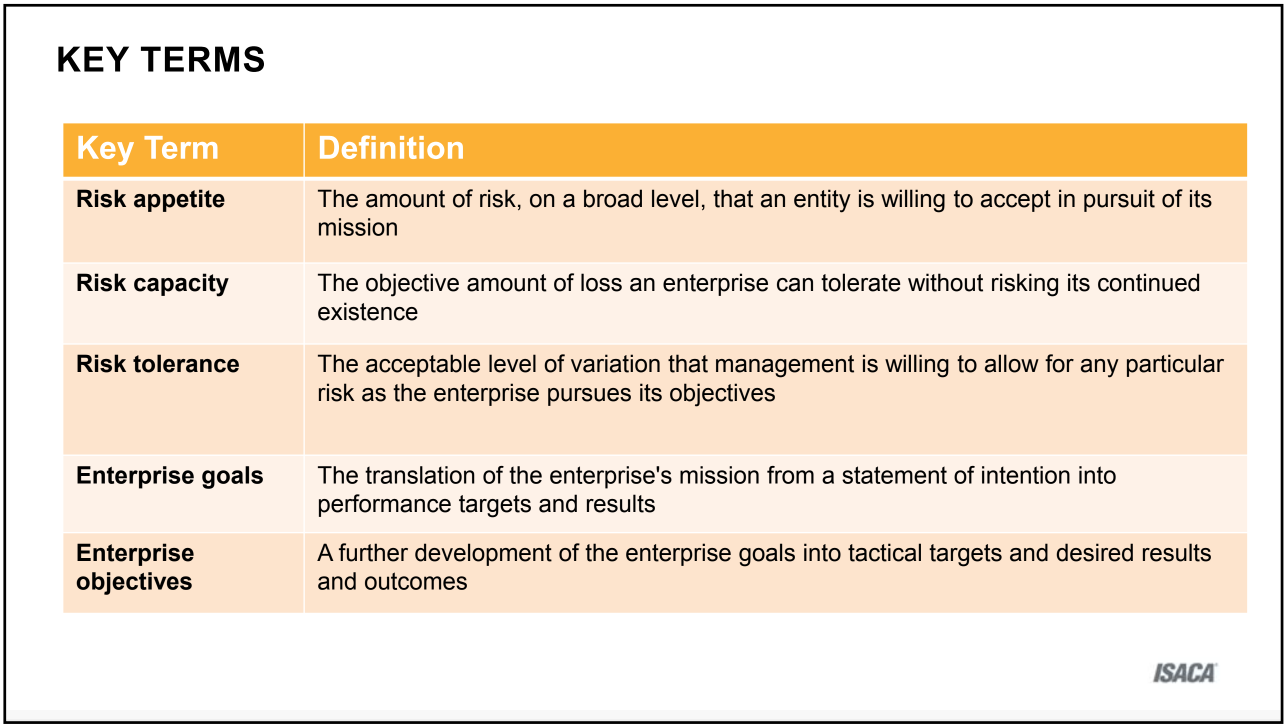
FOCUS ON TASK 1.6



Input:
Information gathered from senior leadership and key stakeholders

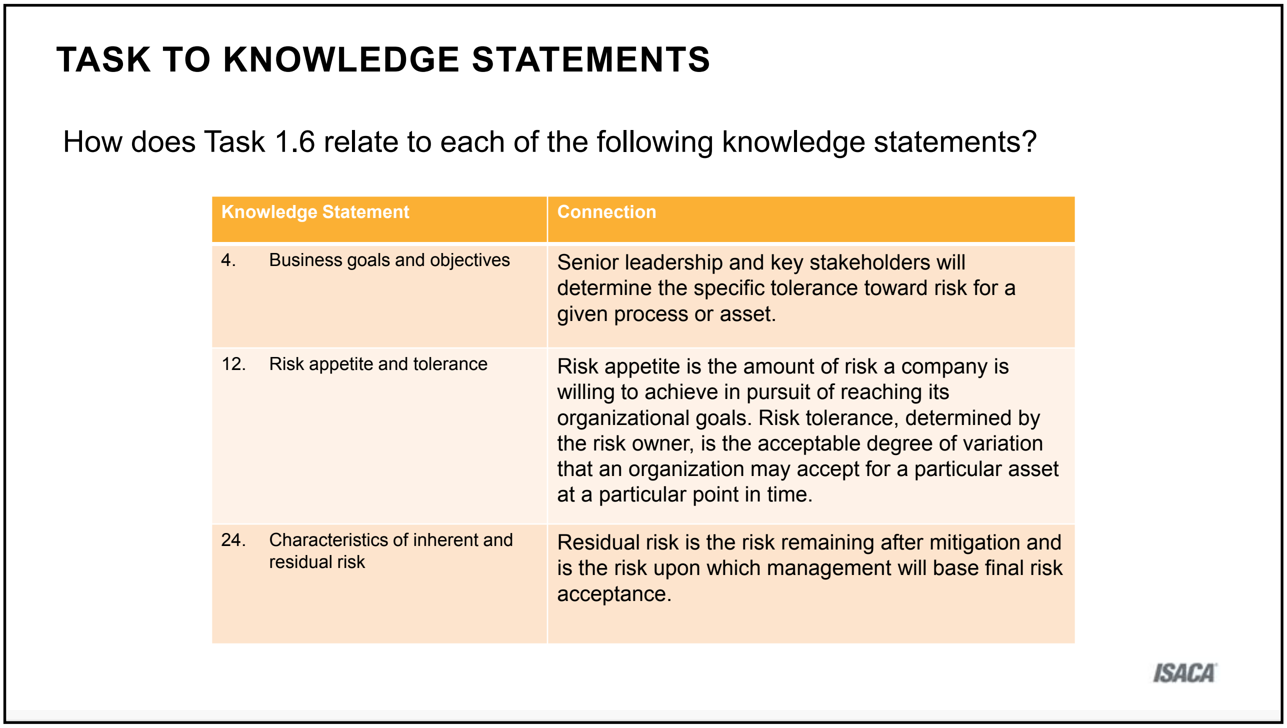
Process:
Identify enterprise risk appetite and tolerance

Output:
A risk approach consistent with business objectives



KEY TERMS

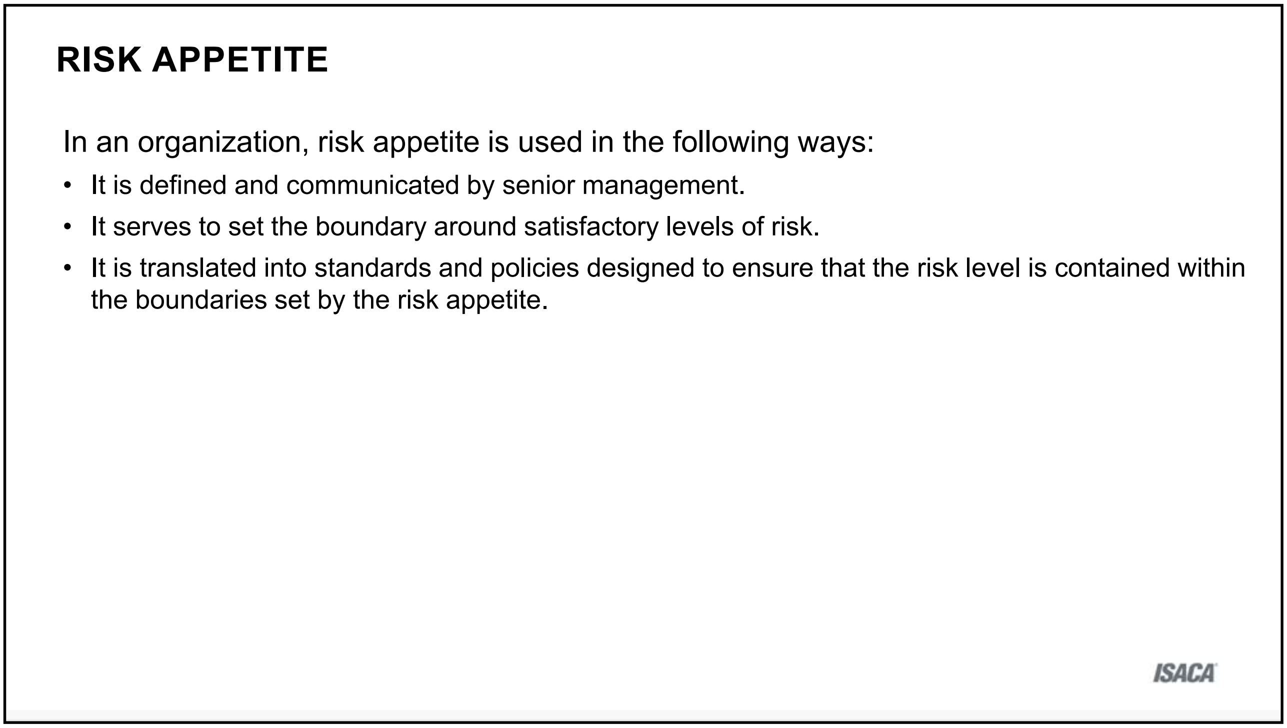
Key Term	Definition
Risk appetite	The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission
Risk capacity	The objective amount of loss an enterprise can tolerate without risking its continued existence
Risk tolerance	The acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives
Enterprise goals	The translation of the enterprise's mission from a statement of intention into performance targets and results
Enterprise objectives	A further development of the enterprise goals into tactical targets and desired results and outcomes



TASK TO KNOWLEDGE STATEMENTS

How does Task 1.6 relate to each of the following knowledge statements?

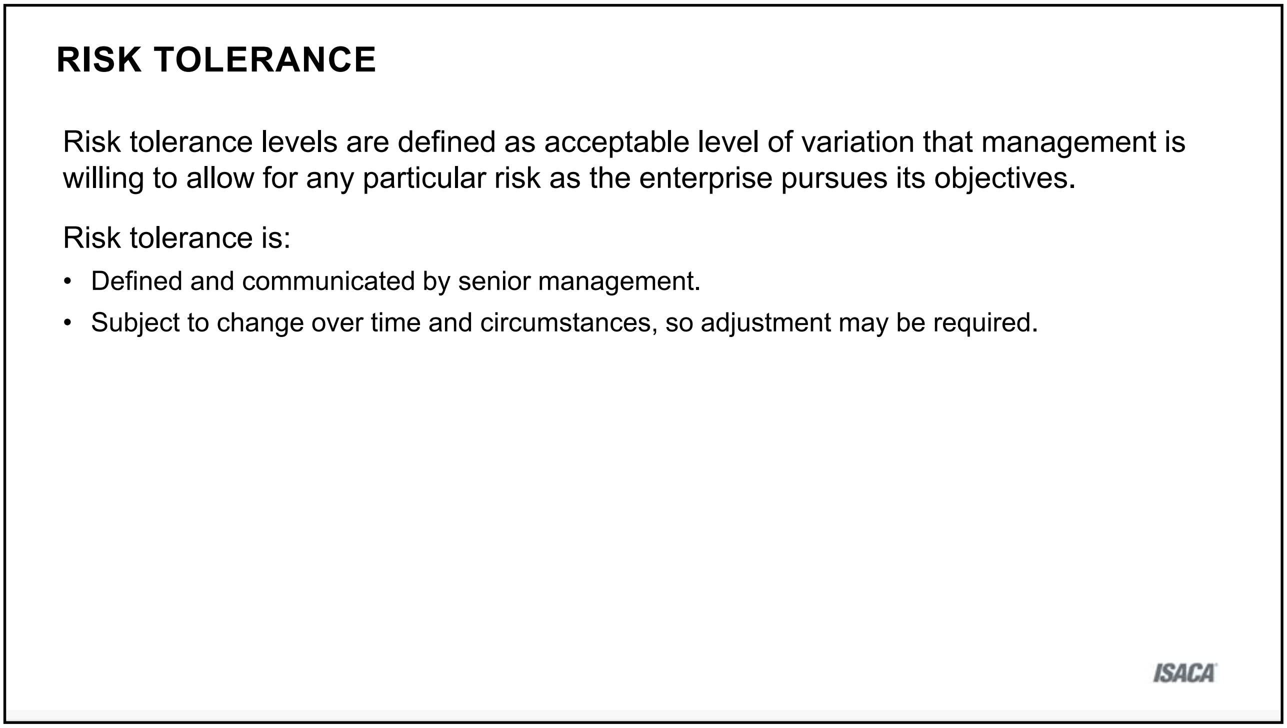
Knowledge Statement	Connection
4. Business goals and objectives	Senior leadership and key stakeholders will determine the specific tolerance toward risk for a given process or asset.
12. Risk appetite and tolerance	Risk appetite is the amount of risk a company is willing to achieve in pursuit of reaching its organizational goals. Risk tolerance, determined by the risk owner, is the acceptable degree of variation that an organization may accept for a particular asset at a particular point in time.
24. Characteristics of inherent and residual risk	Residual risk is the risk remaining after mitigation and is the risk upon which management will base final risk acceptance.



RISK APPETITE

In an organization, risk appetite is used in the following ways:

- It is defined and communicated by senior management.
- It serves to set the boundary around satisfactory levels of risk.
- It is translated into standards and policies designed to ensure that the risk level is contained within the boundaries set by the risk appetite.

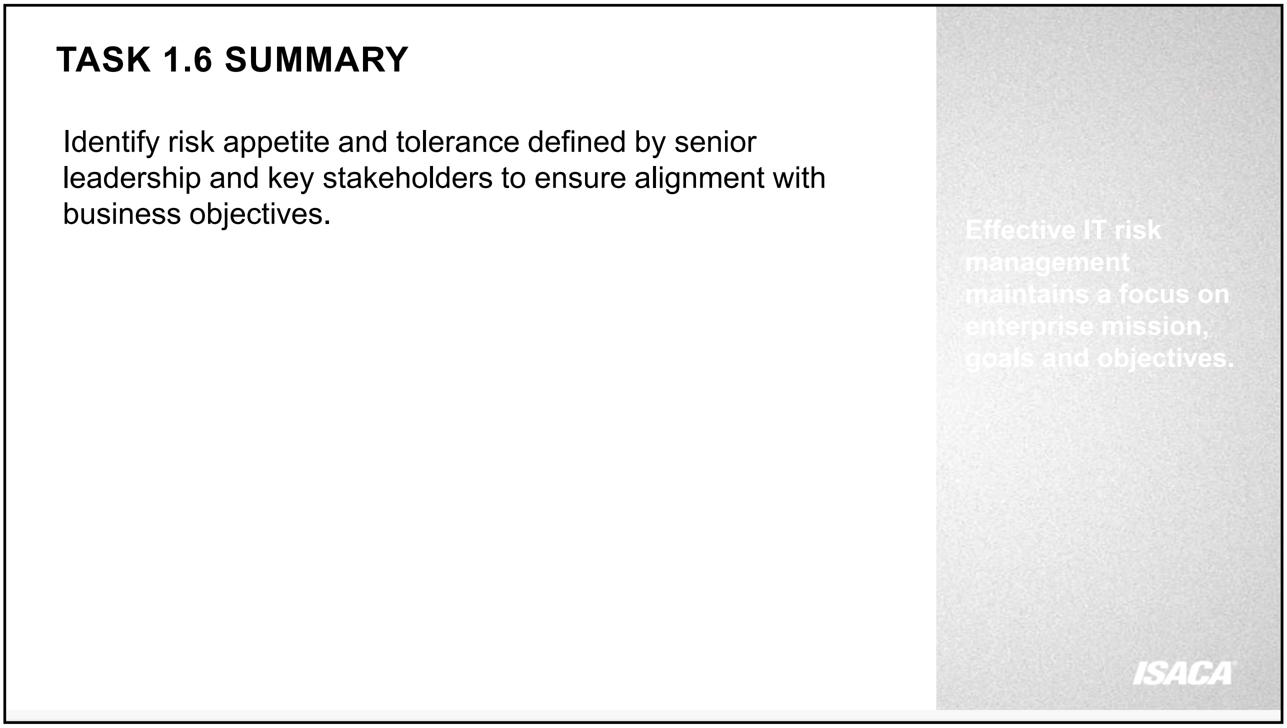


RISK TOLERANCE

Risk tolerance levels are defined as acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives.

Risk tolerance is:

- Defined and communicated by senior management.
- Subject to change over time and circumstances, so adjustment may be required.



TASK 1.6 SUMMARY

Identify risk appetite and tolerance defined by senior leadership and key stakeholders to ensure alignment with business objectives.

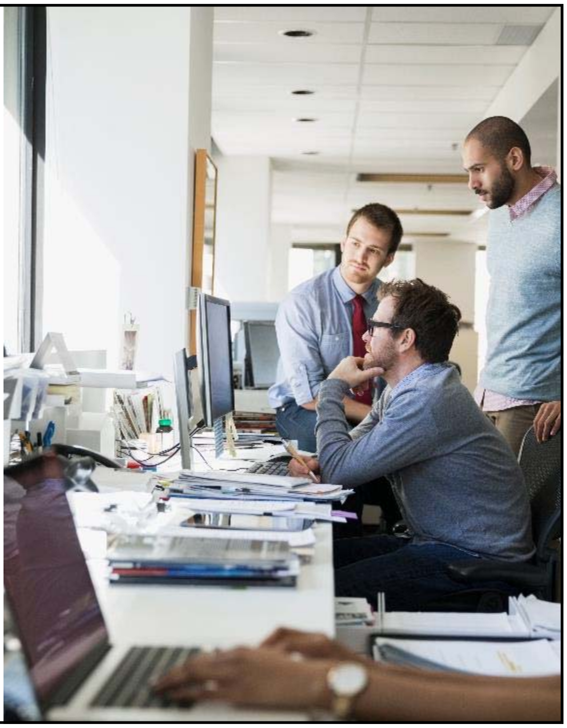
Effective IT risk management maintains a focus on enterprise mission, goals and objectives.

TASK 1.6 DISCUSSION

Describe your organization's risk appetite and risk tolerance positions.

Are these in writing?

What are the enterprise objectives for your company? How did you learn these?



DISCUSSION QUESTION

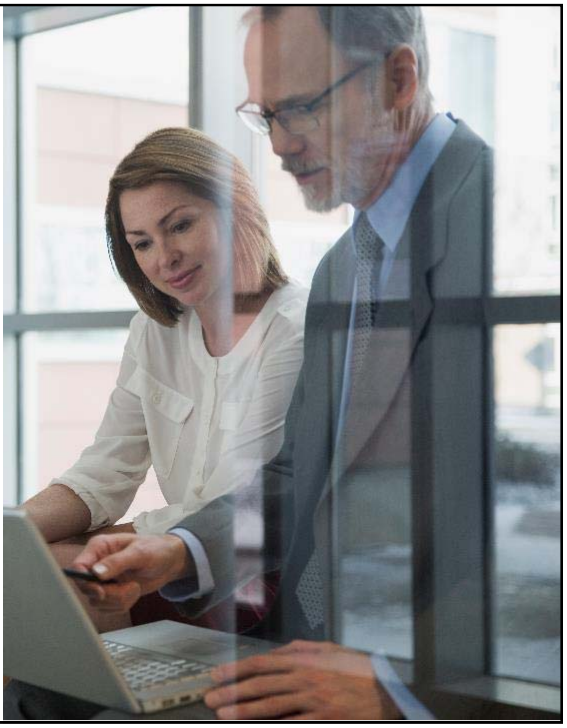
It is MOST important that risk appetite be aligned with business objectives to ensure that:

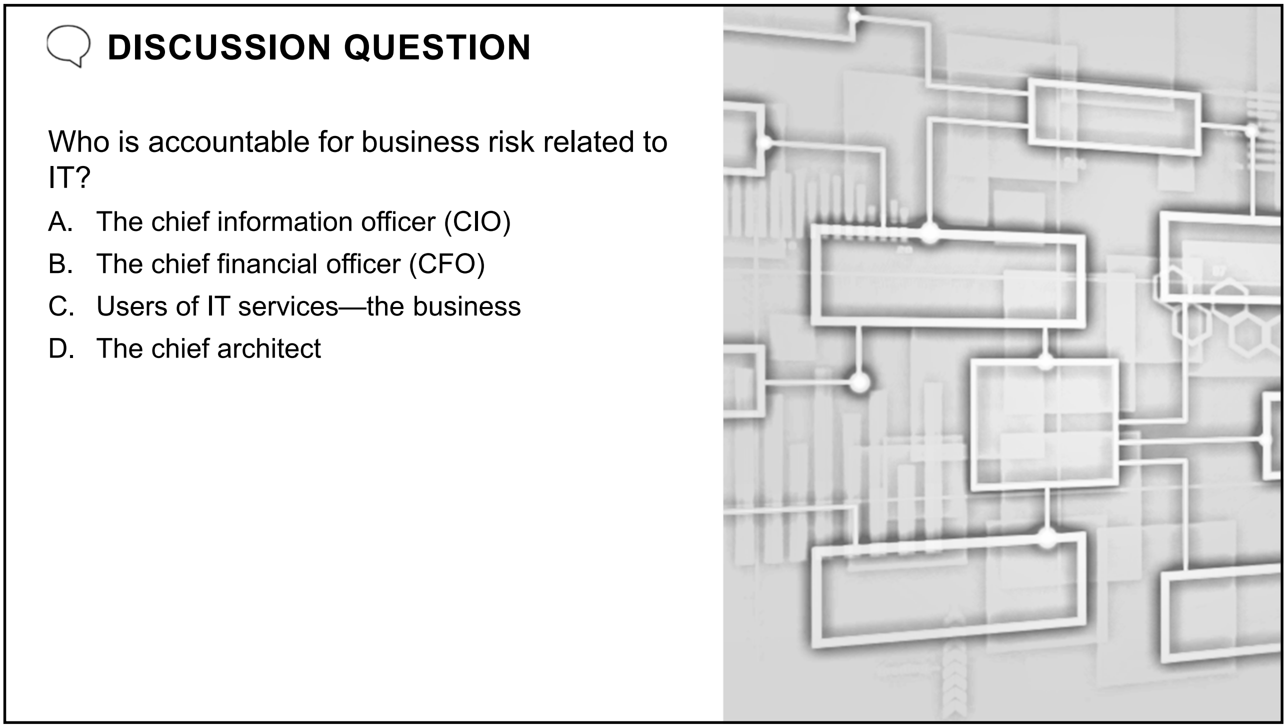
A. resources are directed toward areas of low risk tolerance.

B. major risk is identified and eliminated.

C. IT and business goals are aligned.

D. the risk strategy is adequately communicated.





DISCUSSION QUESTION

Who is accountable for business risk related to IT?

A. The chief information officer (CIO)

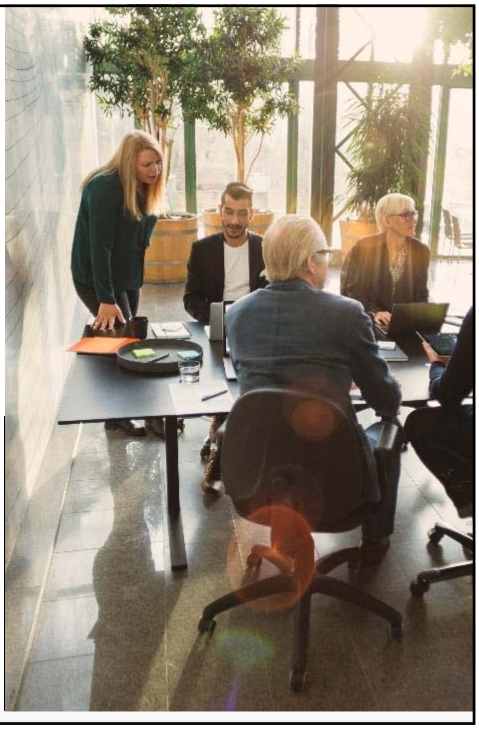
B. The chief financial officer (CFO)

C. Users of IT services—the business

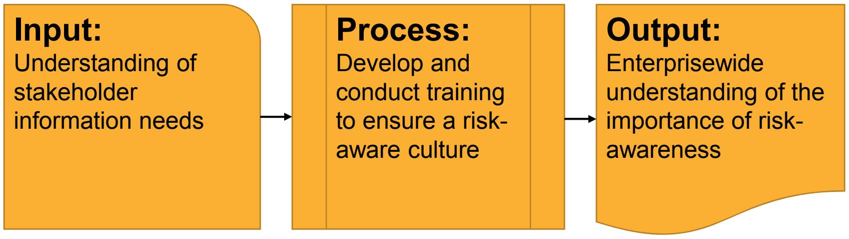
D. The chief architect

TASK 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.



FOCUS ON TASK 1.7

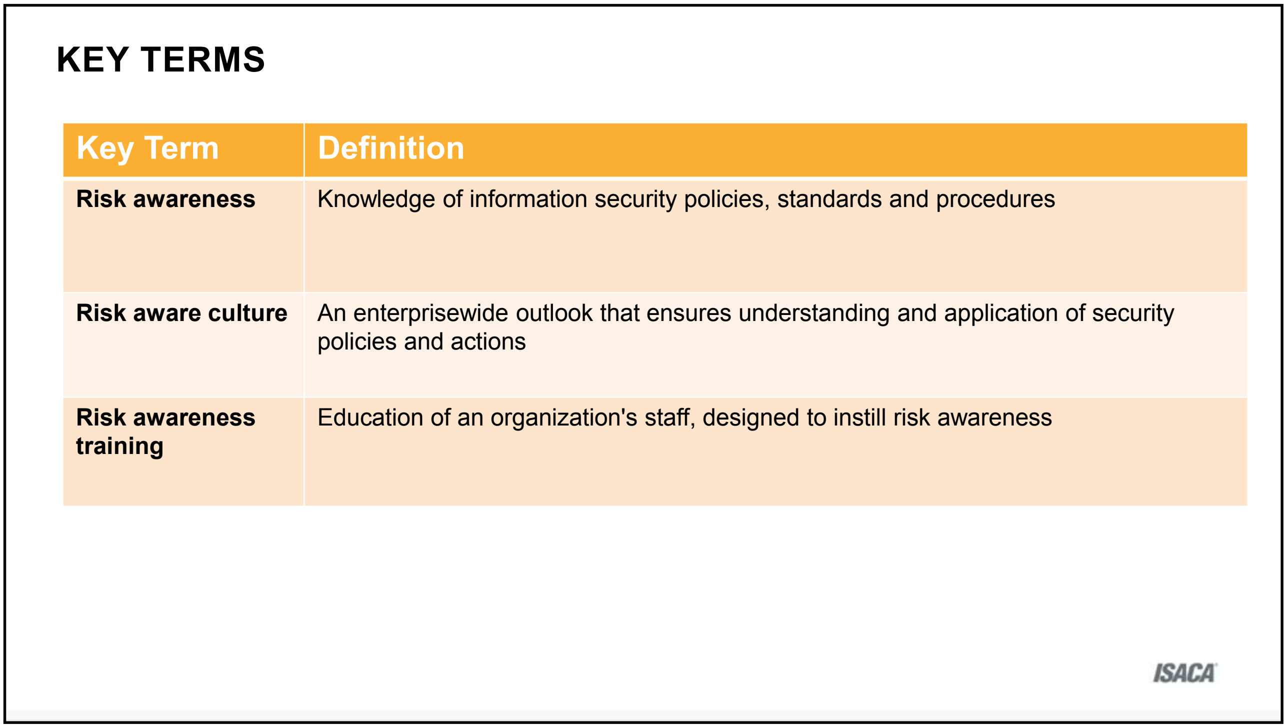


Input: Understanding of stakeholder information needs

Process: Develop and conduct training to ensure a risk-aware culture

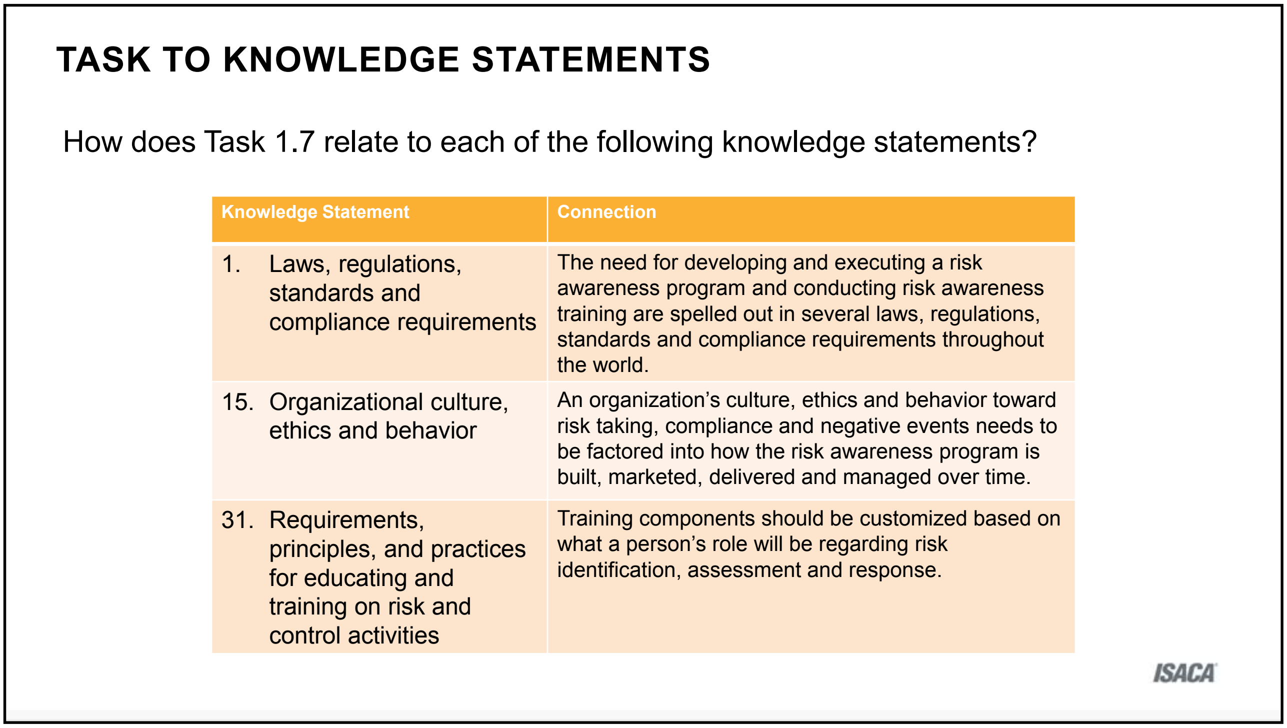
Output: Enterprisewide understanding of the importance of risk-awareness

ISACA



KEY TERMS

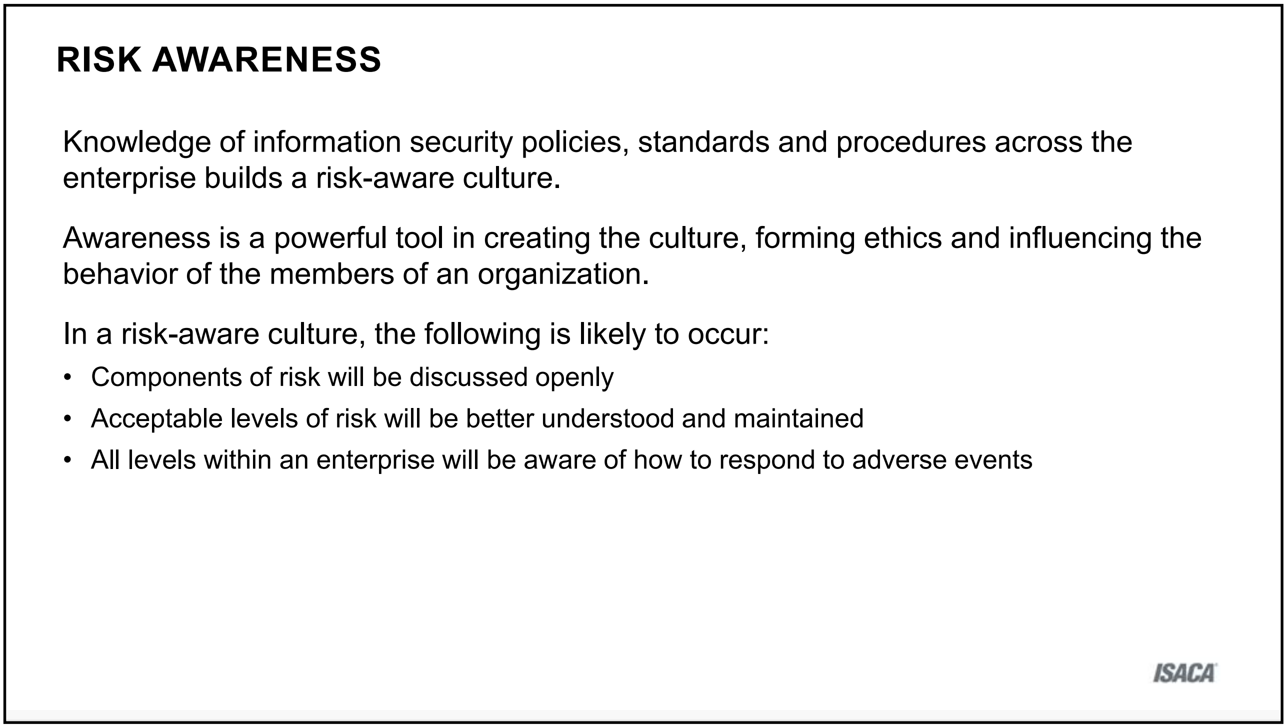
Key Term	Definition
Risk awareness	Knowledge of information security policies, standards and procedures
Risk aware culture	An enterprisewide outlook that ensures understanding and application of security policies and actions
Risk awareness training	Education of an organization's staff, designed to instill risk awareness



TASK TO KNOWLEDGE STATEMENTS

How does Task 1.7 relate to each of the following knowledge statements?

Knowledge Statement	Connection
1. Laws, regulations, standards and compliance requirements	The need for developing and executing a risk awareness program and conducting risk awareness training are spelled out in several laws, regulations, standards and compliance requirements throughout the world.
15. Organizational culture, ethics and behavior	An organization's culture, ethics and behavior toward risk taking, compliance and negative events needs to be factored into how the risk awareness program is built, marketed, delivered and managed over time.
31. Requirements, principles, and practices for educating and training on risk and control activities	Training components should be customized based on what a person's role will be regarding risk identification, assessment and response.



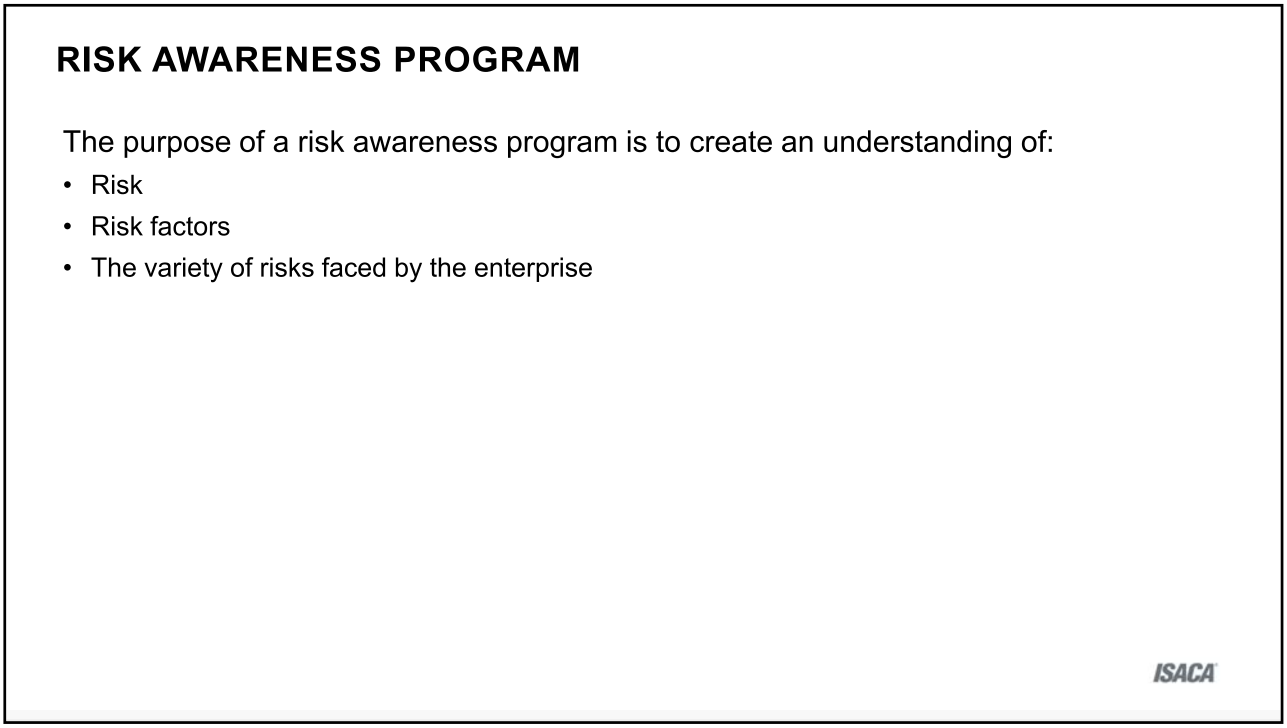
RISK AWARENESS

Knowledge of information security policies, standards and procedures across the enterprise builds a risk-aware culture.

Awareness is a powerful tool in creating the culture, forming ethics and influencing the behavior of the members of an organization.

In a risk-aware culture, the following is likely to occur:

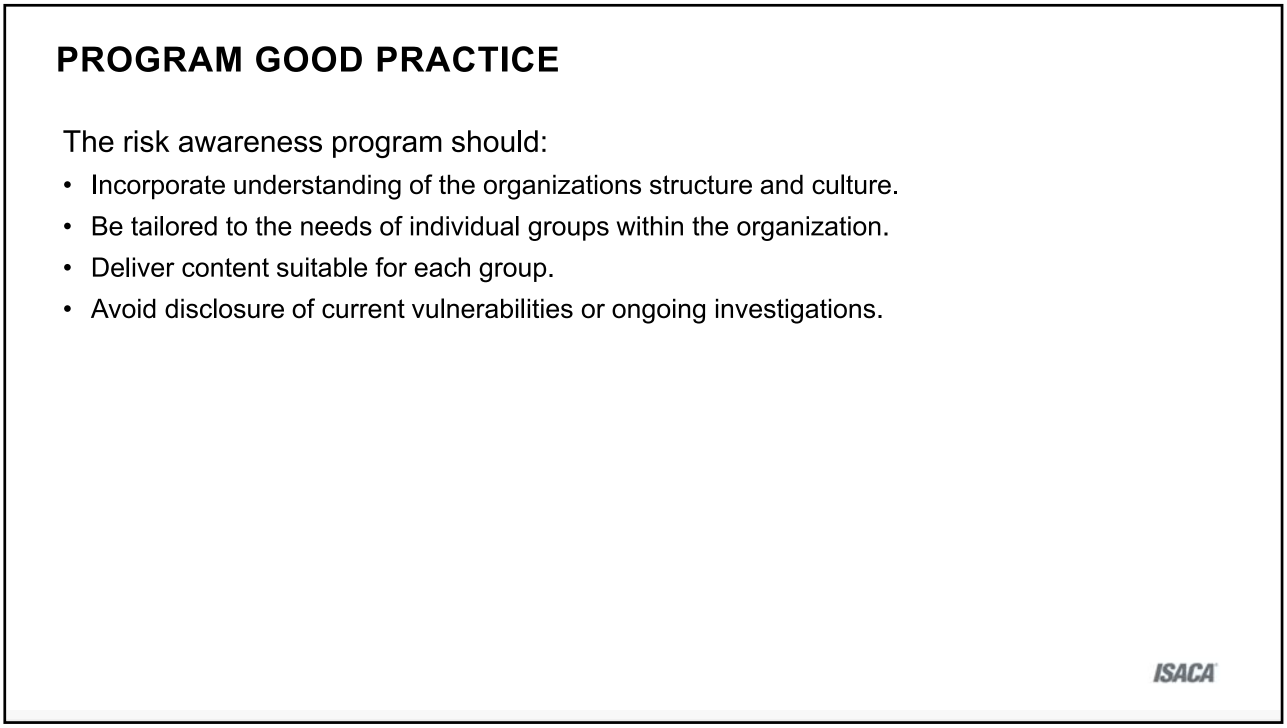
- Components of risk will be discussed openly
- Acceptable levels of risk will be better understood and maintained
- All levels within an enterprise will be aware of how to respond to adverse events



RISK AWARENESS PROGRAM

The purpose of a risk awareness program is to create an understanding of:

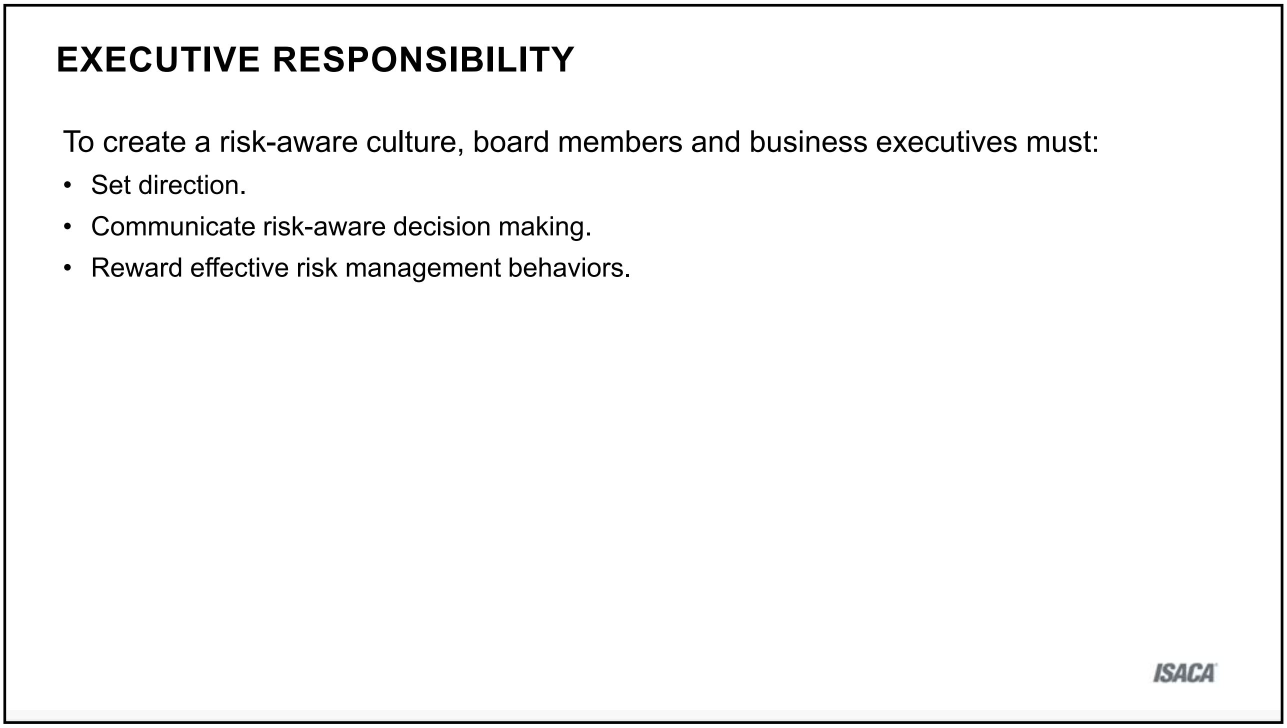
- Risk
- Risk factors
- The variety of risks faced by the enterprise



PROGRAM GOOD PRACTICE

The risk awareness program should:

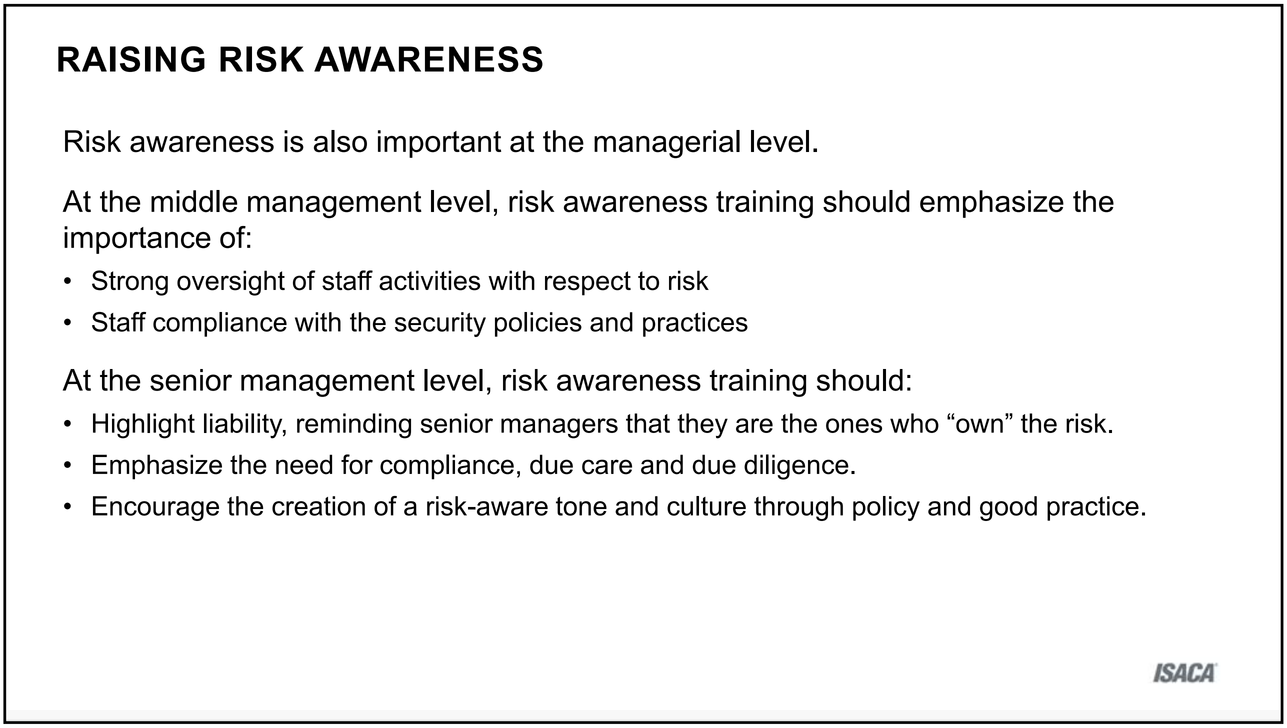
- Incorporate understanding of the organizations structure and culture.
- Be tailored to the needs of individual groups within the organization.
- Deliver content suitable for each group.
- Avoid disclosure of current vulnerabilities or ongoing investigations.



EXECUTIVE RESPONSIBILITY

To create a risk-aware culture, board members and business executives must:

- Set direction.
- Communicate risk-aware decision making.
- Reward effective risk management behaviors.



RAISING RISK AWARENESS

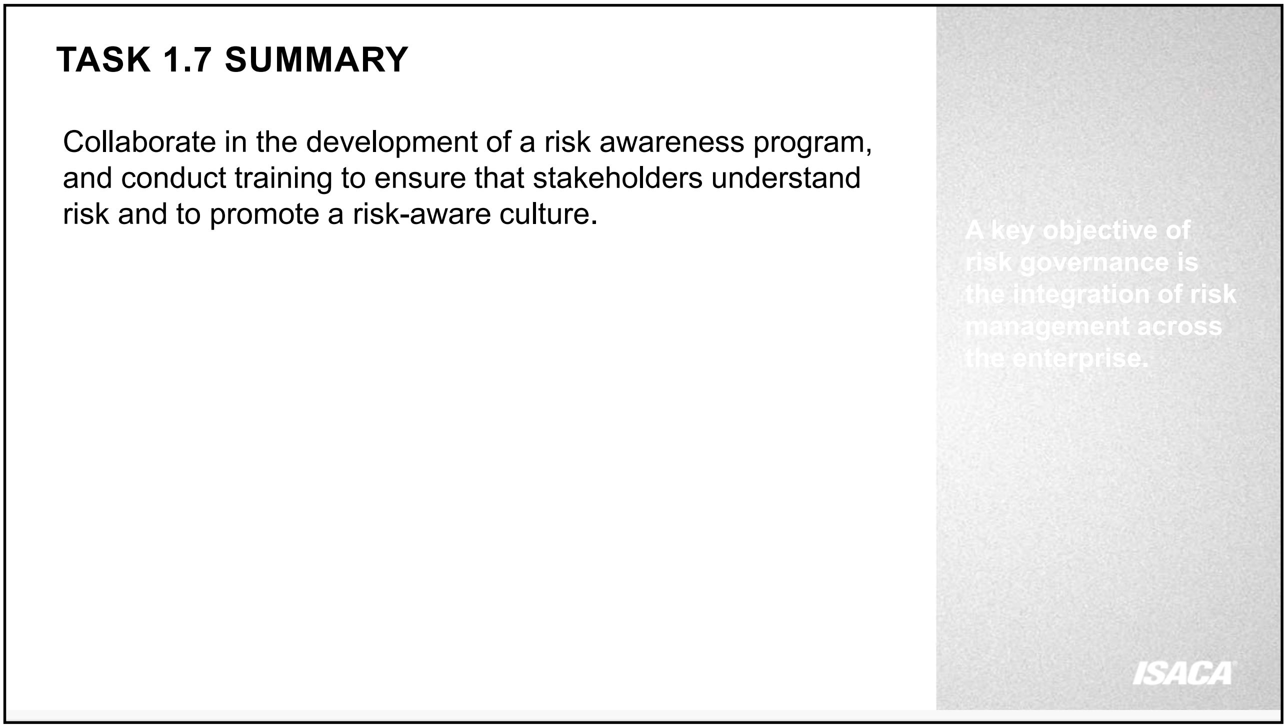
Risk awareness is also important at the managerial level.

At the middle management level, risk awareness training should emphasize the importance of:

- Strong oversight of staff activities with respect to risk
- Staff compliance with the security policies and practices

At the senior management level, risk awareness training should:

- Highlight liability, reminding senior managers that they are the ones who “own” the risk.
- Emphasize the need for compliance, due care and due diligence.
- Encourage the creation of a risk-aware tone and culture through policy and good practice.



TASK 1.7 SUMMARY

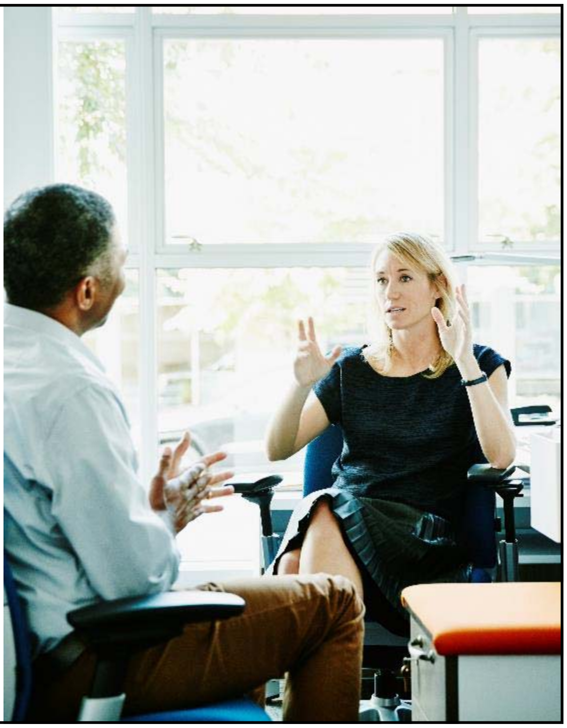
Collaborate in the development of a risk awareness program, and conduct training to ensure that stakeholders understand risk and to promote a risk-aware culture.

A key objective of risk governance is the integration of risk management across the enterprise.

🗨 TASK 1.7 DISCUSSION

What does your company currently do regarding risk awareness training?

Where may opportunities lie in the future?



DISCUSSION QUESTION

Which of the following is a PRIMARY consideration when developing an IT risk awareness program?

A. Why technology risk is owned by IT

B. How technology risk can impact each attendee's area of business

C. How business process owners can transfer technology risk

D. Why technology risk is more difficult to manage compared to other risk

DISCUSSION QUESTION

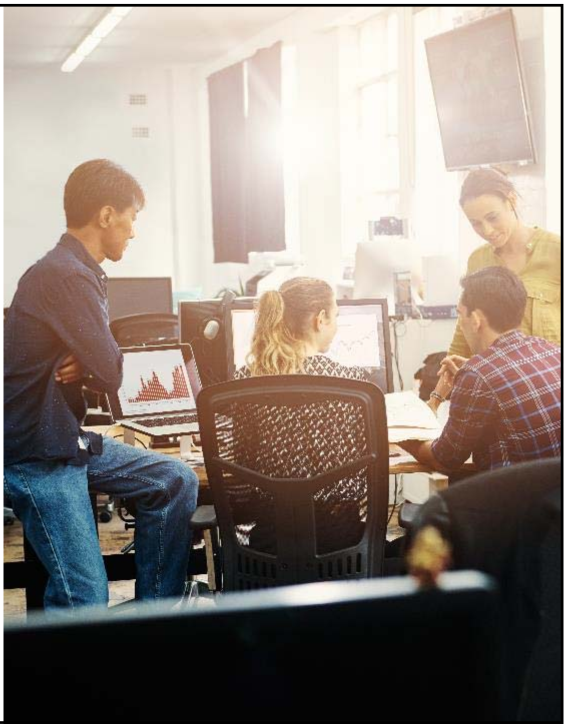
Which of the following is the GREATEST benefit of a risk-aware culture?

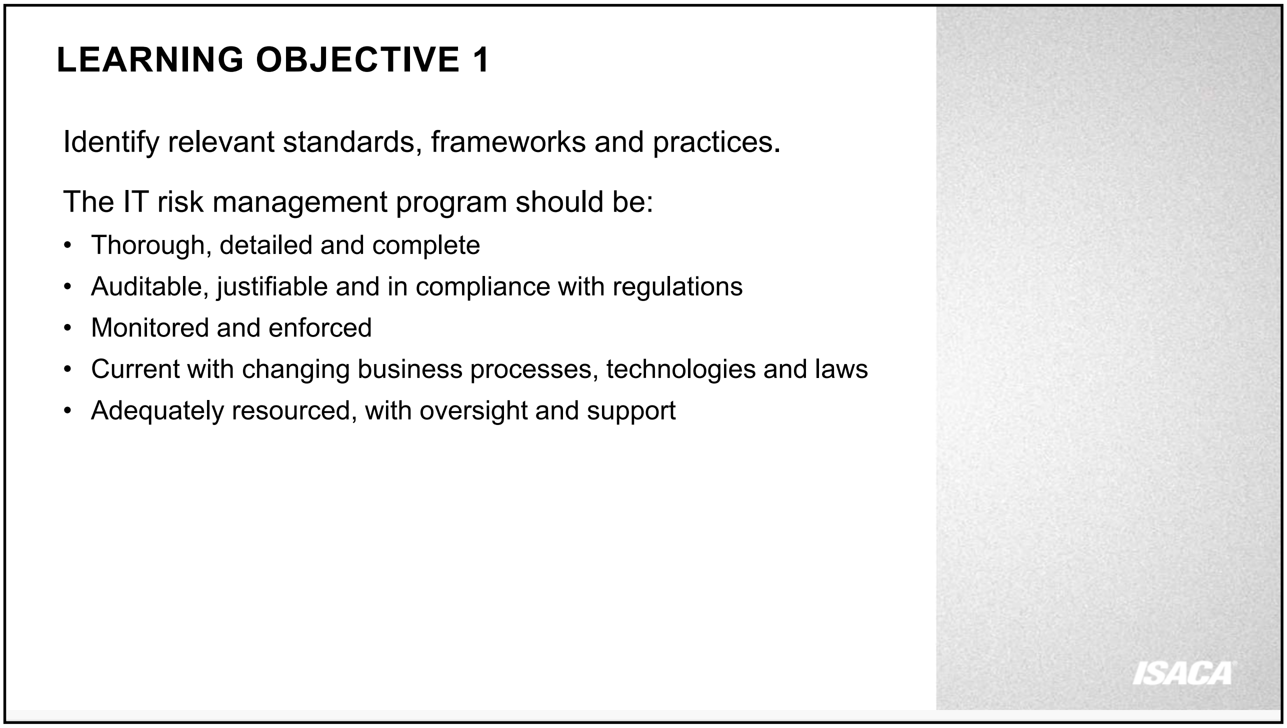
A. Issues are escalated when suspicious activity is noticed.

B. Controls are double-checked to anticipate any issues.

C. Individuals communicate with peers for knowledge sharing.

D. Employees are self-motivated to learn about costs and benefits.



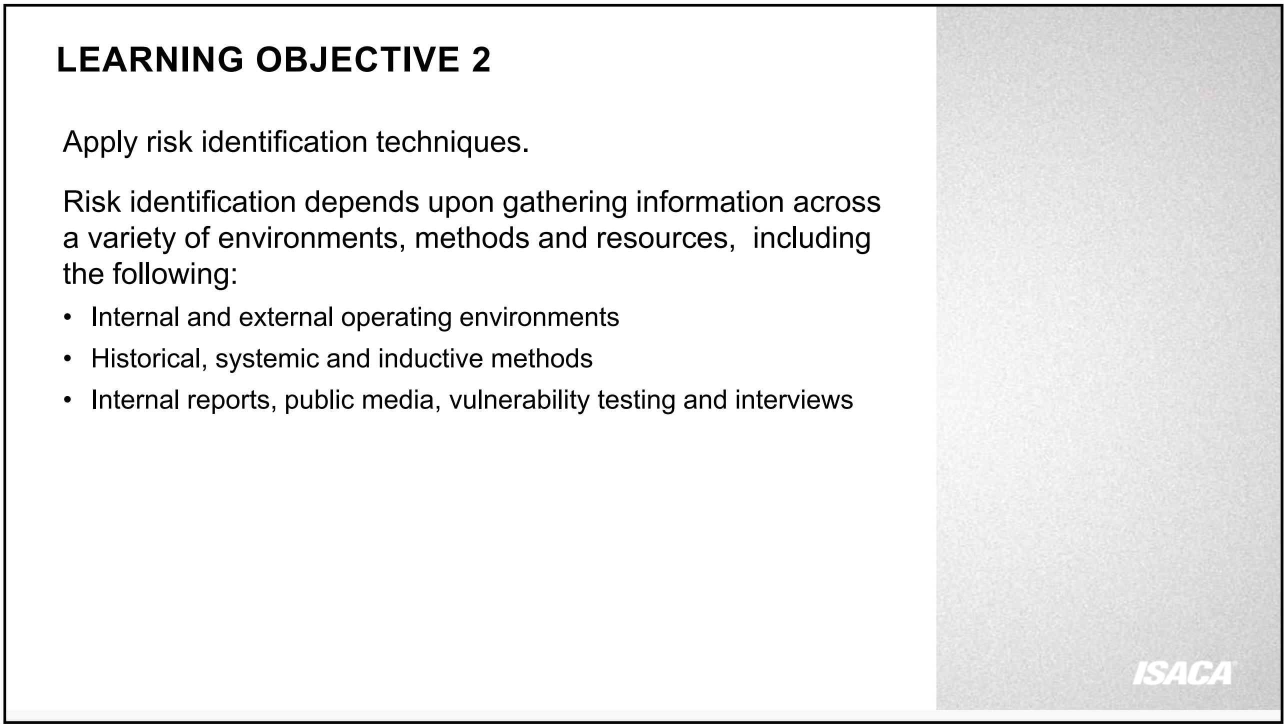


LEARNING OBJECTIVE 1

Identify relevant standards, frameworks and practices.

The IT risk management program should be:

- Thorough, detailed and complete
- Auditable, justifiable and in compliance with regulations
- Monitored and enforced
- Current with changing business processes, technologies and laws
- Adequately resourced, with oversight and support

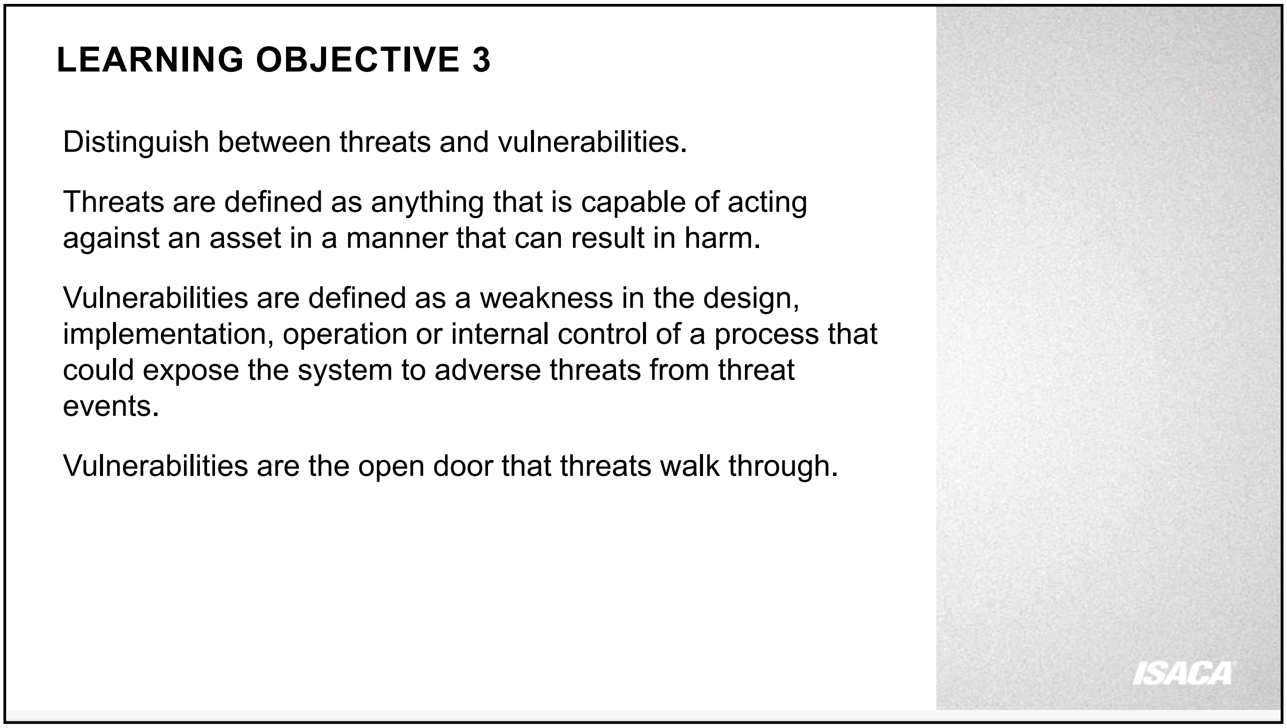


LEARNING OBJECTIVE 2

Apply risk identification techniques.

Risk identification depends upon gathering information across a variety of environments, methods and resources, including the following:

- Internal and external operating environments
- Historical, systemic and inductive methods
- Internal reports, public media, vulnerability testing and interviews



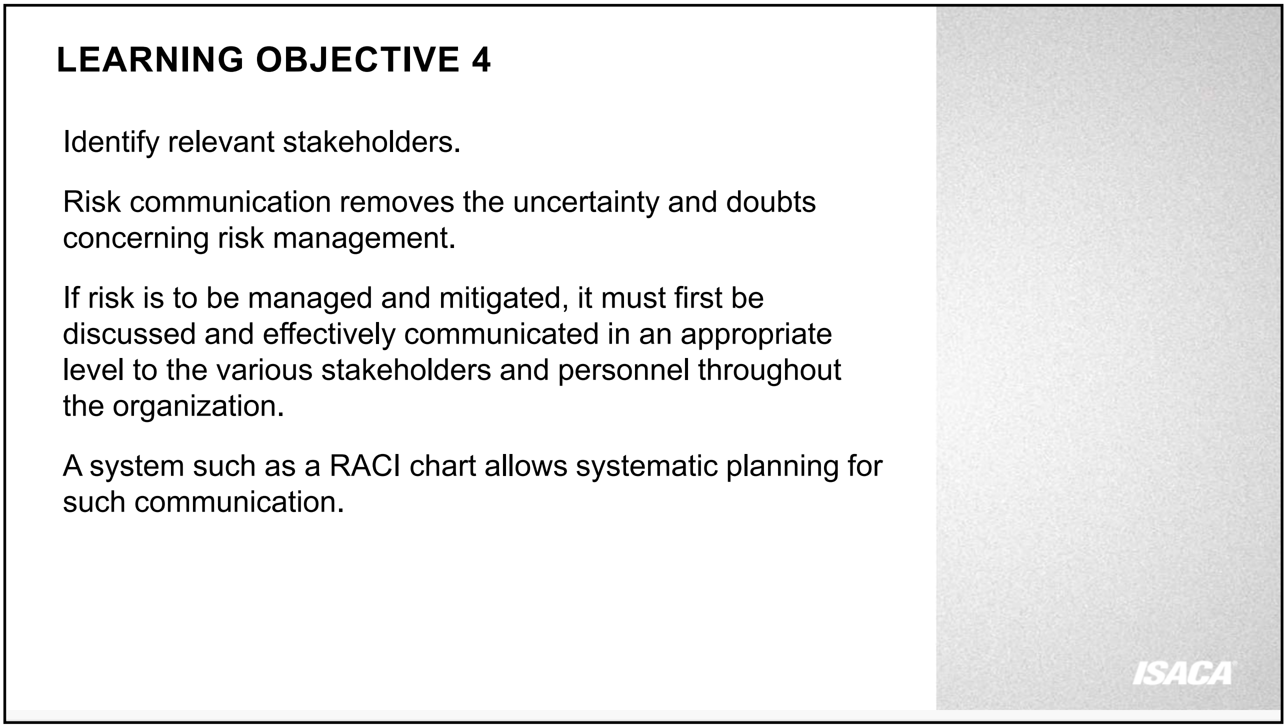
LEARNING OBJECTIVE 3

Distinguish between threats and vulnerabilities.

Threats are defined as anything that is capable of acting against an asset in a manner that can result in harm.

Vulnerabilities are defined as a weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events.

Vulnerabilities are the open door that threats walk through.



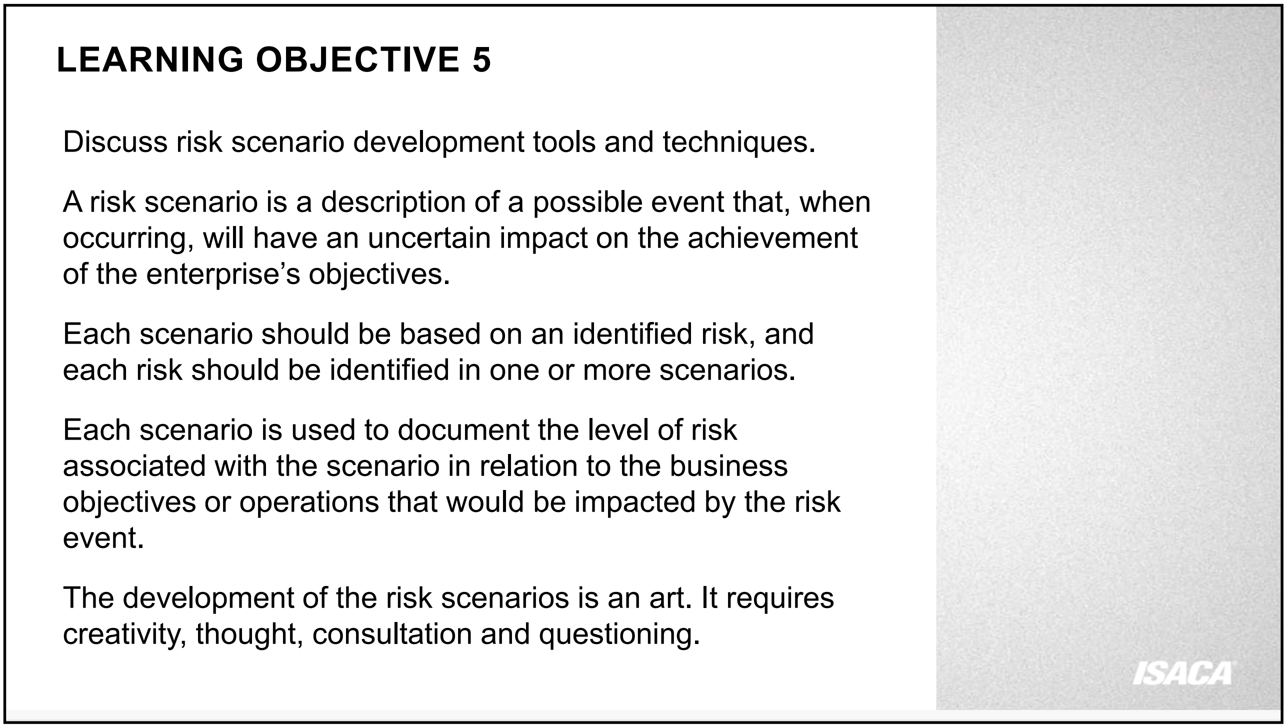
LEARNING OBJECTIVE 4

Identify relevant stakeholders.

Risk communication removes the uncertainty and doubts concerning risk management.

If risk is to be managed and mitigated, it must first be discussed and effectively communicated in an appropriate level to the various stakeholders and personnel throughout the organization.

A system such as a RACI chart allows systematic planning for such communication.



LEARNING OBJECTIVE 5

Discuss risk scenario development tools and techniques.

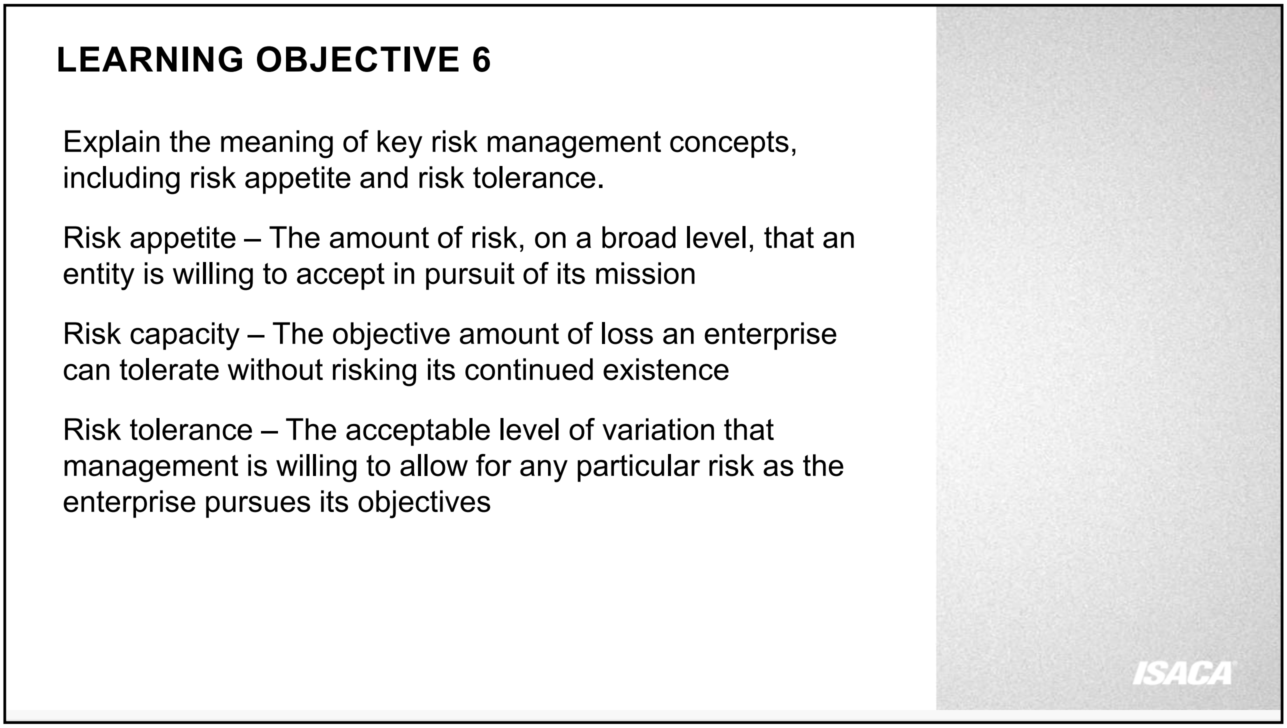
A risk scenario is a description of a possible event that, when occurring, will have an uncertain impact on the achievement of the enterprise’s objectives.

Each scenario should be based on an identified risk, and each risk should be identified in one or more scenarios.

Each scenario is used to document the level of risk associated with the scenario in relation to the business objectives or operations that would be impacted by the risk event.

The development of the risk scenarios is an art. It requires creativity, thought, consultation and questioning.

ISACA



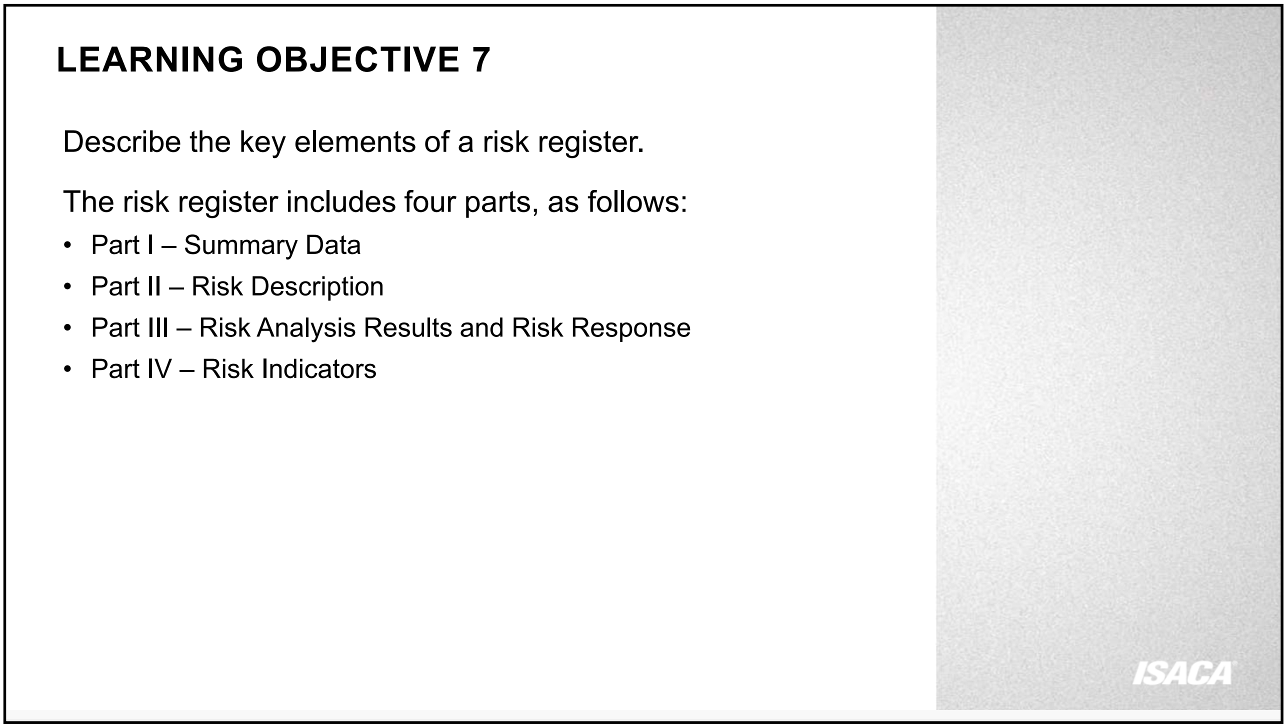
LEARNING OBJECTIVE 6

Explain the meaning of key risk management concepts, including risk appetite and risk tolerance.

Risk appetite – The amount of risk, on a broad level, that an entity is willing to accept in pursuit of its mission

Risk capacity – The objective amount of loss an enterprise can tolerate without risking its continued existence

Risk tolerance – The acceptable level of variation that management is willing to allow for any particular risk as the enterprise pursues its objectives

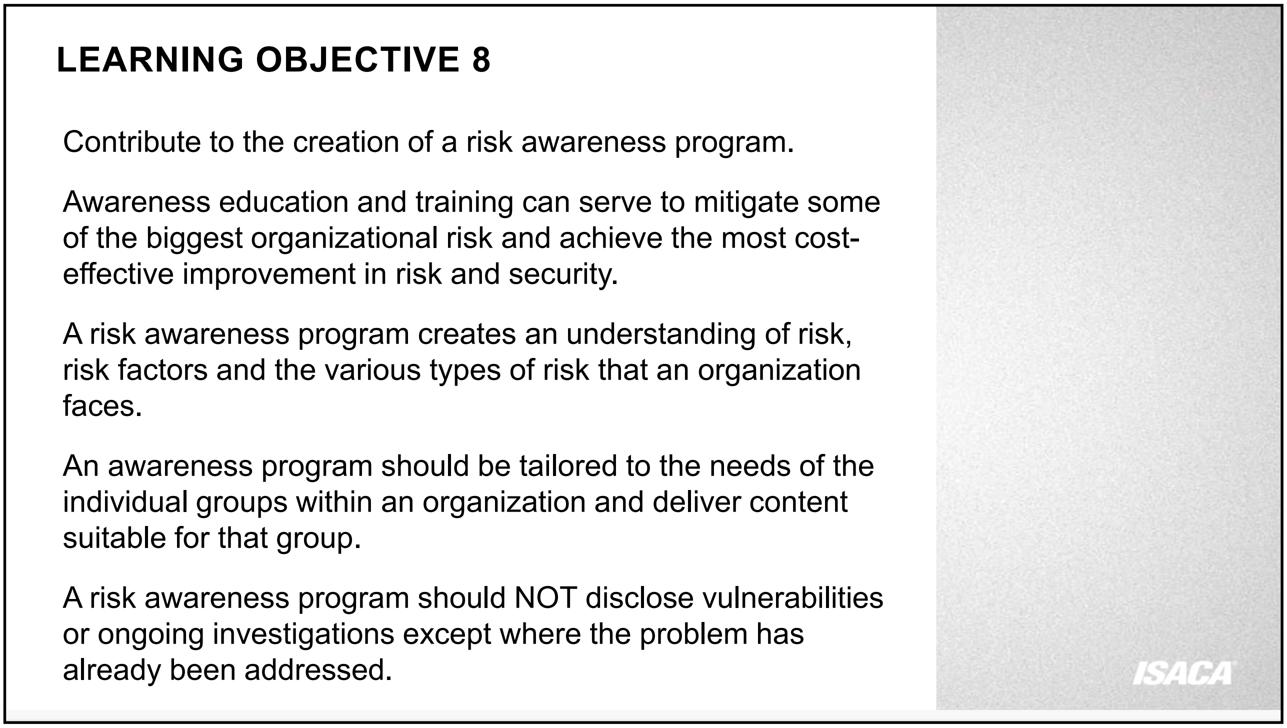


LEARNING OBJECTIVE 7

Describe the key elements of a risk register.

The risk register includes four parts, as follows:

- Part I – Summary Data
- Part II – Risk Description
- Part III – Risk Analysis Results and Risk Response
- Part IV – Risk Indicators



LEARNING OBJECTIVE 8

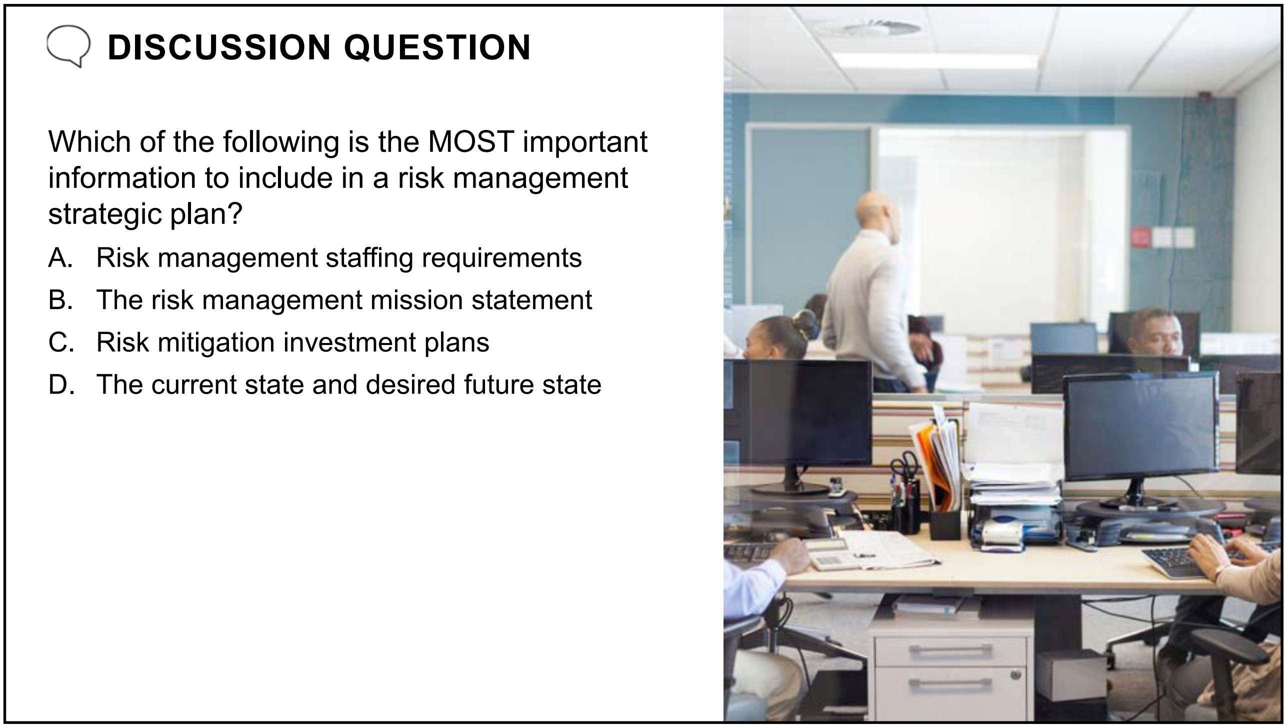
Contribute to the creation of a risk awareness program.

Awareness education and training can serve to mitigate some of the biggest organizational risk and achieve the most cost-effective improvement in risk and security.

A risk awareness program creates an understanding of risk, risk factors and the various types of risk that an organization faces.

An awareness program should be tailored to the needs of the individual groups within an organization and deliver content suitable for that group.

A risk awareness program should NOT disclose vulnerabilities or ongoing investigations except where the problem has already been addressed.



DISCUSSION QUESTION

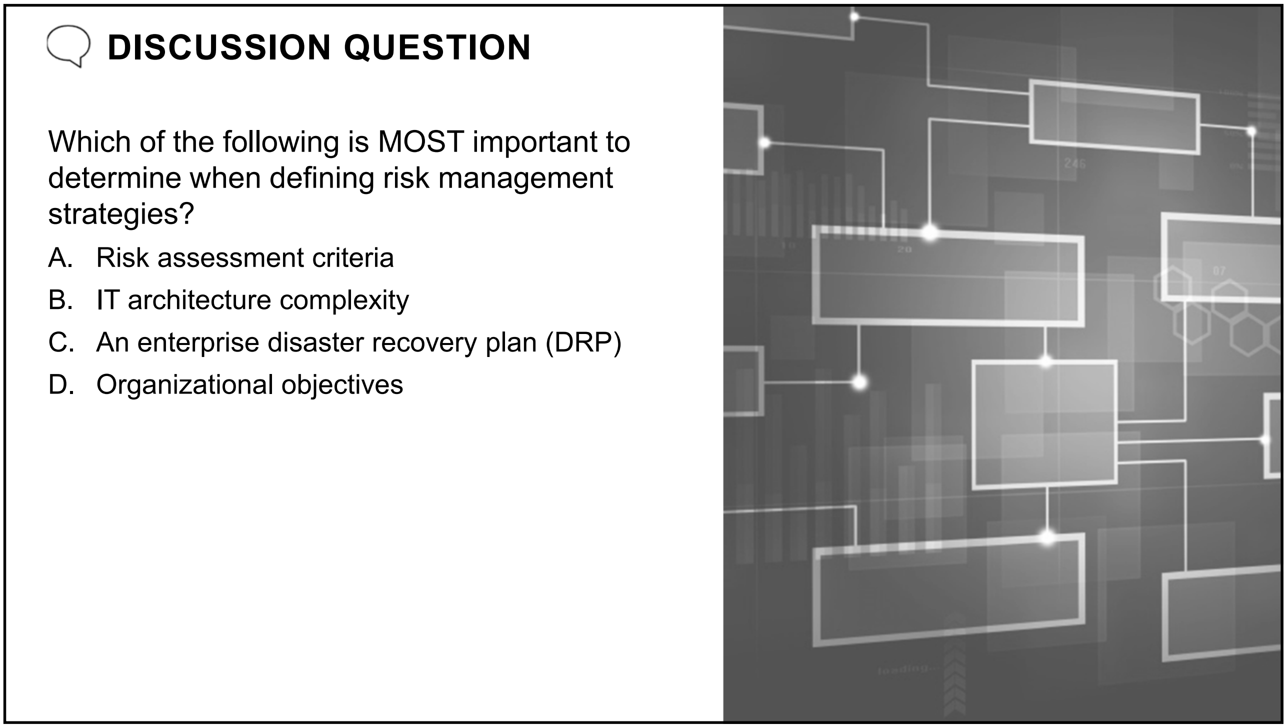
Which of the following is the MOST important information to include in a risk management strategic plan?

A. Risk management staffing requirements

B. The risk management mission statement

C. Risk mitigation investment plans

D. The current state and desired future state



DISCUSSION QUESTION

Which of the following is MOST important to determine when defining risk management strategies?

A. Risk assessment criteria

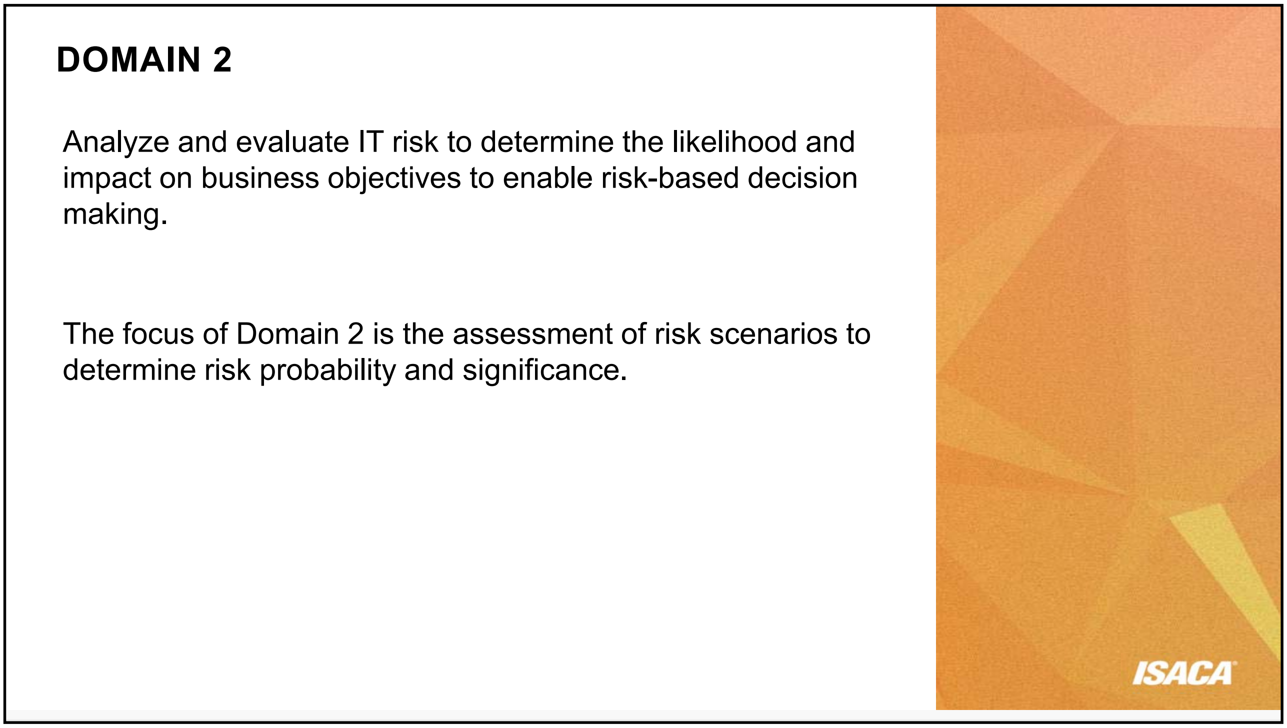
B. IT architecture complexity

C. An enterprise disaster recovery plan (DRP)

D. Organizational objectives

DOMAIN 2

IT RISK ASSESSMENT



DOMAIN 2

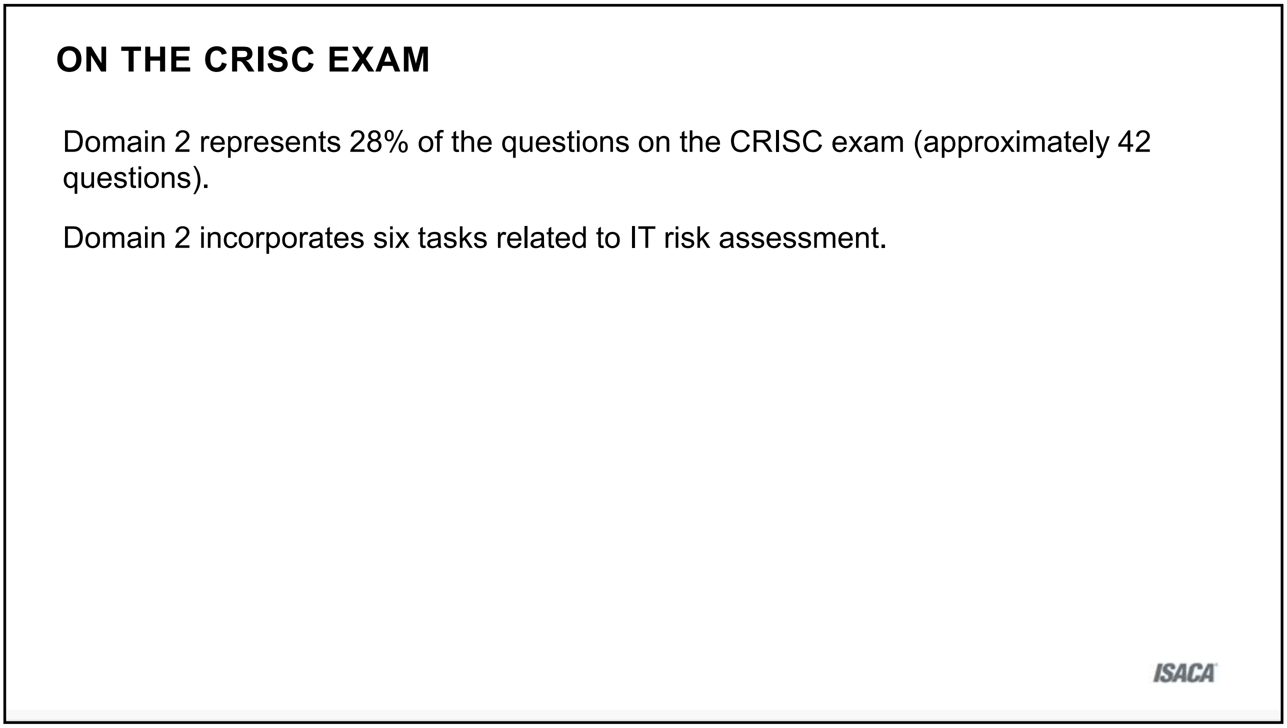
Analyze and evaluate IT risk to determine the likelihood and impact on business objectives to enable risk-based decision making.

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:

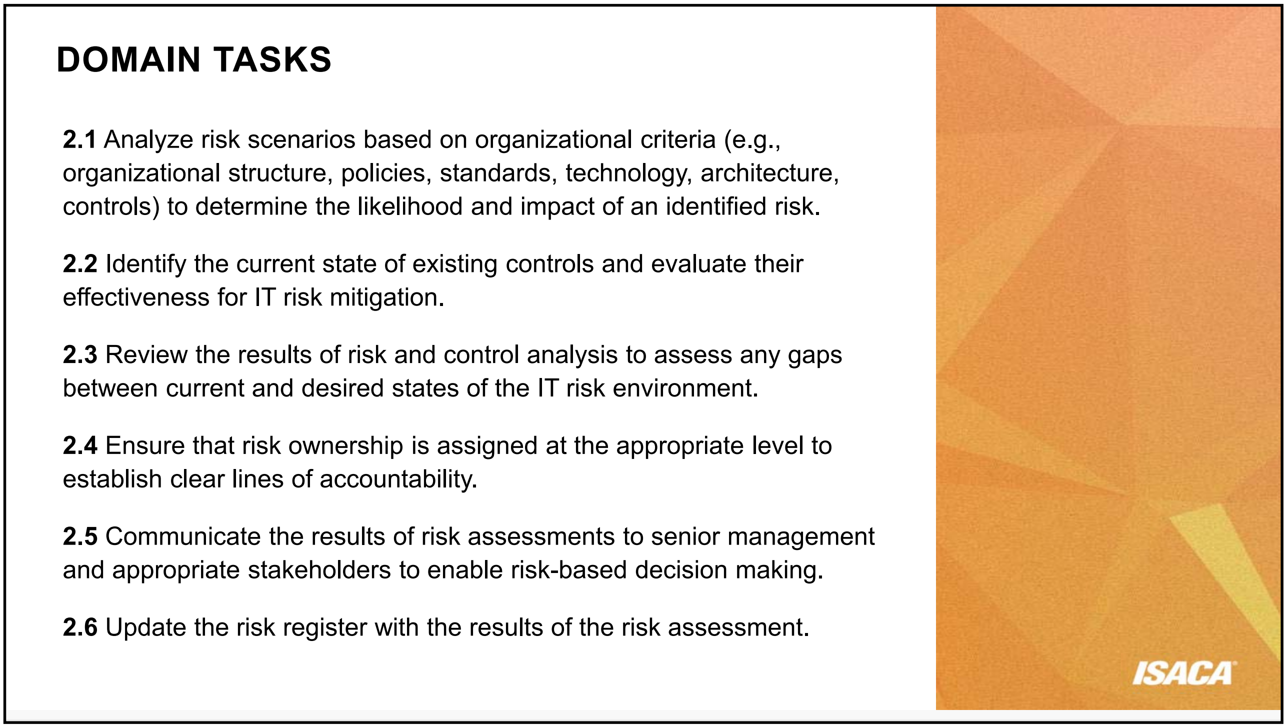
1. Identify and apply risk assessment techniques
2. Analyze risk scenarios
3. Identify current state of controls
4. Assess gaps between current and desired states of the IT risk environment
5. Communicate IT risk assessment results to relevant stakeholders



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.

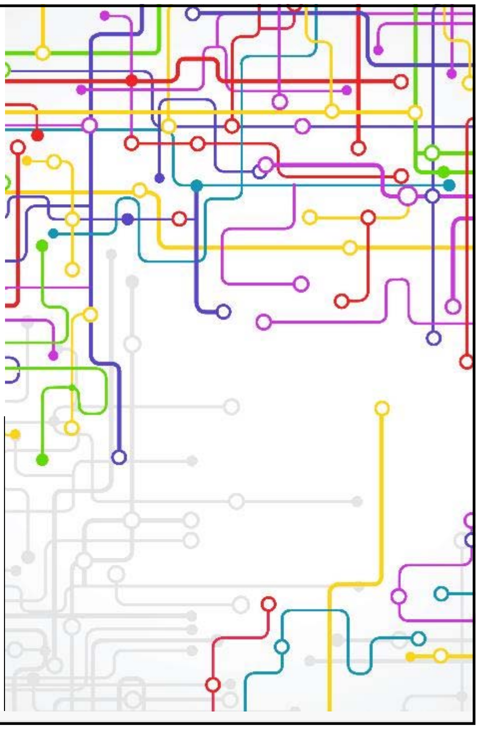
2.5 Communicate the results of risk assessments to senior management and appropriate stakeholders to enable risk-based decision making.

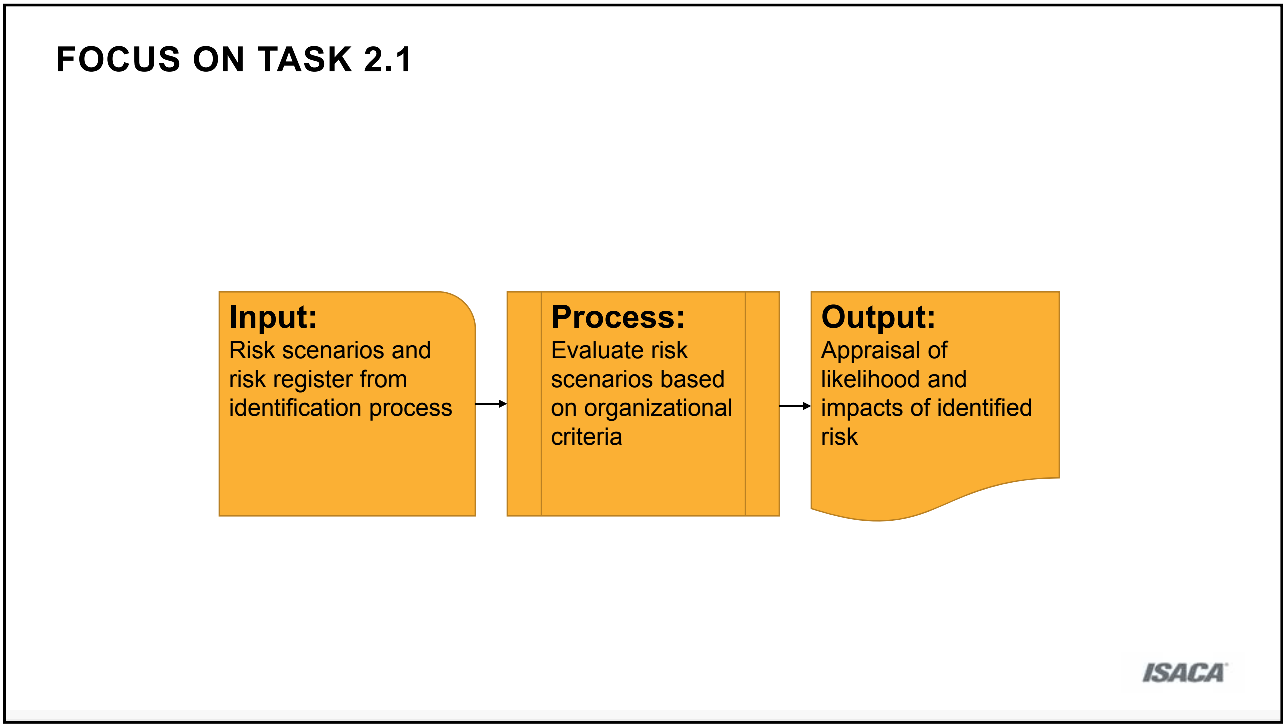
2.6 Update the risk register with the results of the risk assessment.

ISACA

TASK 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.



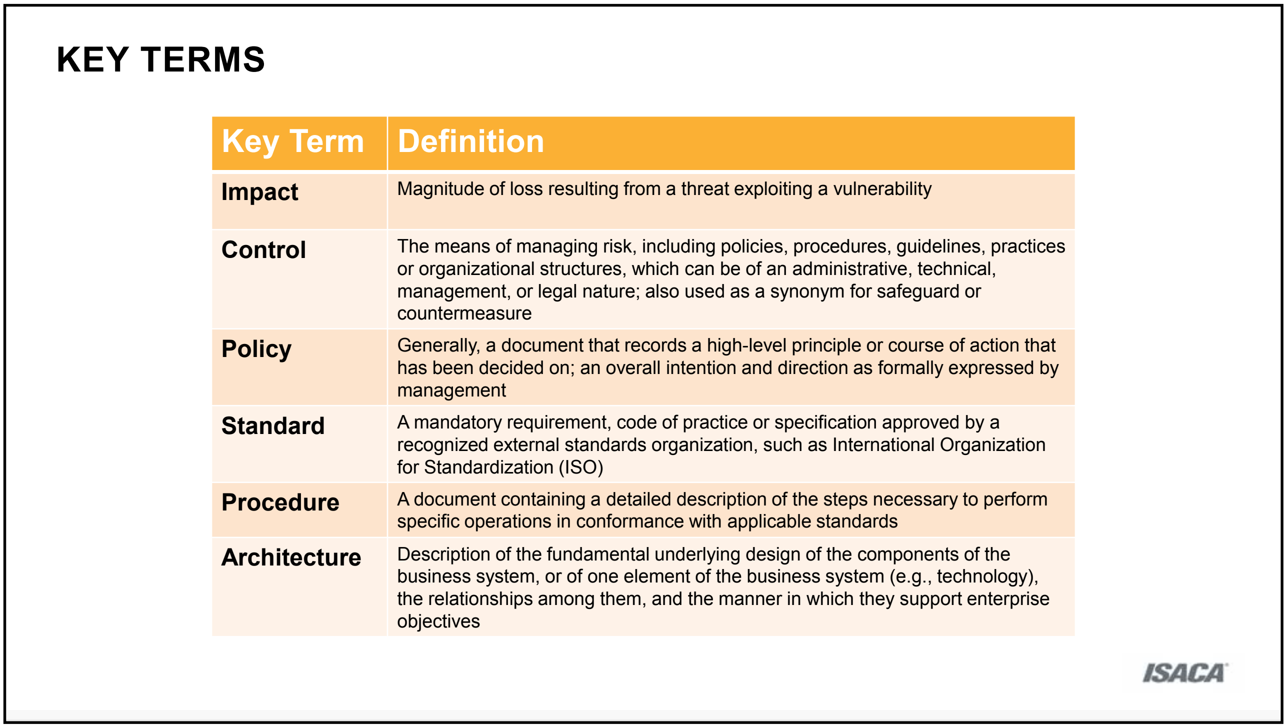


FOCUS ON TASK 2.1

Input:
Risk scenarios and risk register from identification process

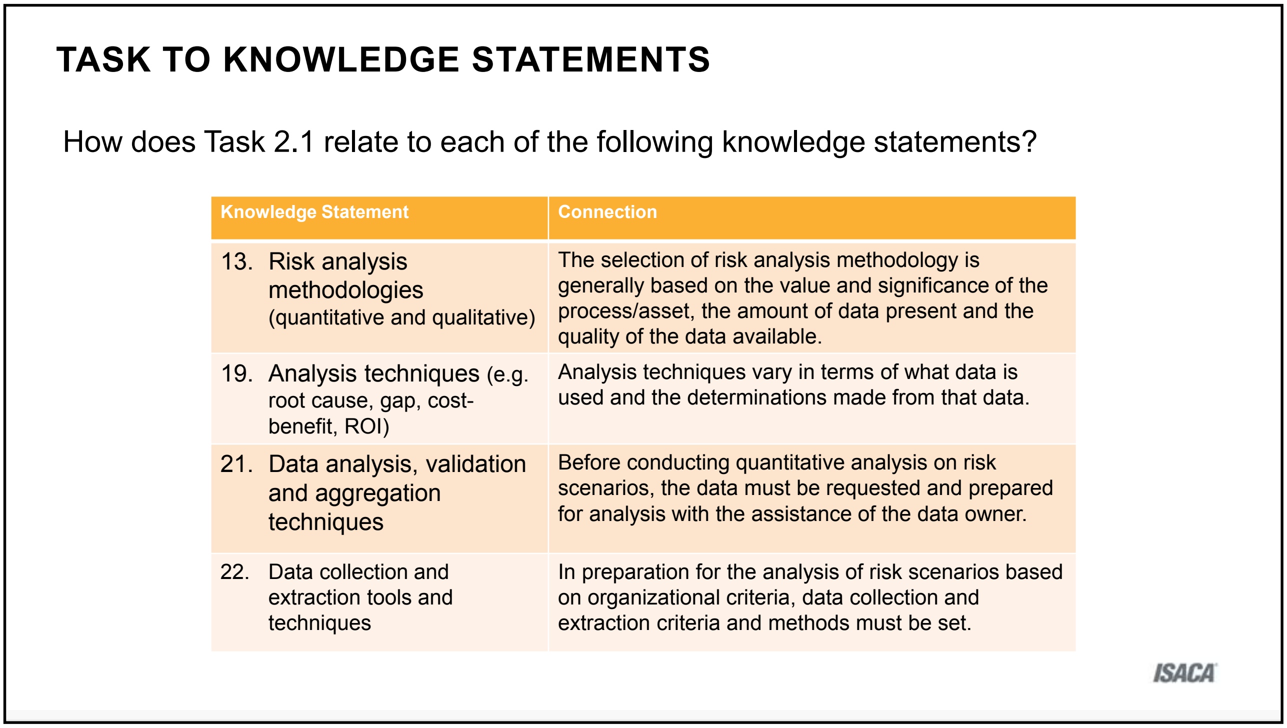
Process:
Evaluate risk scenarios based on organizational criteria

Output:
Appraisal of likelihood and impacts of identified risk



KEY TERMS

Key Term	Definition
Impact	Magnitude of loss resulting from a threat exploiting a vulnerability
Control	The means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, technical, management, or legal nature; also used as a synonym for safeguard or countermeasure
Policy	Generally, a document that records a high-level principle or course of action that has been decided on; an overall intention and direction as formally expressed by management
Standard	A mandatory requirement, code of practice or specification approved by a recognized external standards organization, such as International Organization for Standardization (ISO)
Procedure	A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards
Architecture	Description of the fundamental underlying design of the components of the business system, or of one element of the business system (e.g., technology), the relationships among them, and the manner in which they support enterprise objectives

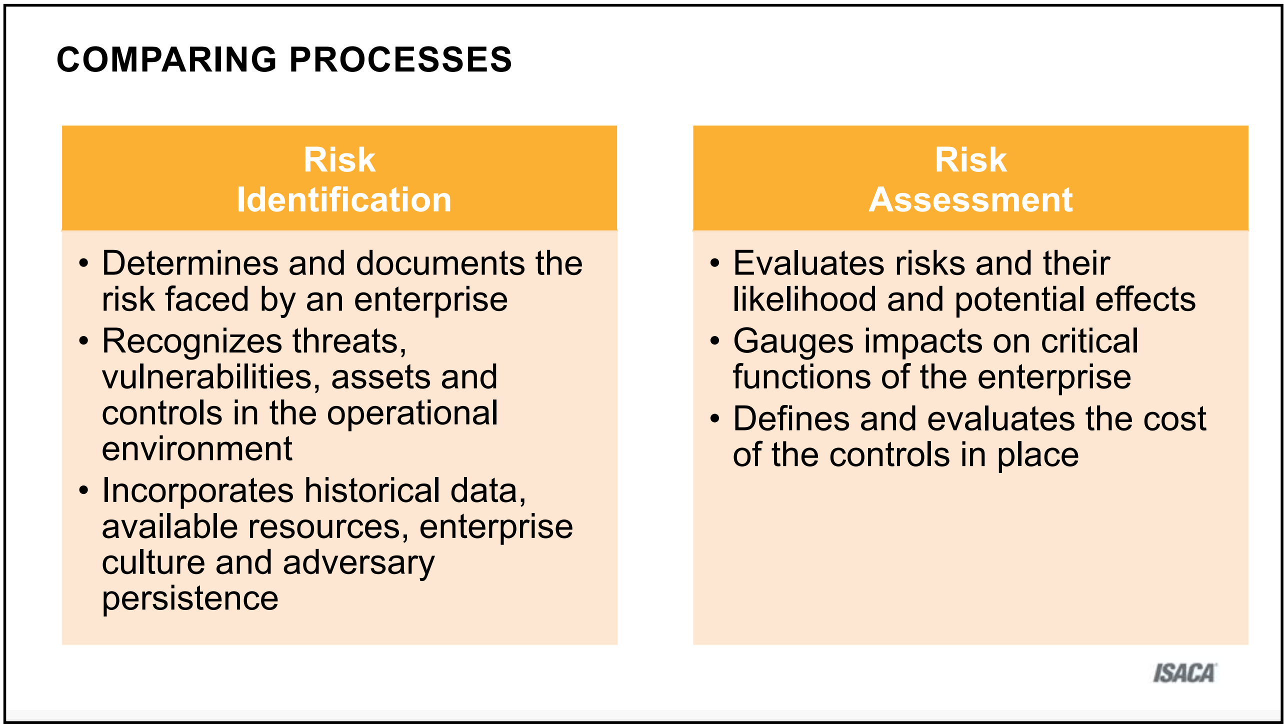


TASK TO KNOWLEDGE STATEMENTS

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.

ISACA



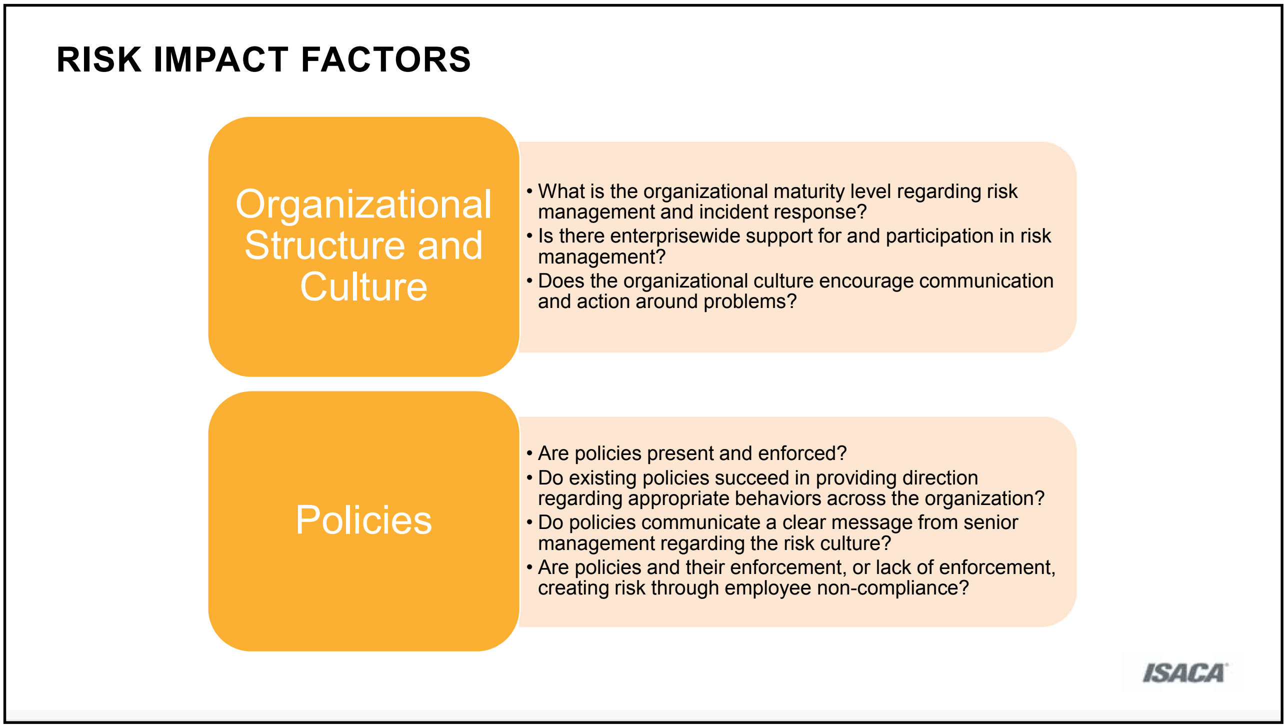
COMPARING PROCESSES

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



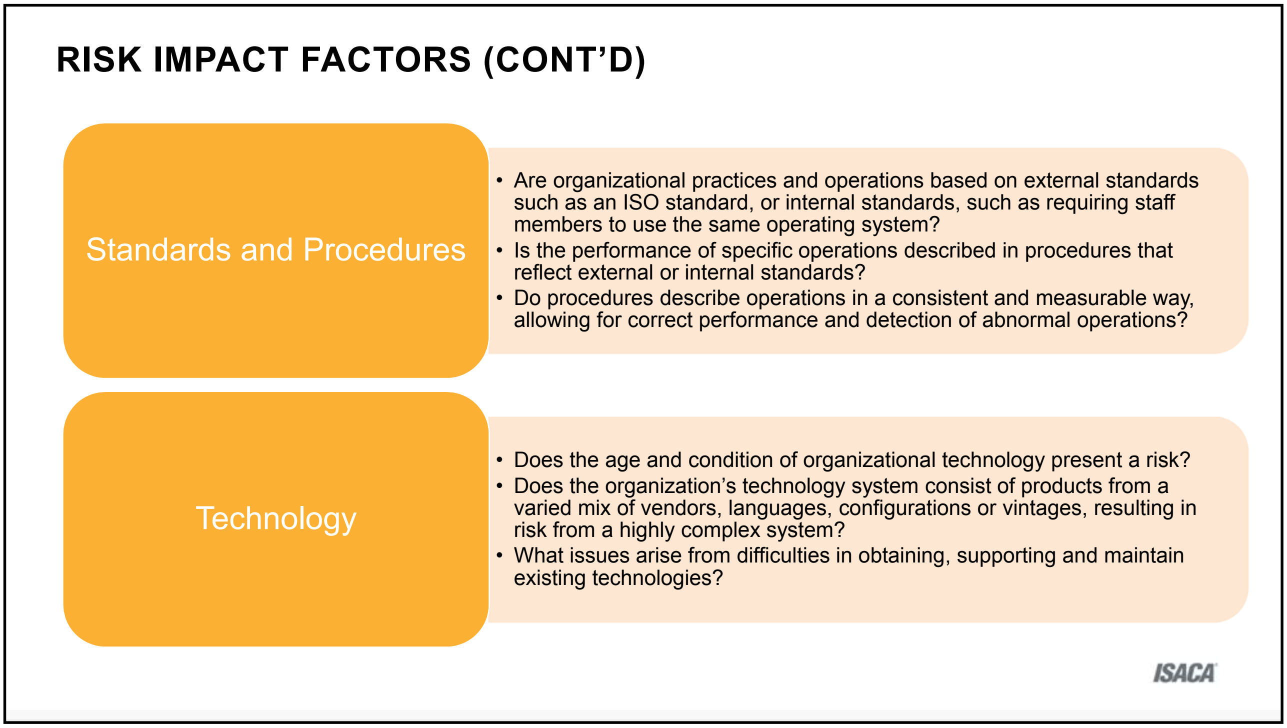
RISK IMPACT FACTORS

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?



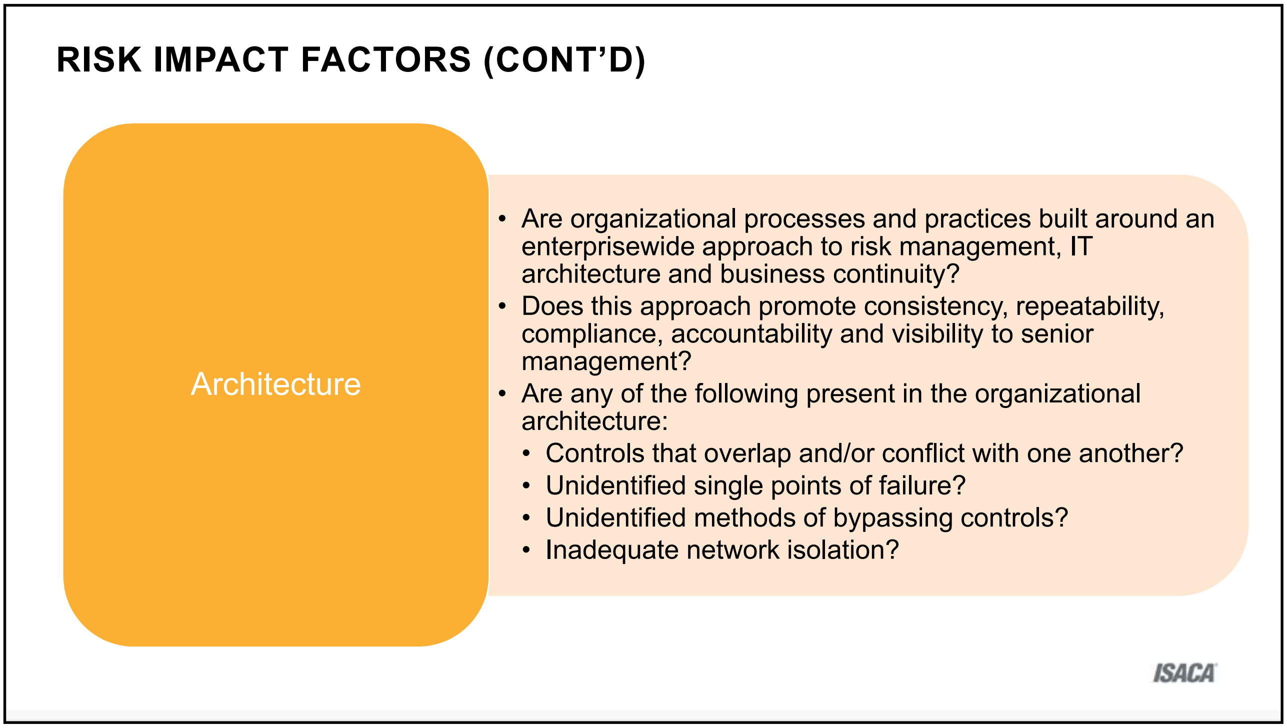
RISK IMPACT FACTORS (CONT'D)

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

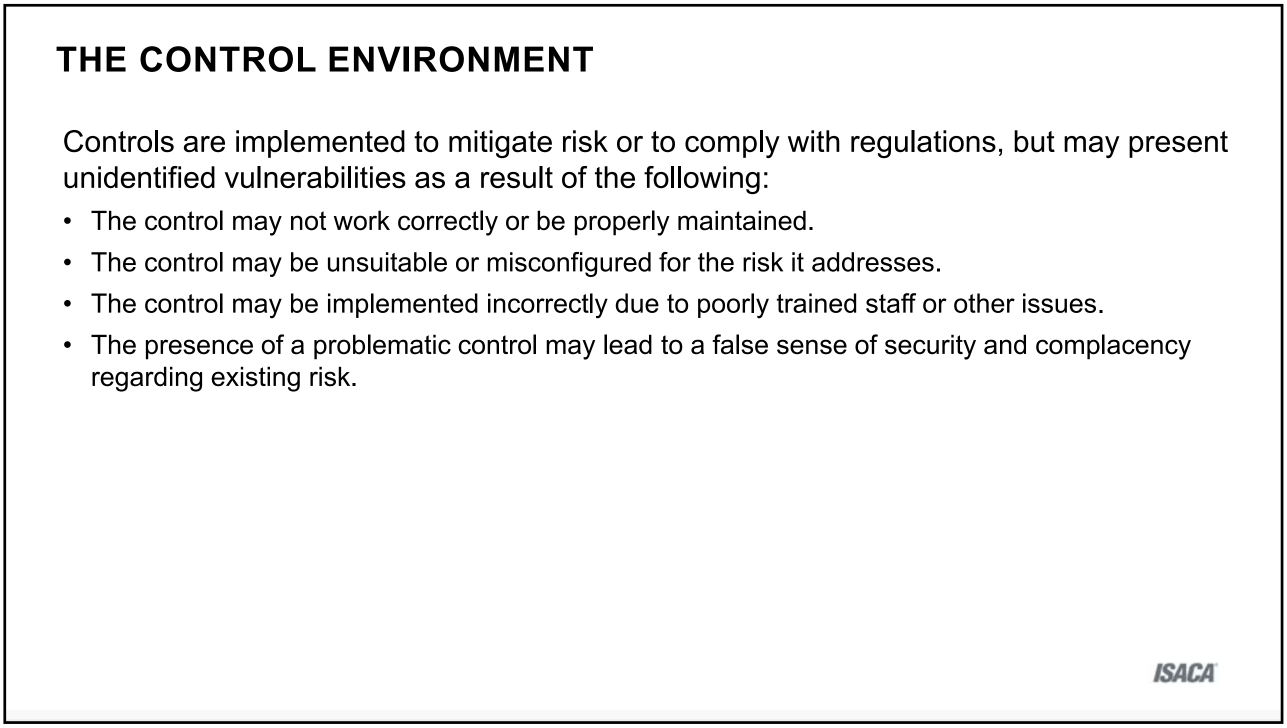
- Does the age and condition of organizational technology present a risk?
- Does the organization's technology system consist of products from a varied mix of vendors, languages, configurations or vintages, resulting in risk from a highly complex system?
- What issues arise from difficulties in obtaining,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



RISK IMPACT FACTORS (CONT'D)

Architecture

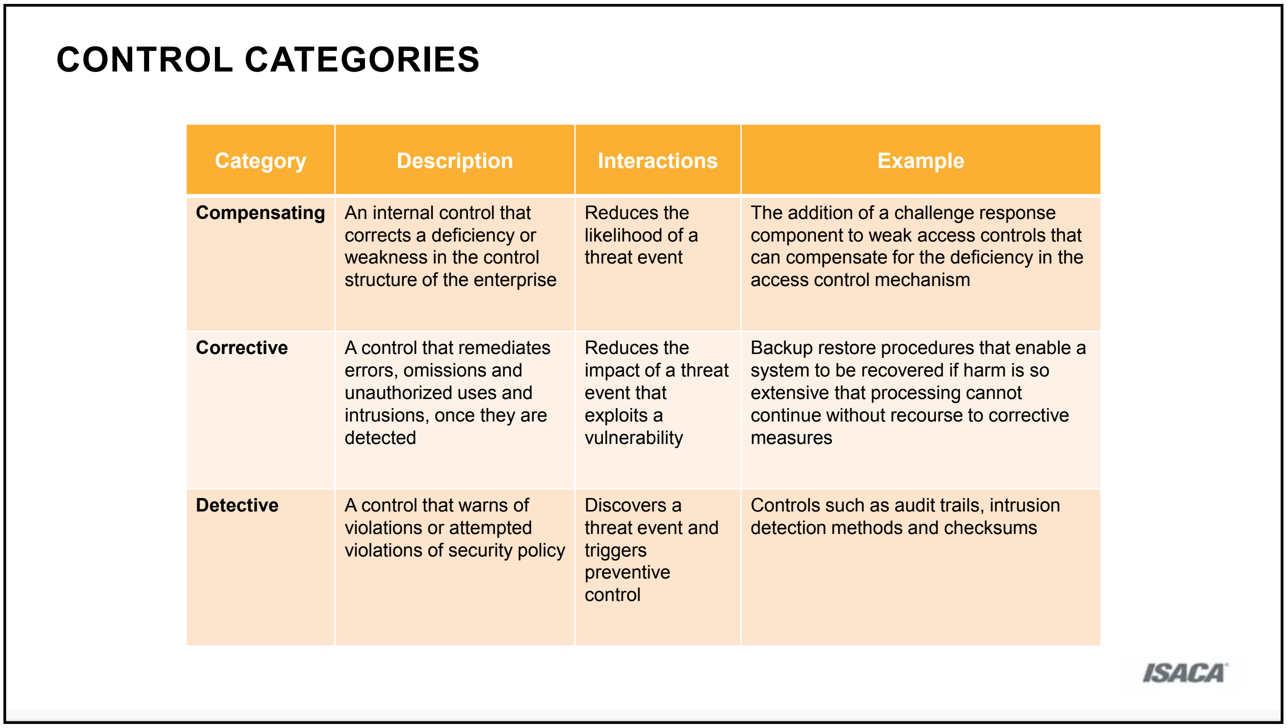
- Are organizational processes and practices built around an enterprisewide approach to risk management, IT architecture and business continuity?
- Does this approach promote consistency, repeatability, compliance, accountability and visibility to senior management?
- Are any of the following present 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:

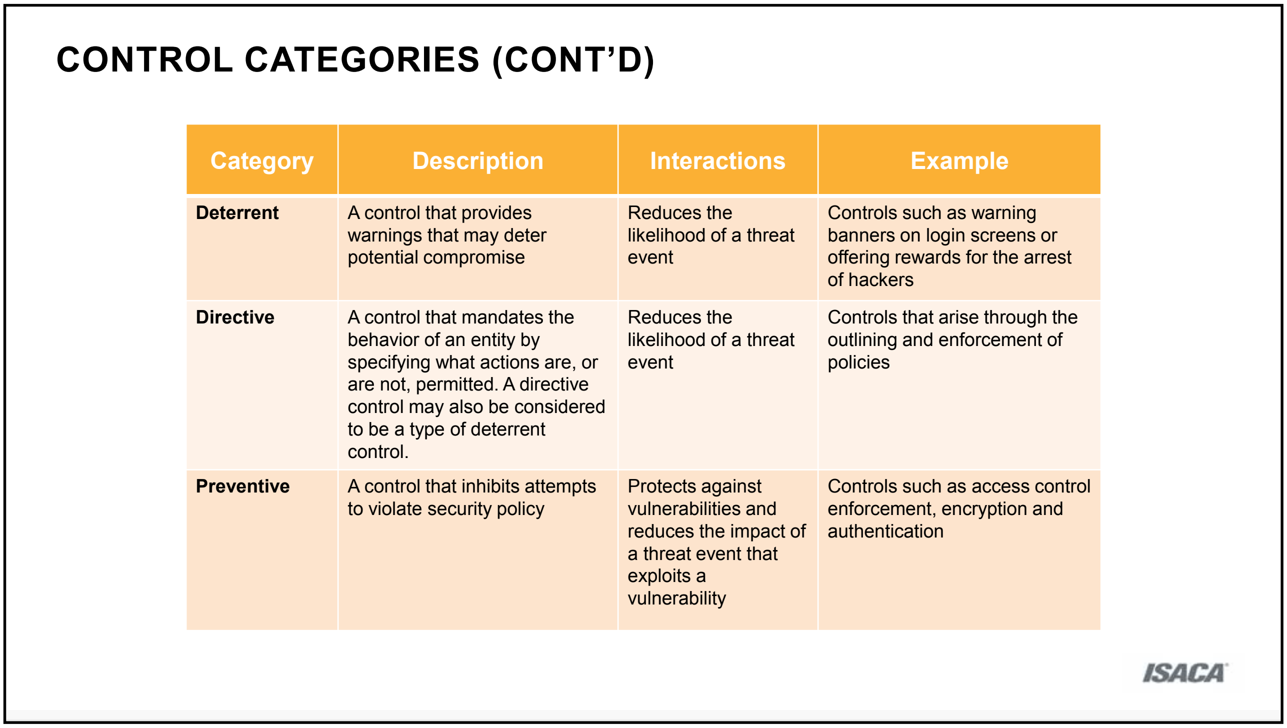
- The control may not work correctly or be properly maintained.
- The control may be unsuitable or misconfigured for the risk it addresses.
- The control may be implemented incorrectly due to poorly trained staff or other issues.
- The presence of a problematic control may lead to a false sense of security and complacency regarding existing risk.



CONTROL CATEGORIES

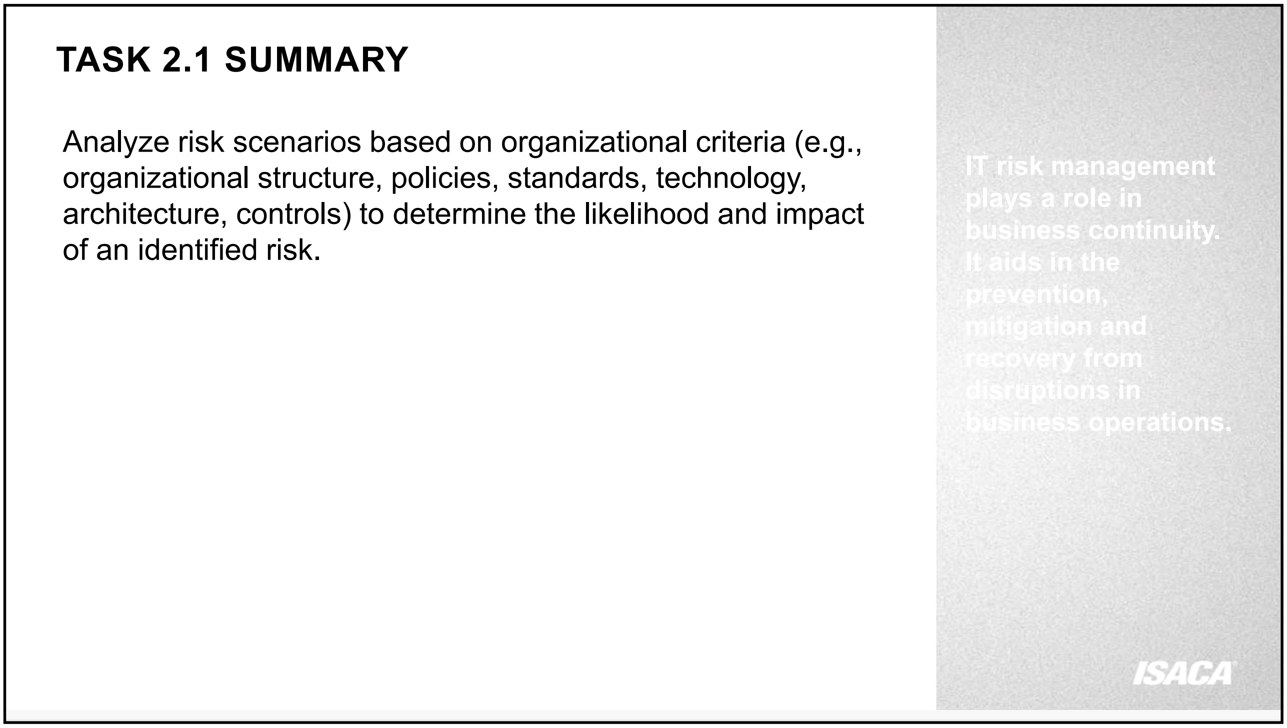
Category	Description	Interactions	Example
Compensating	An internal control that corrects a deficiency or weakness in the control structure of the enterprise	Reduces the likelihood of a threat event	The addition of a challenge response component to weak access controls that can compensate for the deficiency 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

ISACA



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



TASK 2.1 SUMMARY

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.

IT risk management plays a role in business continuity. It aids in the prevention, mitigation and recovery from disruptions in business operations.

TASK 2.1 DISCUSSION

There have been several high-profile events related to IT-risk in the news recently. Some examples include the U.S. Office of Personnel Management data breach, the Sony Wiper virus challenge and the Target data breach.

Discuss the ways in which the organizational criteria we've just discussed can be seen to have played a role in one of these events.

DISCUSSION QUESTION

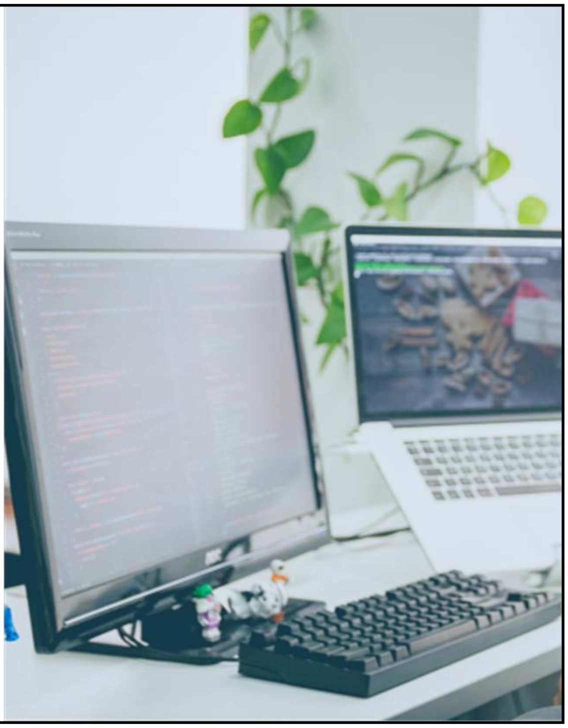
Which of the following BEST ensures that identified risk is kept at an acceptable level?

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.

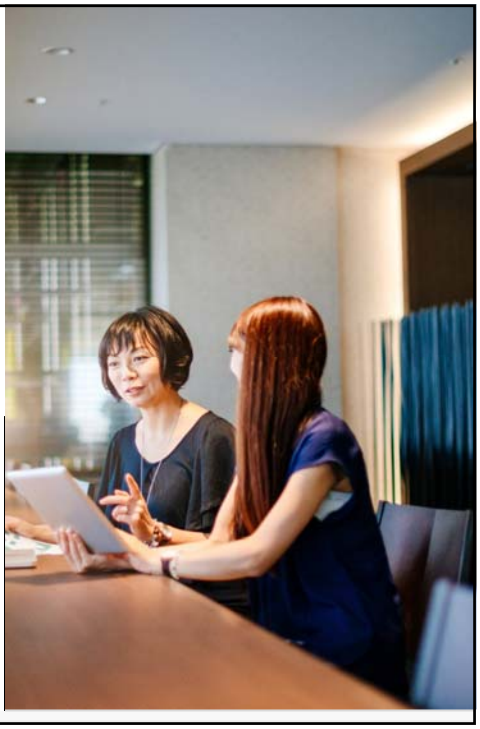
B. policies and standards.

C. recent audit findings and recommendations.

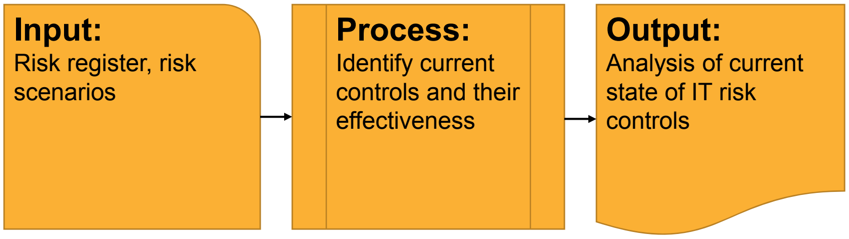
D. system and its subsystems.

TASK 2.2

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



FOCUS ON TASK 2.2

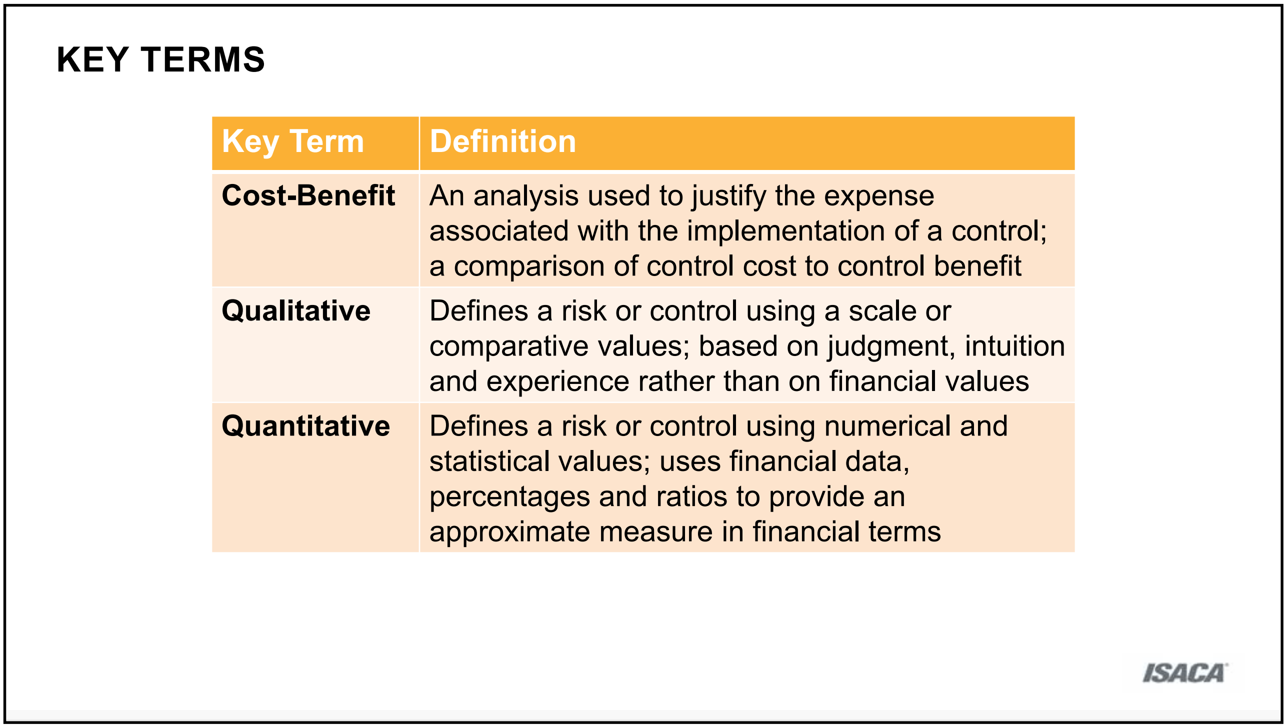


Input: Risk register, risk scenarios

Process: Identify current controls and their effectiveness

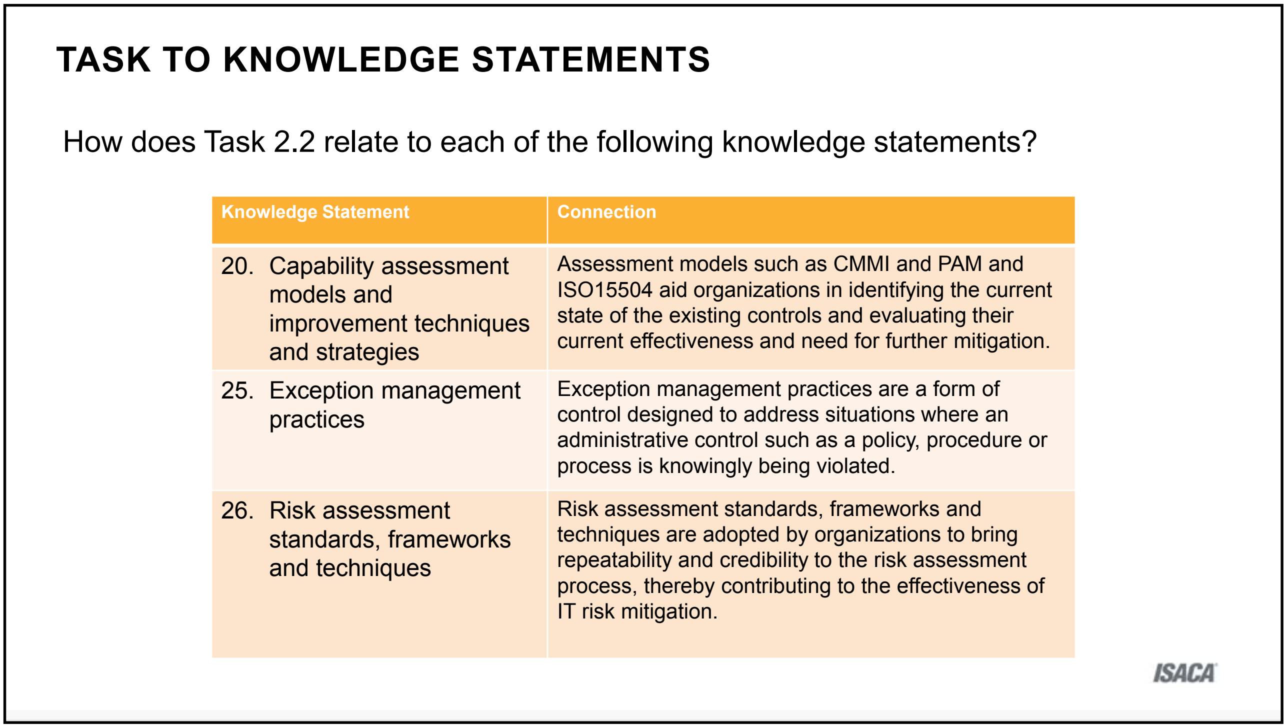
Output: Analysis of current state of IT risk controls

ISACA



KEY TERMS

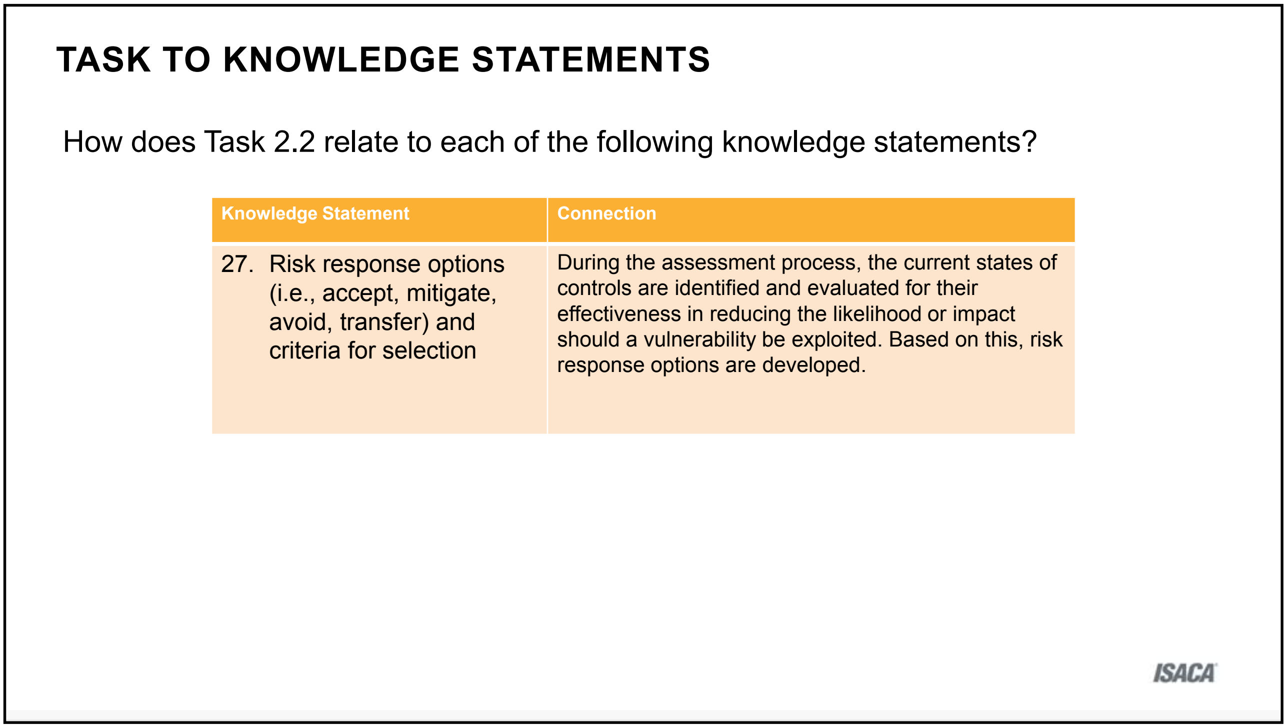
Key Term	Definition
Cost-Benefit	An analysis used to justify the expense associated with the implementation of a control; a comparison of control cost to control benefit
Qualitative	Defines a risk or control using a scale or comparative values; based on judgment, intuition and experience rather than on financial values
Quantitative	Defines a risk or control using numerical and statistical values; uses financial data, percentages and ratios to provide an approximate measure in financial terms



TASK TO KNOWLEDGE STATEMENTS

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

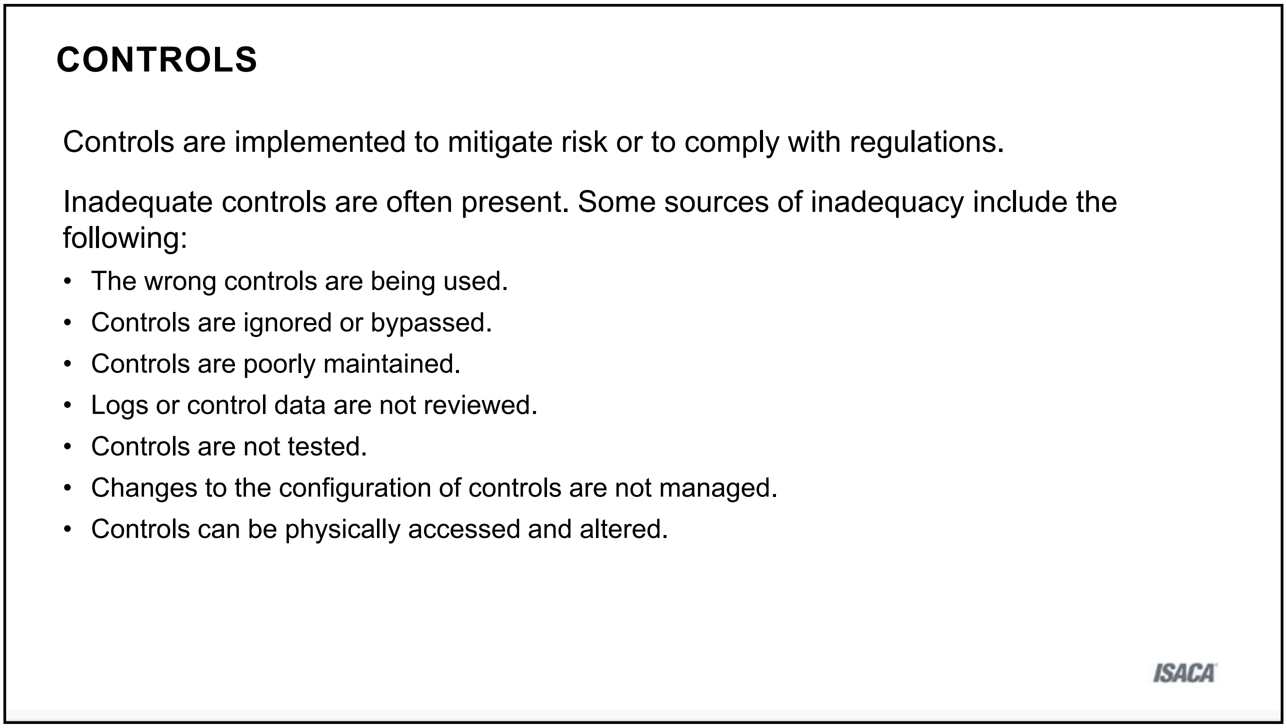
Knowledge Statement	Connection
20. Capability assessment models and improvement techniques and strategies	Assessment models such as CMMI and PAM and ISO15504 aid organizations in identifying the current state of the existing controls and evaluating their current effectiveness and need for further mitigation.
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

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.

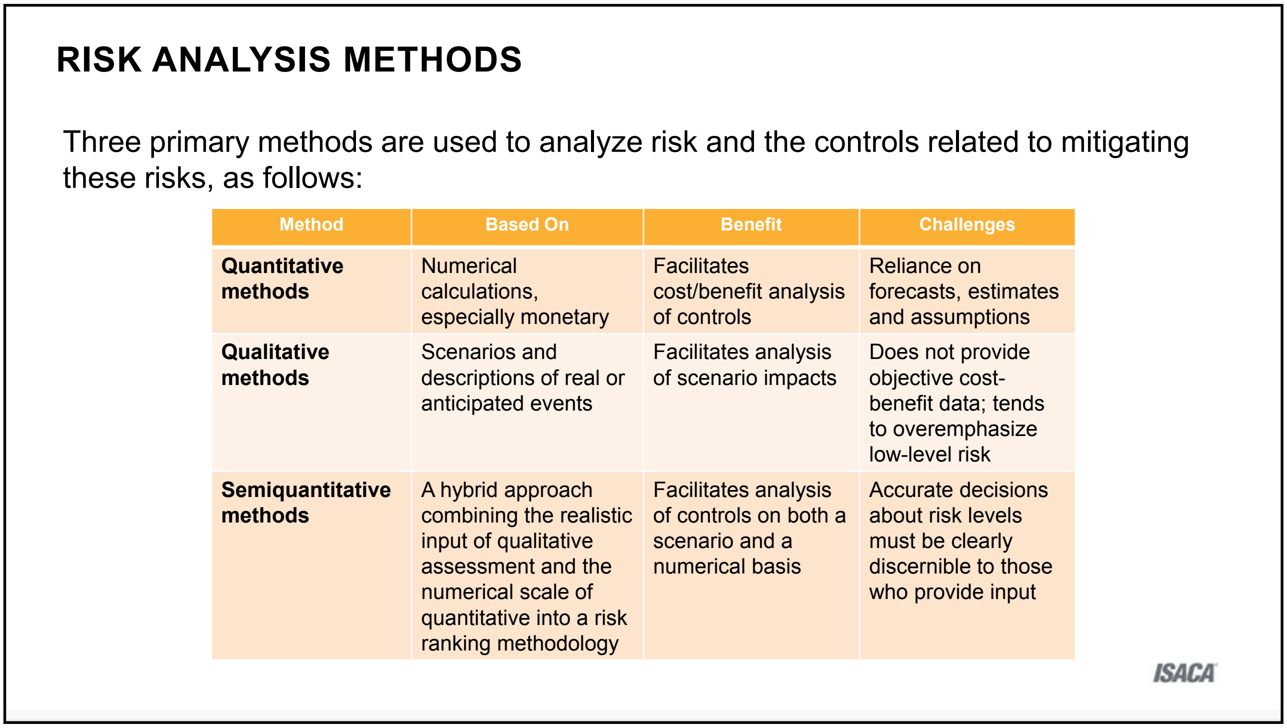


CONTROLS

Controls are implemented to mitigate risk or to comply with regulations.

Inadequate controls are often present. Some sources of inadequacy include the following:

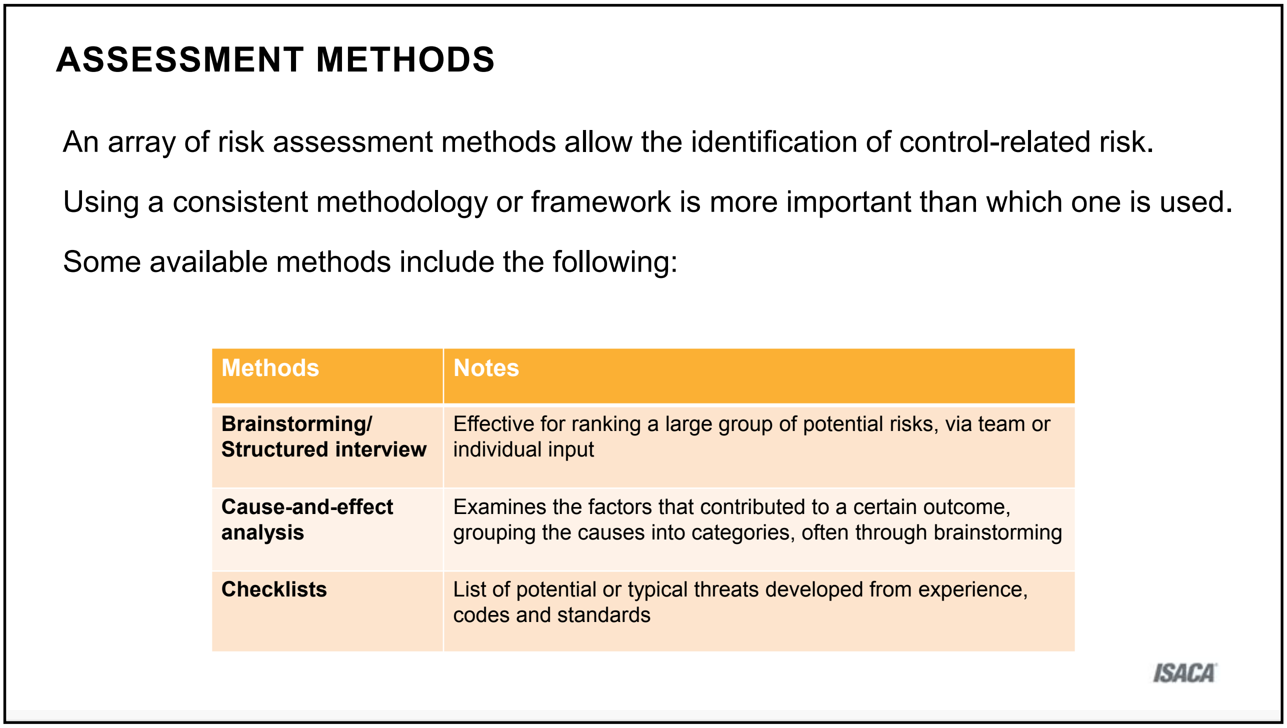
- The wrong controls are being used.
- Controls are ignored or bypassed.
- Controls are poorly maintained.
- Logs or control data are not reviewed.
- Controls are not tested.
- Changes to the configuration of controls are not managed.
- Controls can be physically accessed and altered.



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.

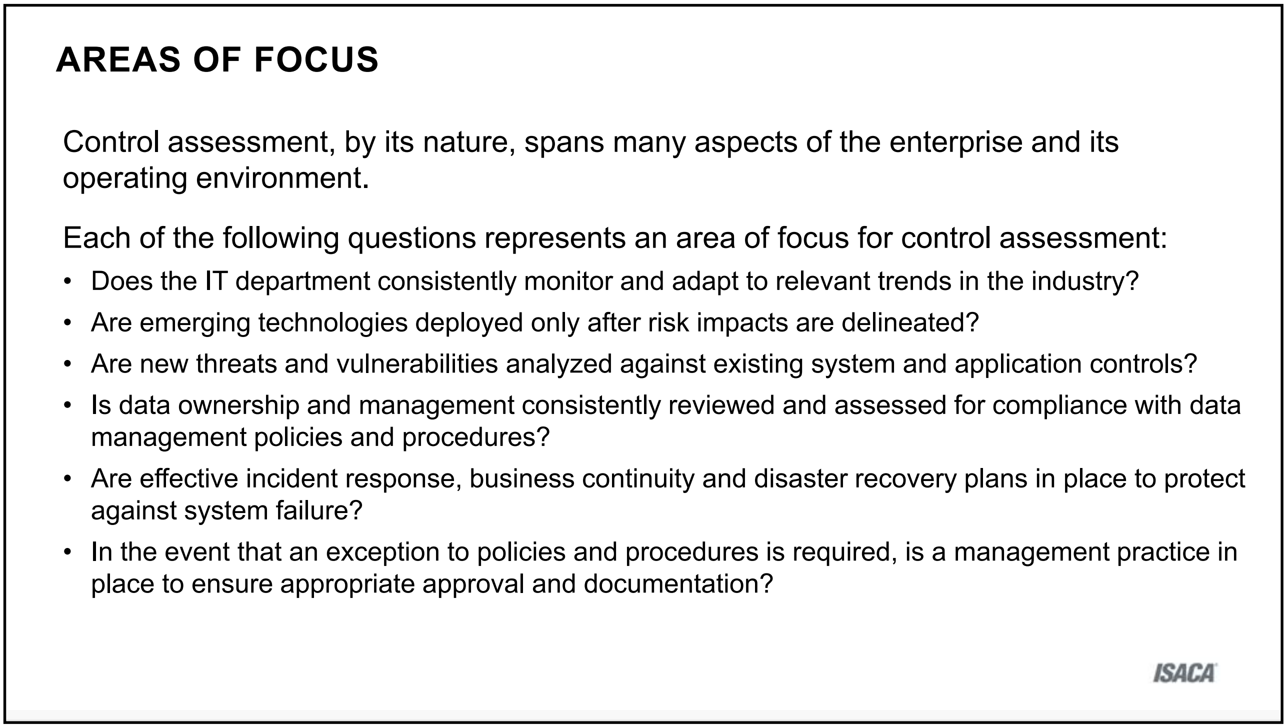
Using a consistent methodology or framework is more important than which one is used.

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.

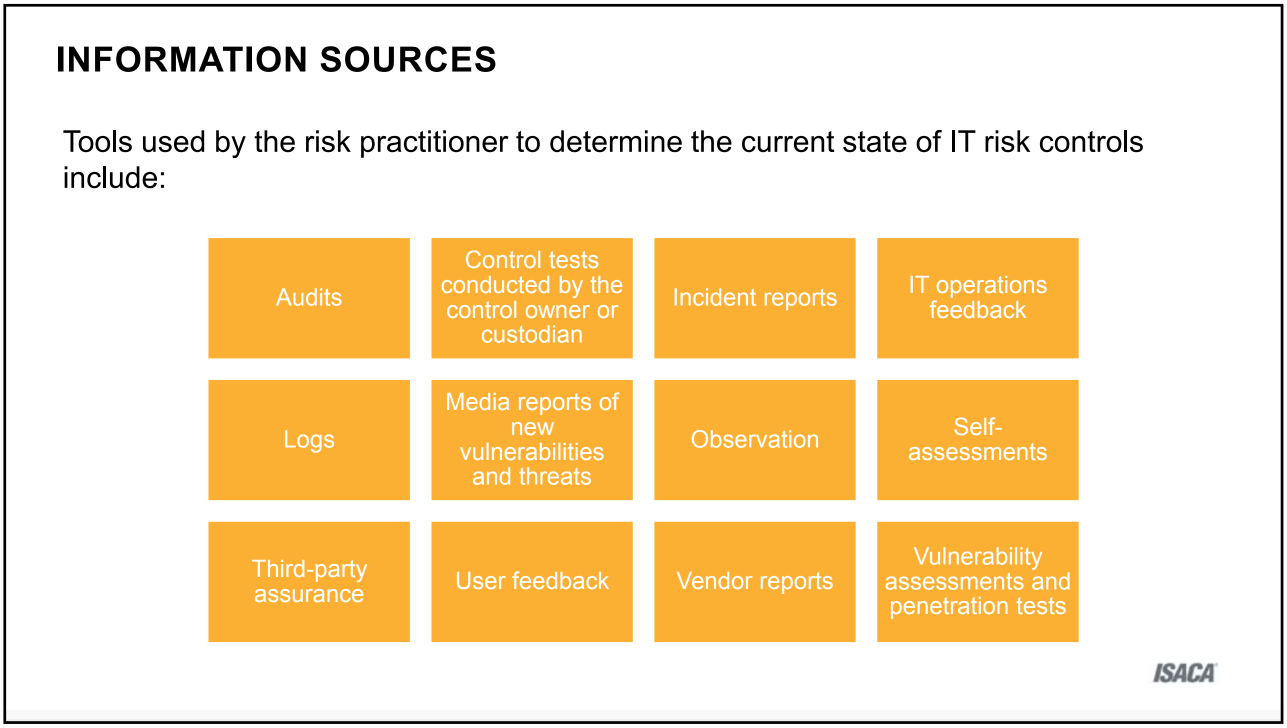


AREAS OF FOCUS

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?

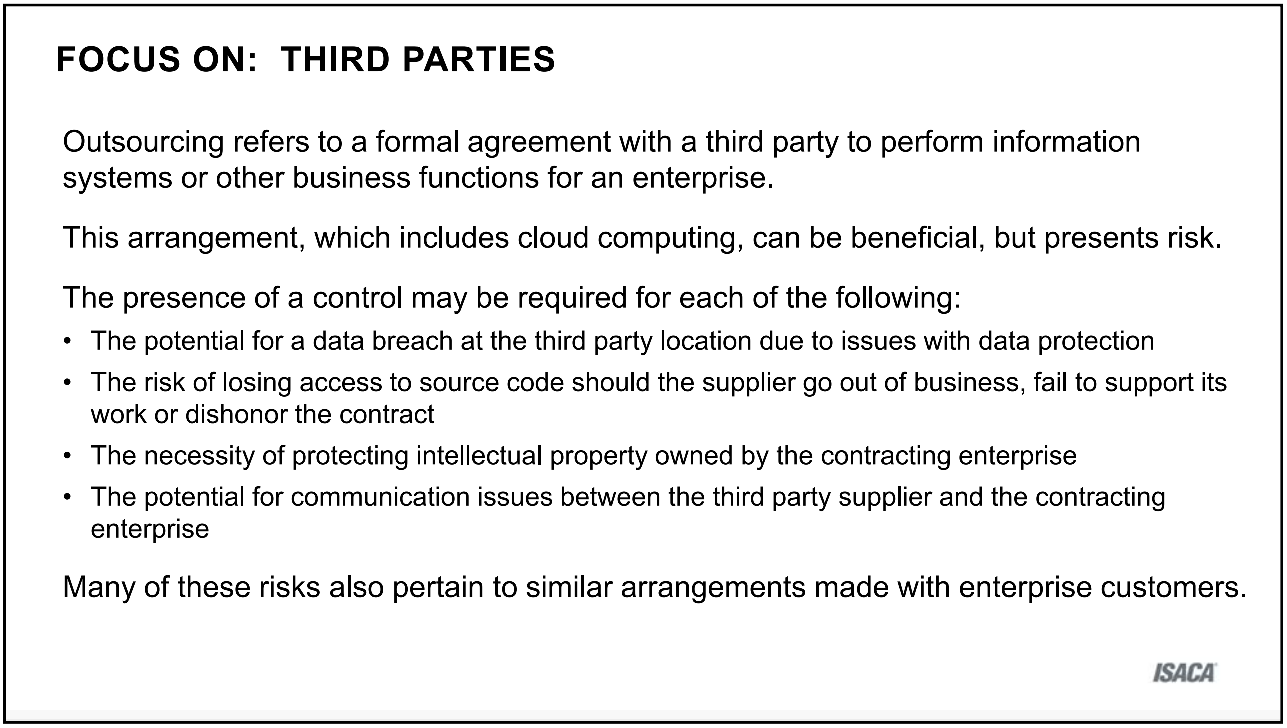


INFORMATION SOURCES

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

ISACA



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.

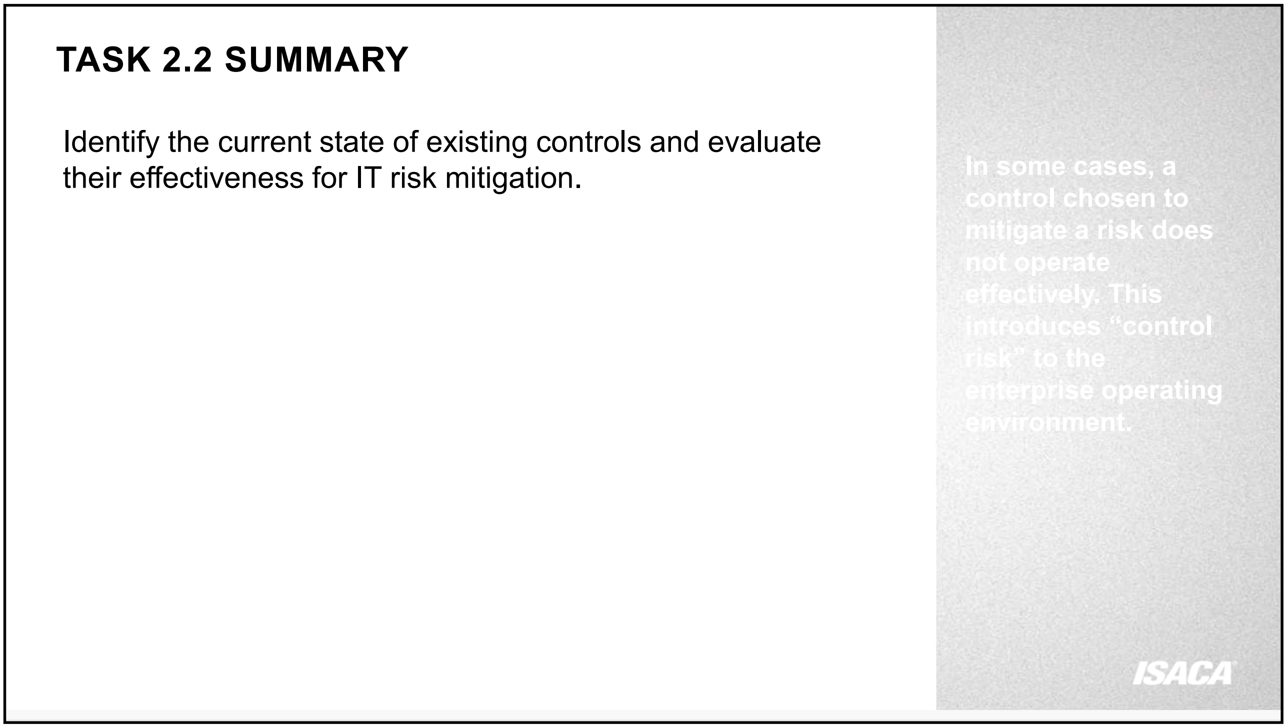
This arrangement, which includes cloud computing, can be beneficial, but presents risk.

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.

ISACA



TASK 2.2 SUMMARY

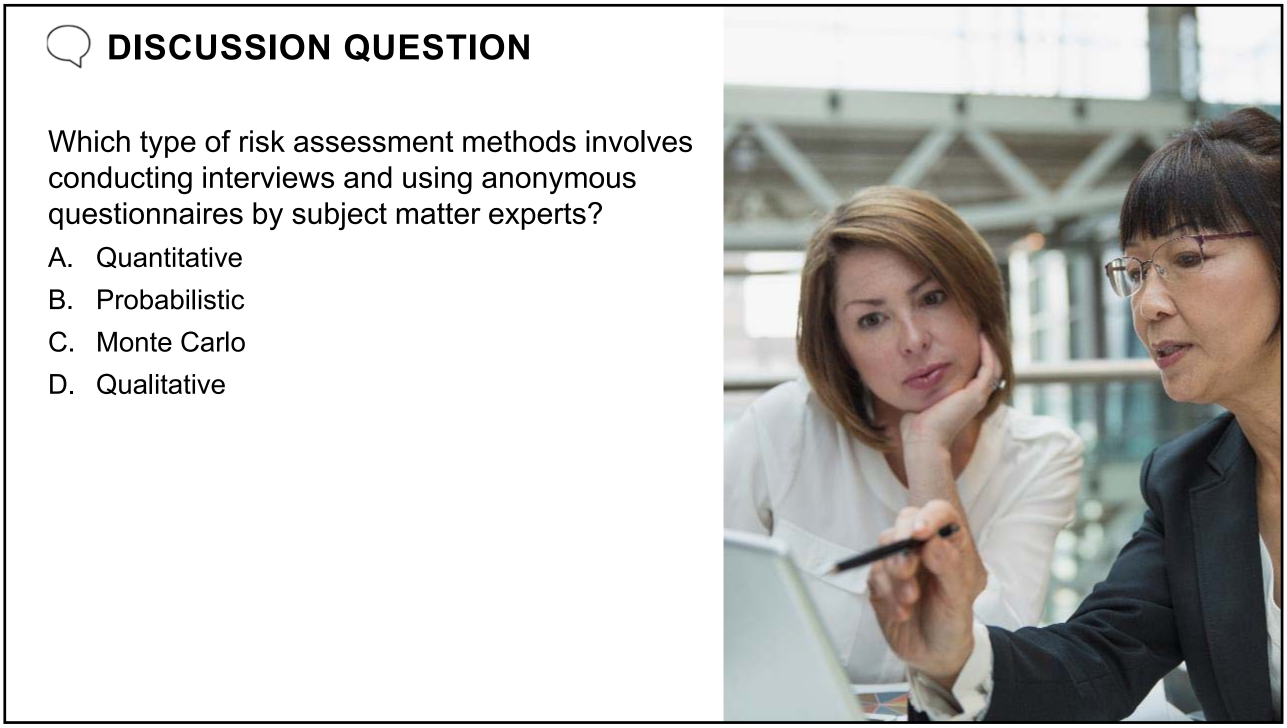
Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation.

In some cases, a control chosen to mitigate a risk does not operate effectively. This introduces “control risk” to the enterprise operating environment.

TASK 2.2 DISCUSSION

How do tool selection and implementation factor into network protection? Why are they a main consideration?

Discuss the importance of key security controls.



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

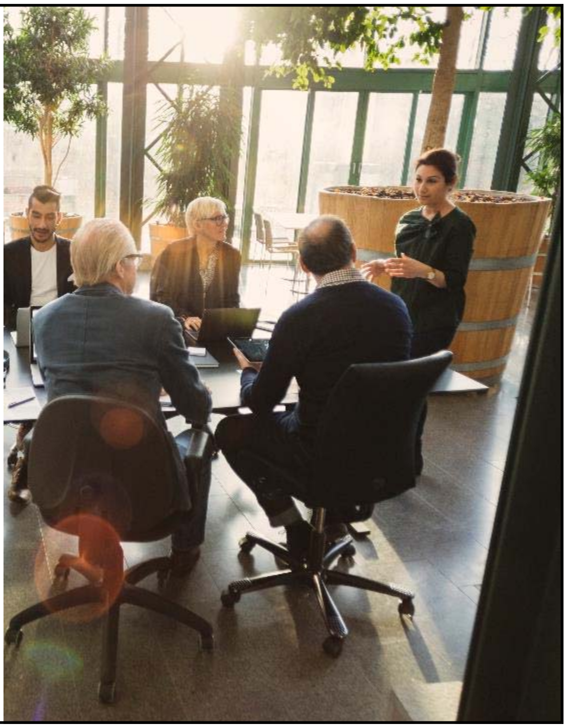
The board of directors wants to know the financial impact of specific, individual risk scenarios. What type of approach is BEST suited to fulfill this requirement?

A. Delphi method

B. Quantitative analysis

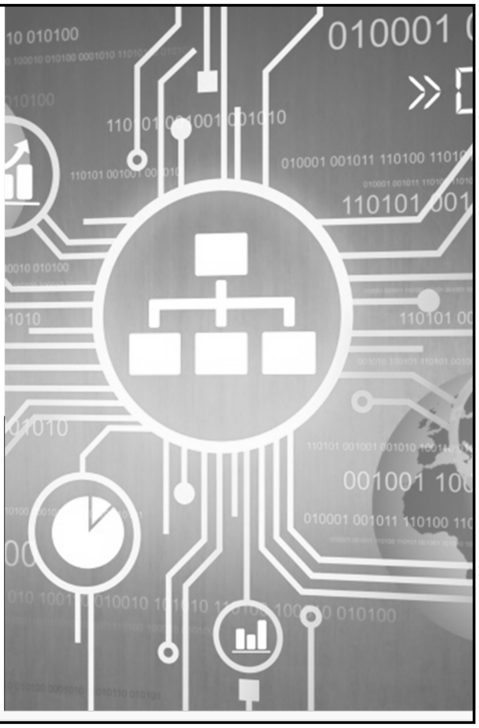
C. Qualitative analysis

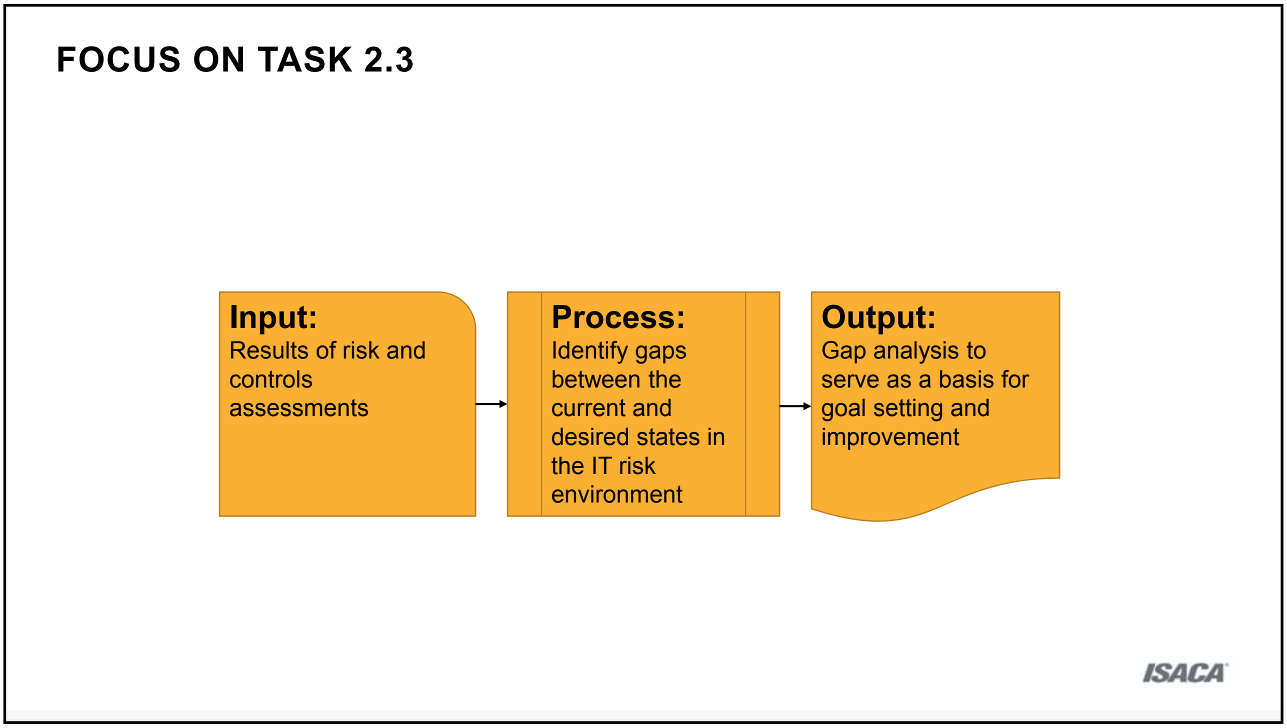
D. Financial risk modeling



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.



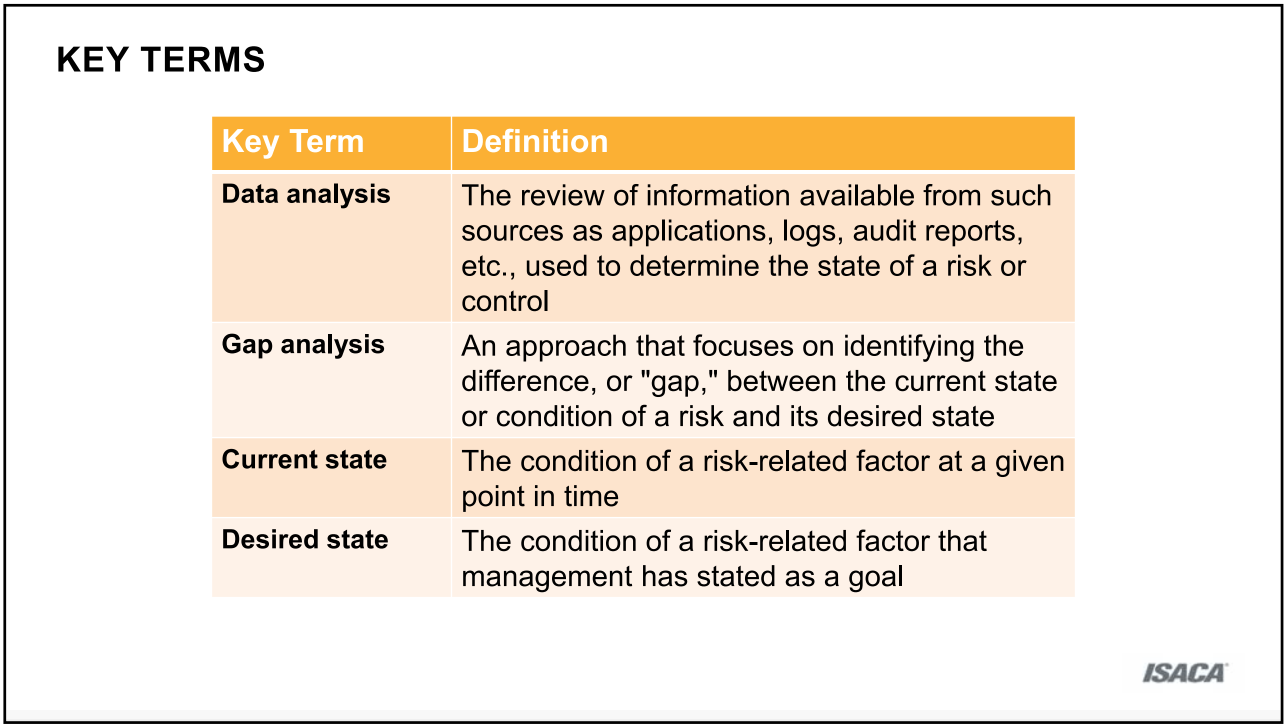


FOCUS ON TASK 2.3

Input:
Results of risk and controls assessments

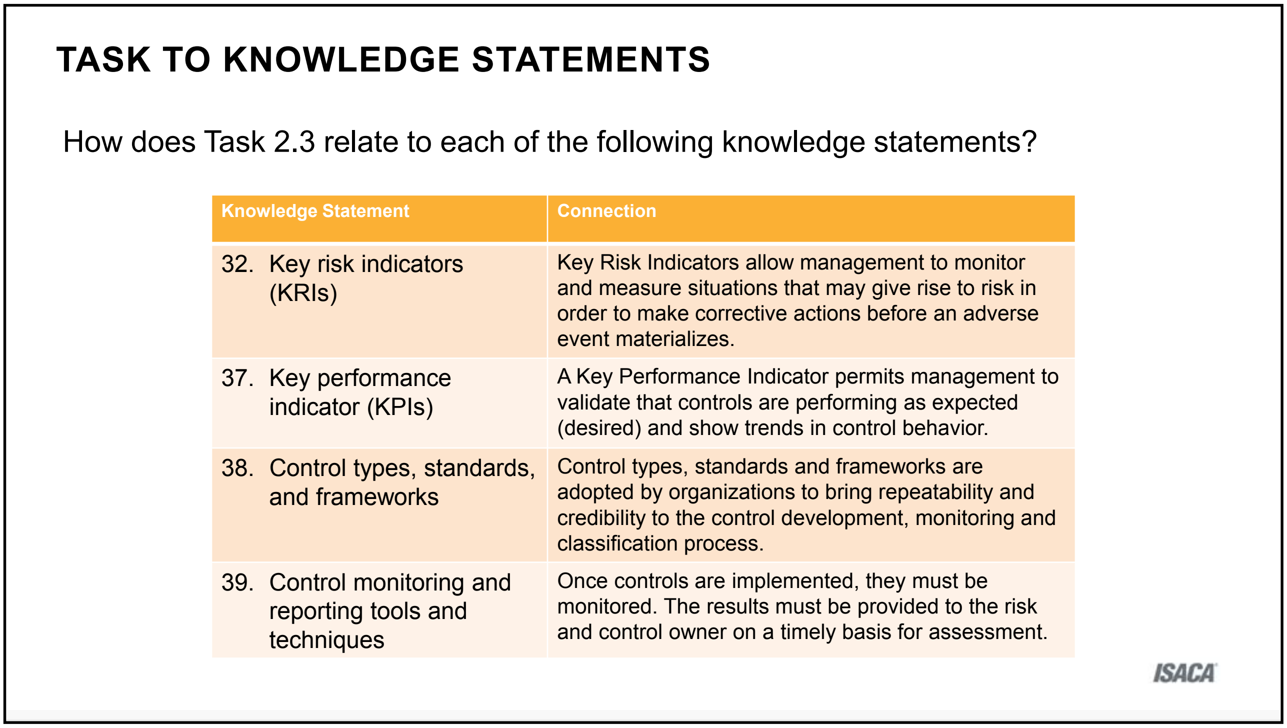
Process:
Identify gaps between the current and desired states in the IT risk environment

Output:
Gap analysis to serve as a basis for goal setting and improvement



KEY TERMS

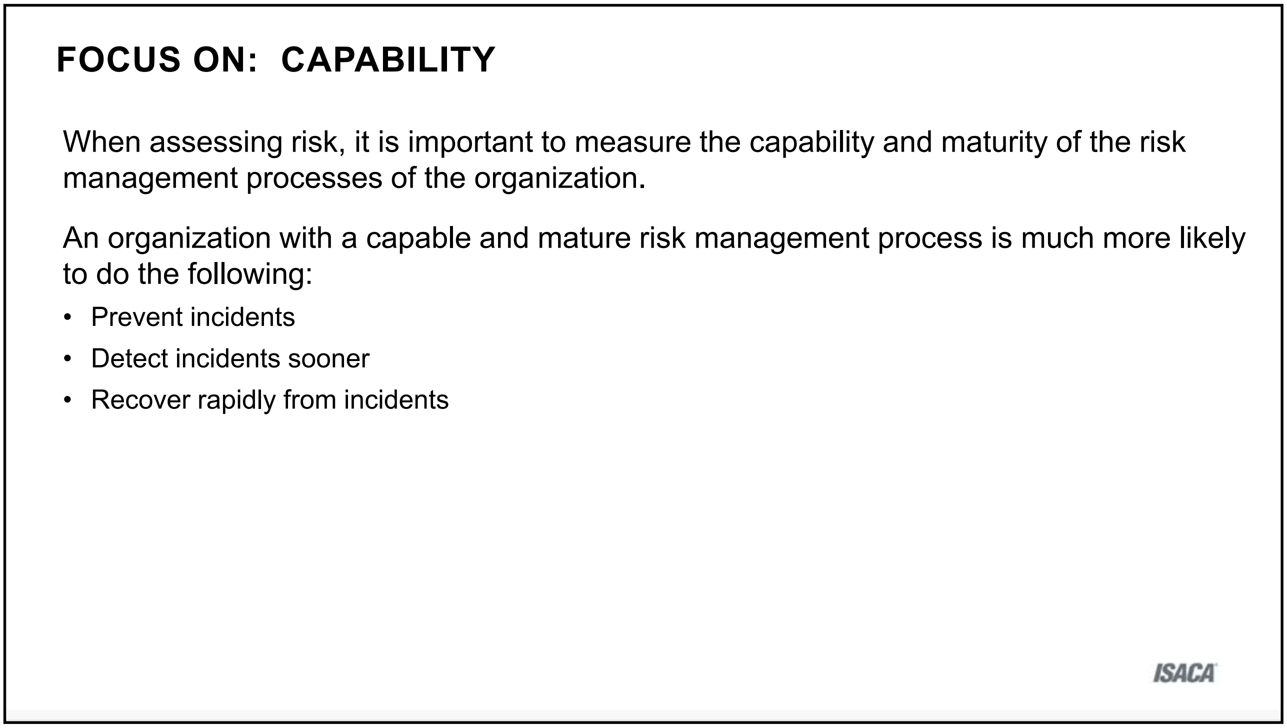
Key Term	Definition
Data analysis	The review of information available from such sources as applications, logs, audit reports, etc., used to determine the state of a risk or control
Gap analysis	An approach that focuses on identifying the difference, or "gap," between the current state or condition of a risk and its desired state
Current state	The condition of a risk-related factor at a given point in time
Desired state	The condition of a risk-related factor that management has stated as a goal



TASK TO KNOWLEDGE STATEMENTS

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.

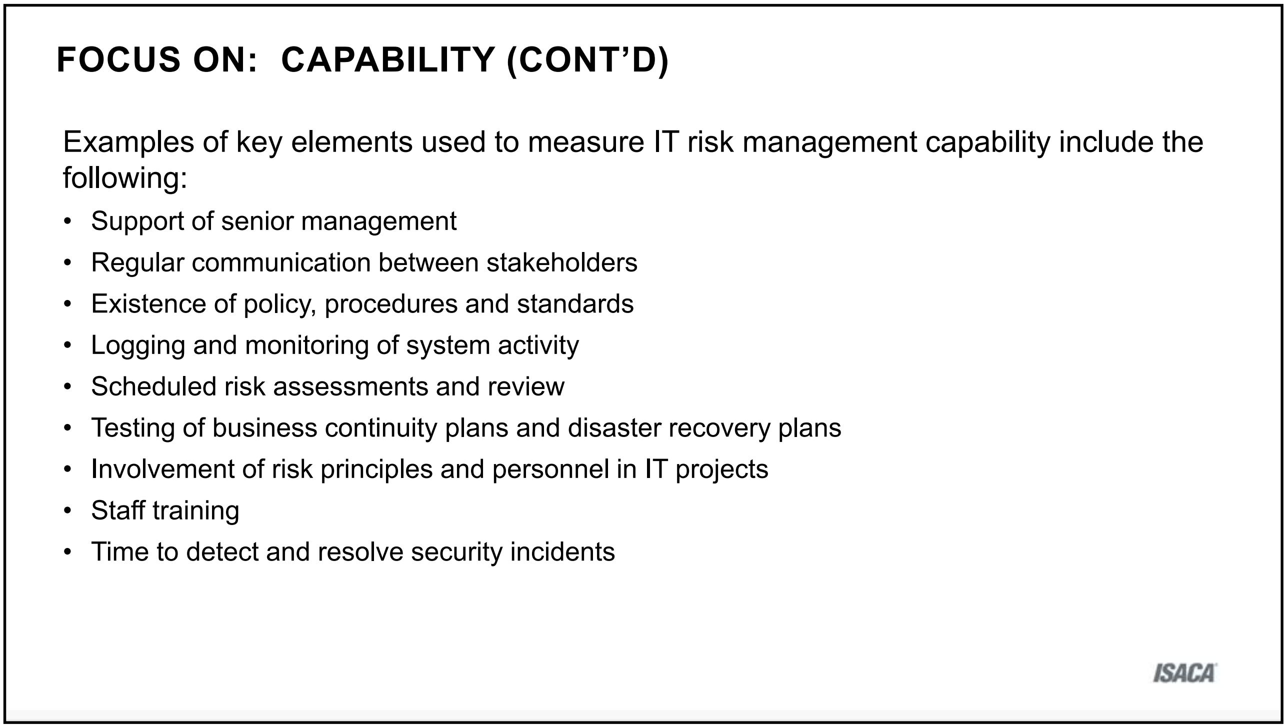


FOCUS ON: CAPABILITY

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

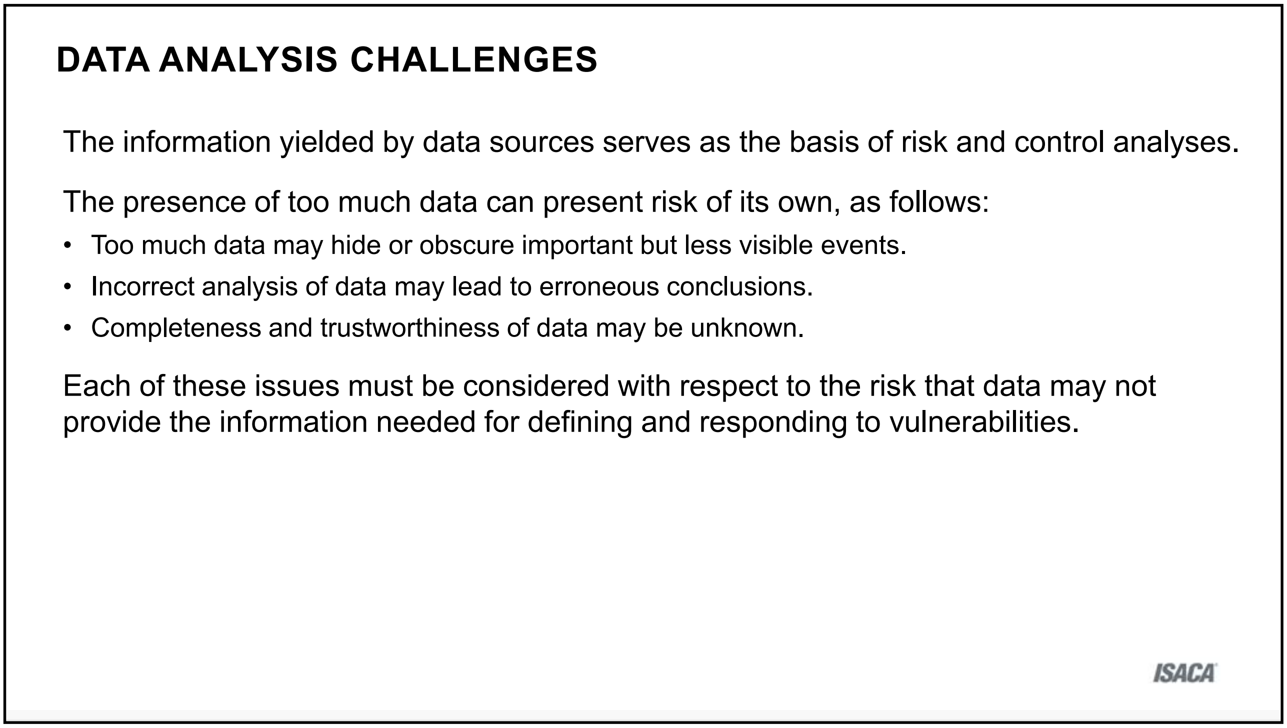


FOCUS ON: CAPABILITY (CONT'D)

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

ISACA



DATA ANALYSIS CHALLENGES

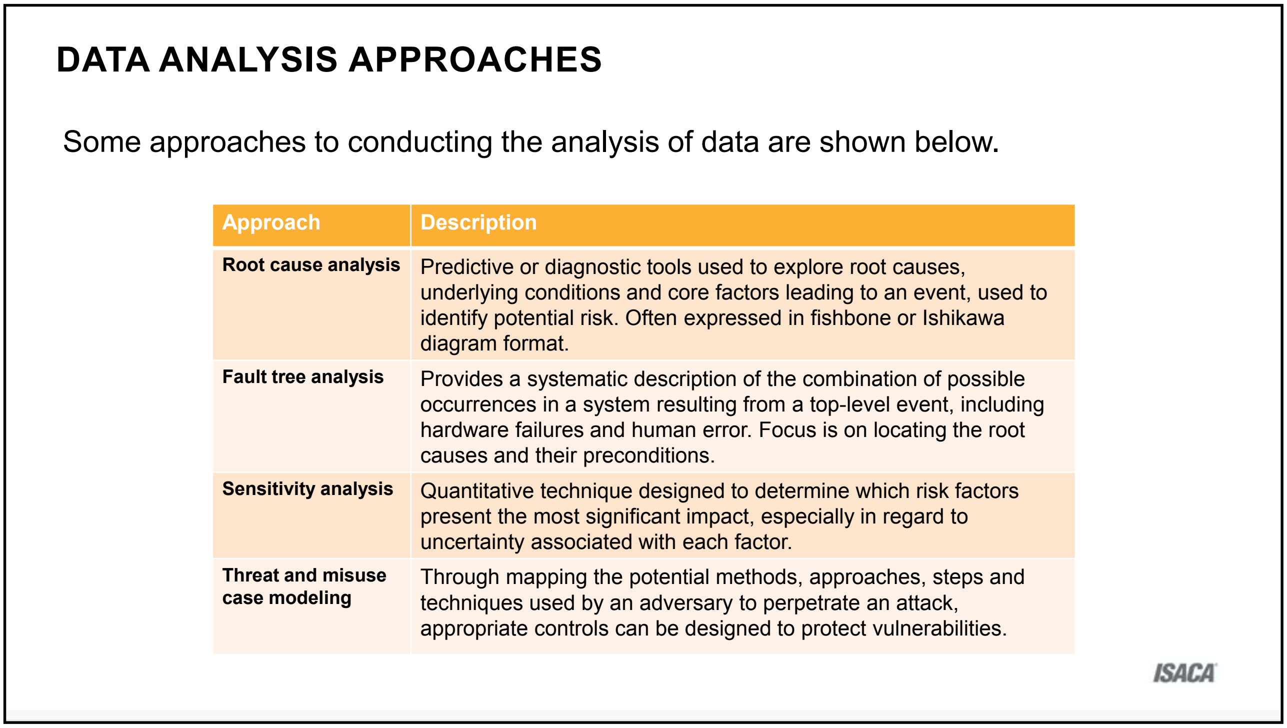
The information yielded by data sources serves as the basis of risk and control analyses.

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.

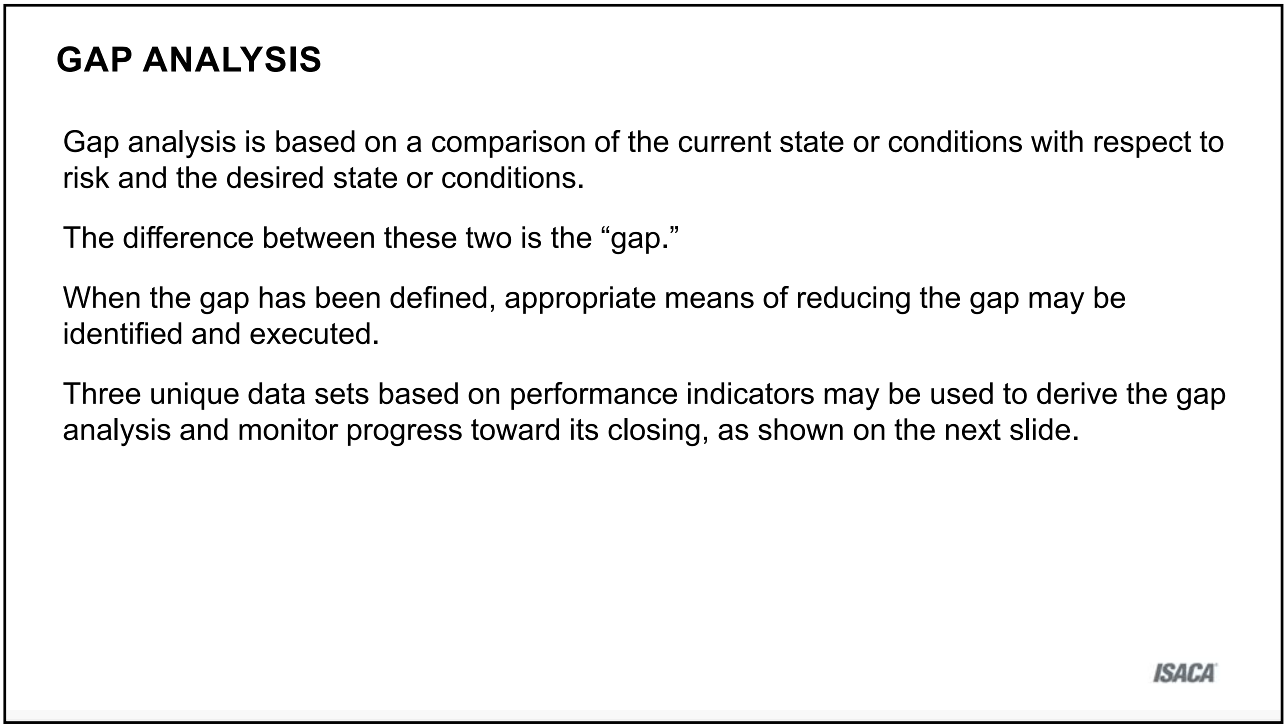
ISACA



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.



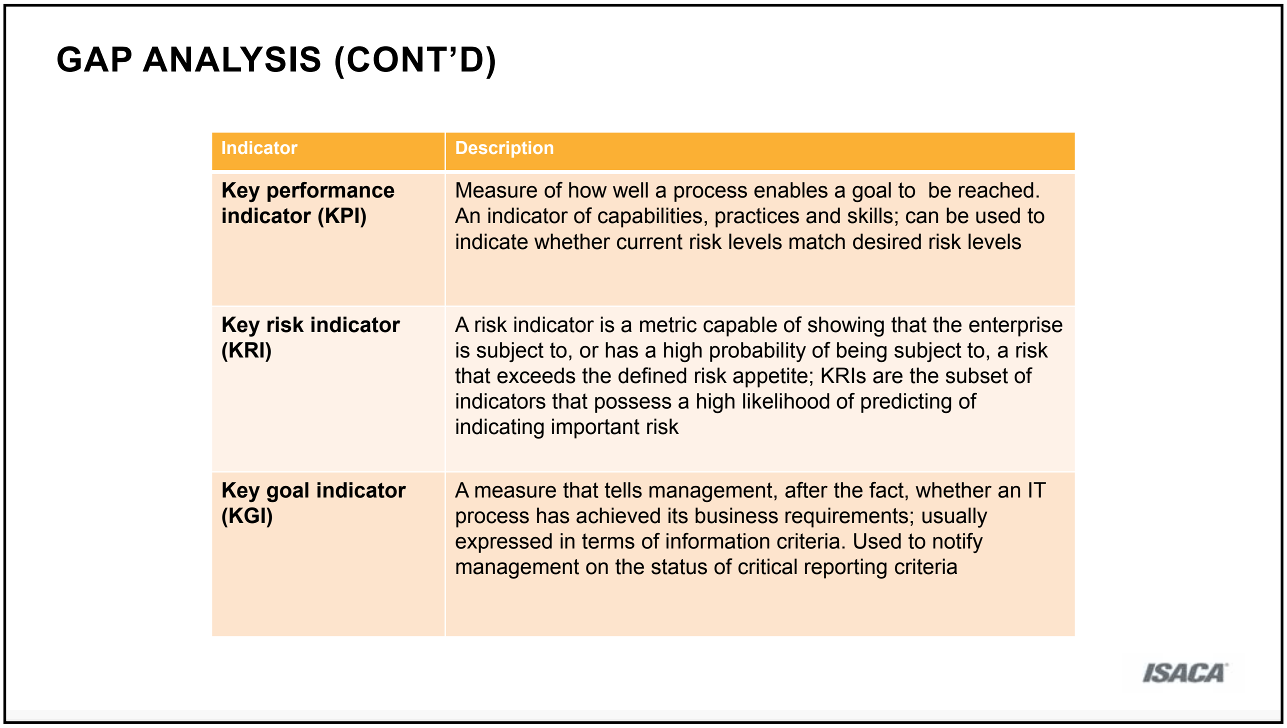
GAP ANALYSIS

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.”

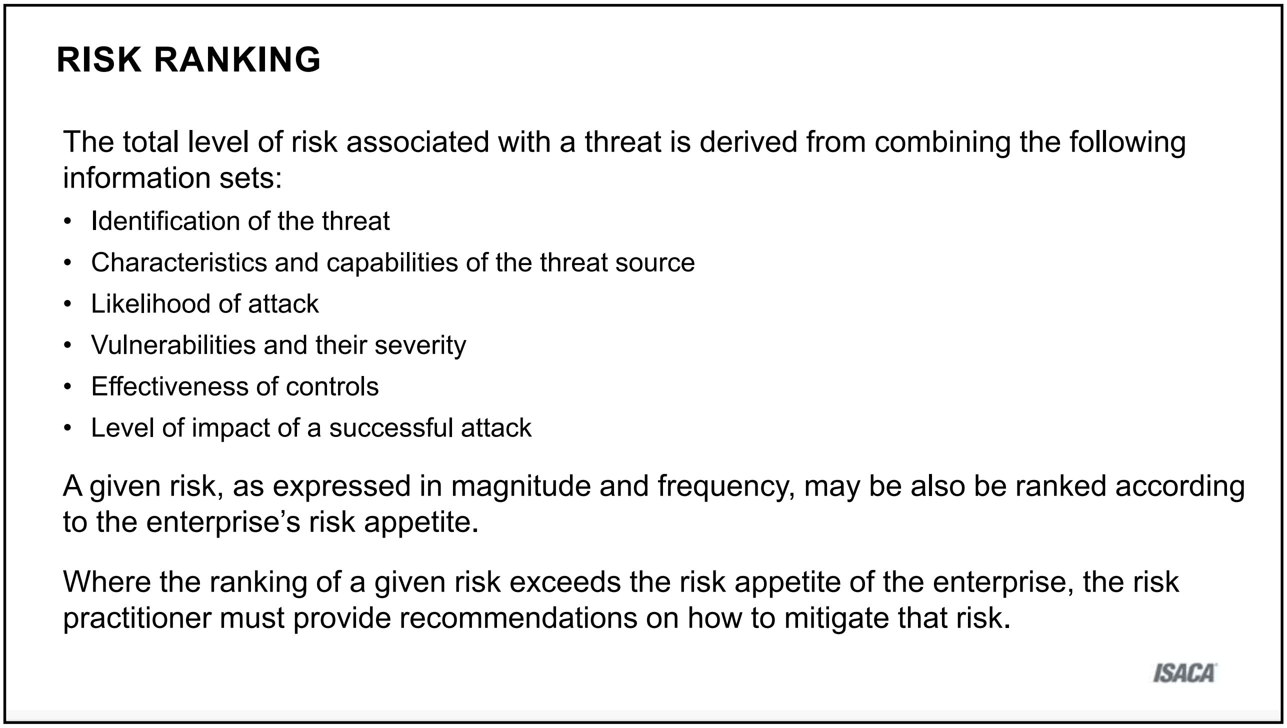
When the gap has been defined, appropriate means of reducing the gap may be identified and executed.

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



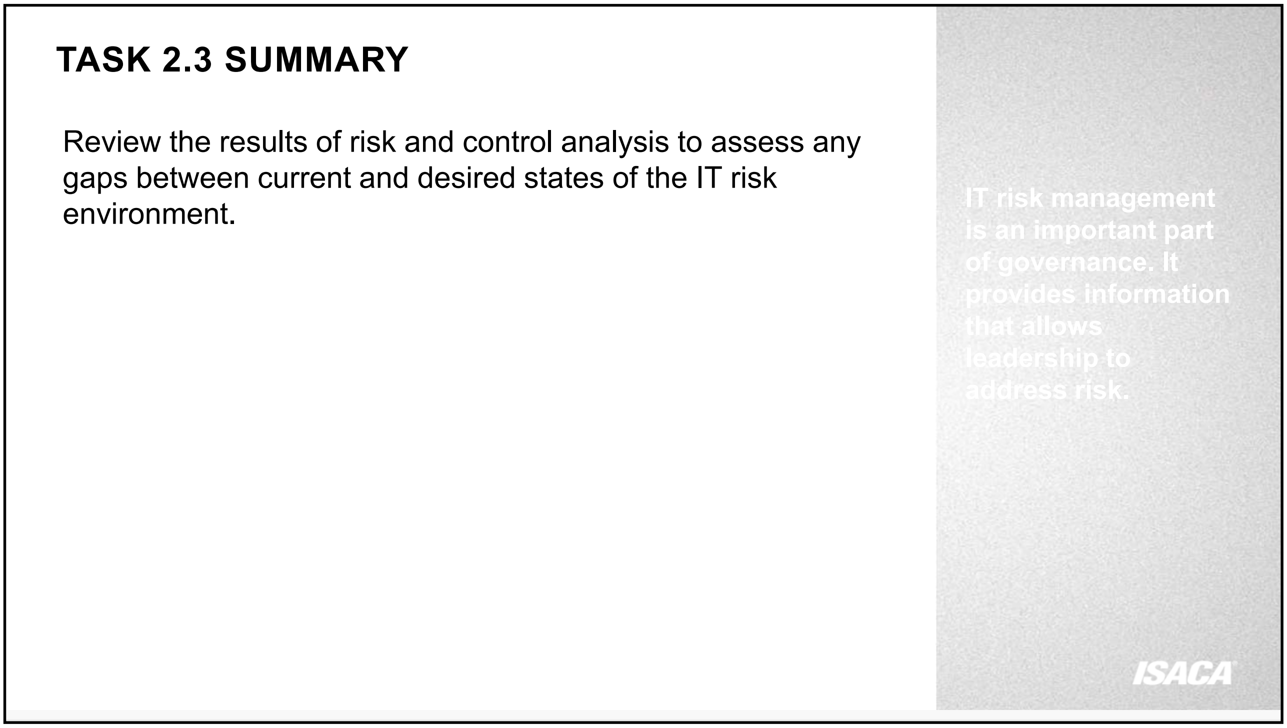
RISK RANKING

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.



TASK 2.3 SUMMARY

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

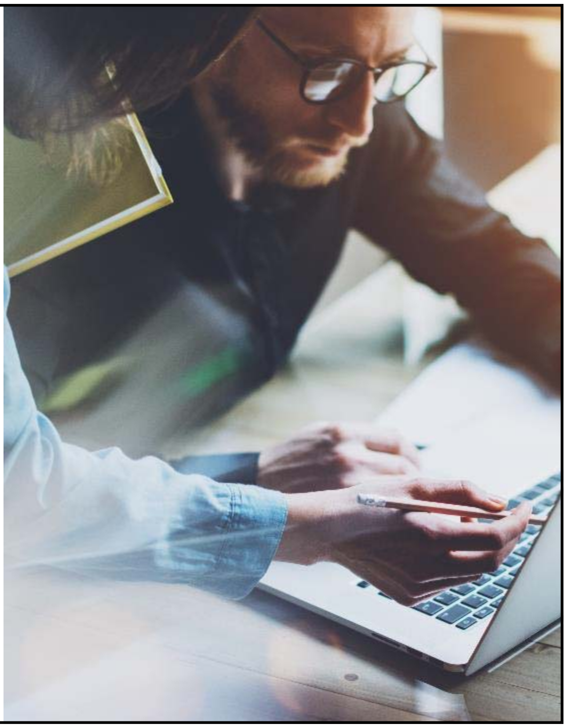
IT risk management is an important part of governance. It provides information that allows leadership to address risk.

TASK 2.3 DISCUSSION

Name some risk management capabilities discussed earlier in this program.

Consider different risk scenarios and discuss the capability level of the existing risk assessment function.

Support your opinions with your learning about risk management capabilities.



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

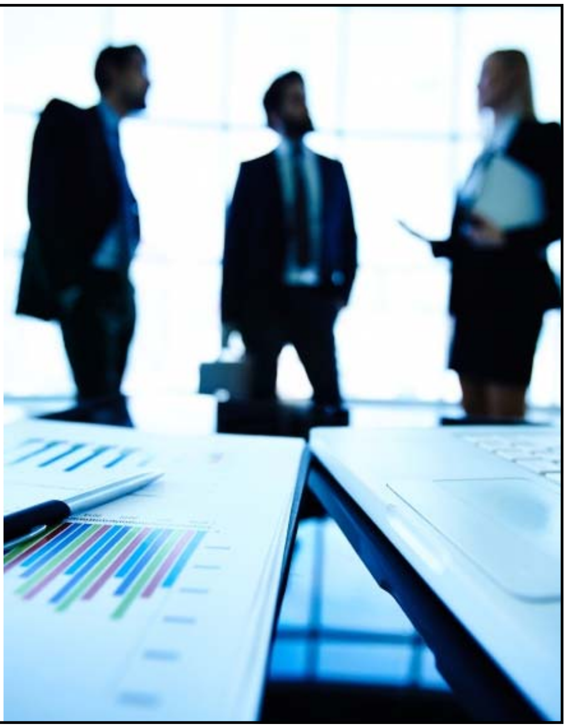
An enterprise is hiring a consultant to help determine the maturity level of the risk management program. The MOST important element of the request for proposal (RFP) is the:

A. sample deliverable.

B. past experience of the engagement team.

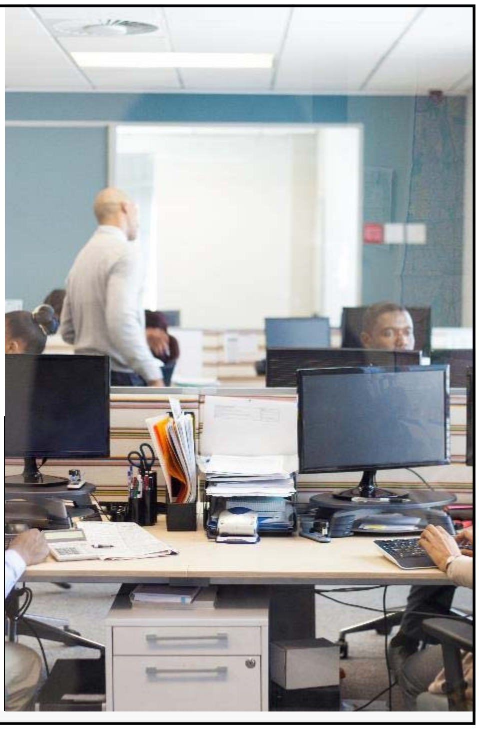
C. methodology used in the assessment.

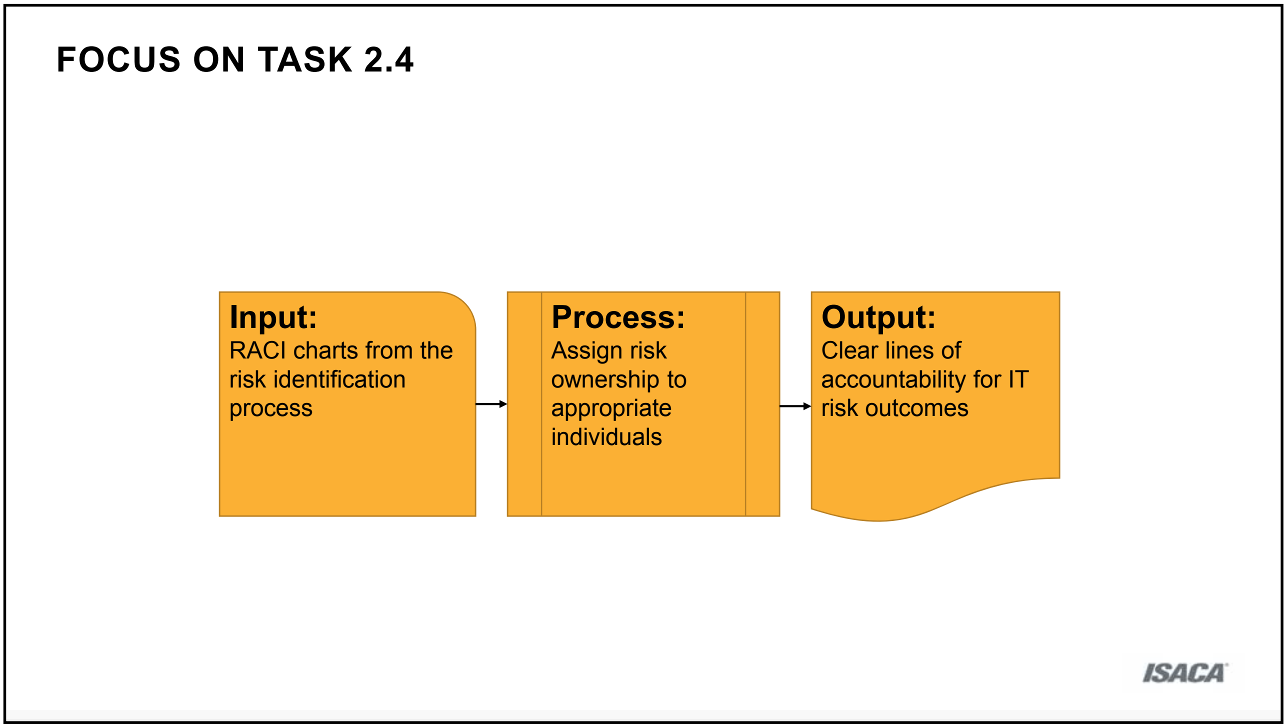
D. references from other organizations.



TASK 2.4

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



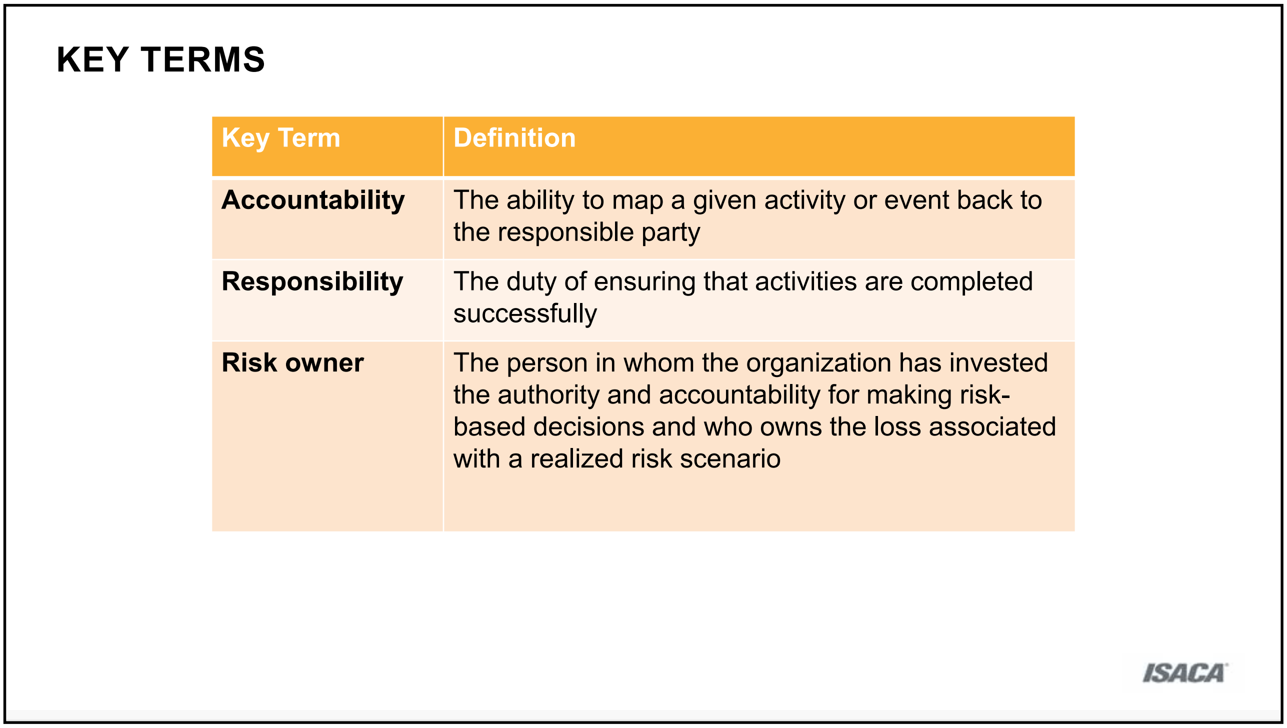


FOCUS ON TASK 2.4

Input:
RACI charts from the risk identification process

Process:
Assign risk ownership to appropriate individuals

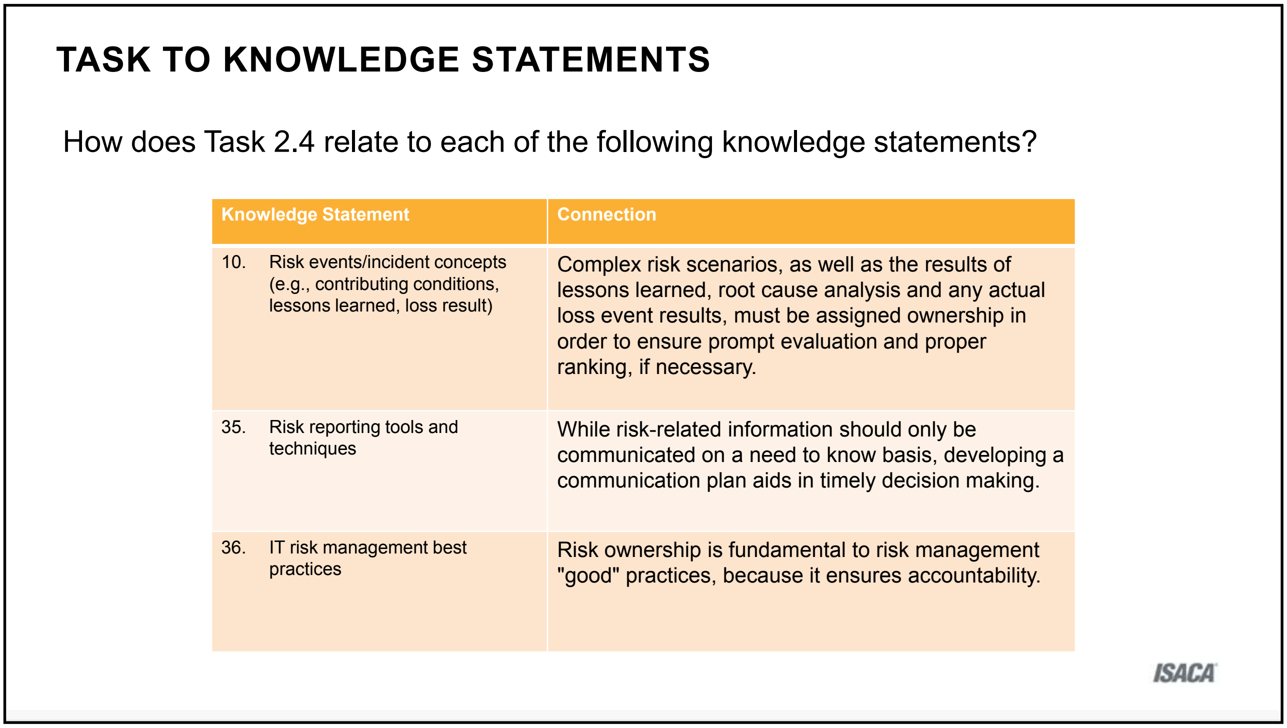
Output:
Clear lines of accountability for IT risk outcomes



KEY TERMS

Key Term	Definition
Accountability	The ability to map a given activity or event back to the responsible party
Responsibility	The duty of ensuring that activities are completed successfully
Risk owner	The person in whom the organization has invested the authority and accountability for making risk-based decisions and who owns the loss associated with a realized risk scenario

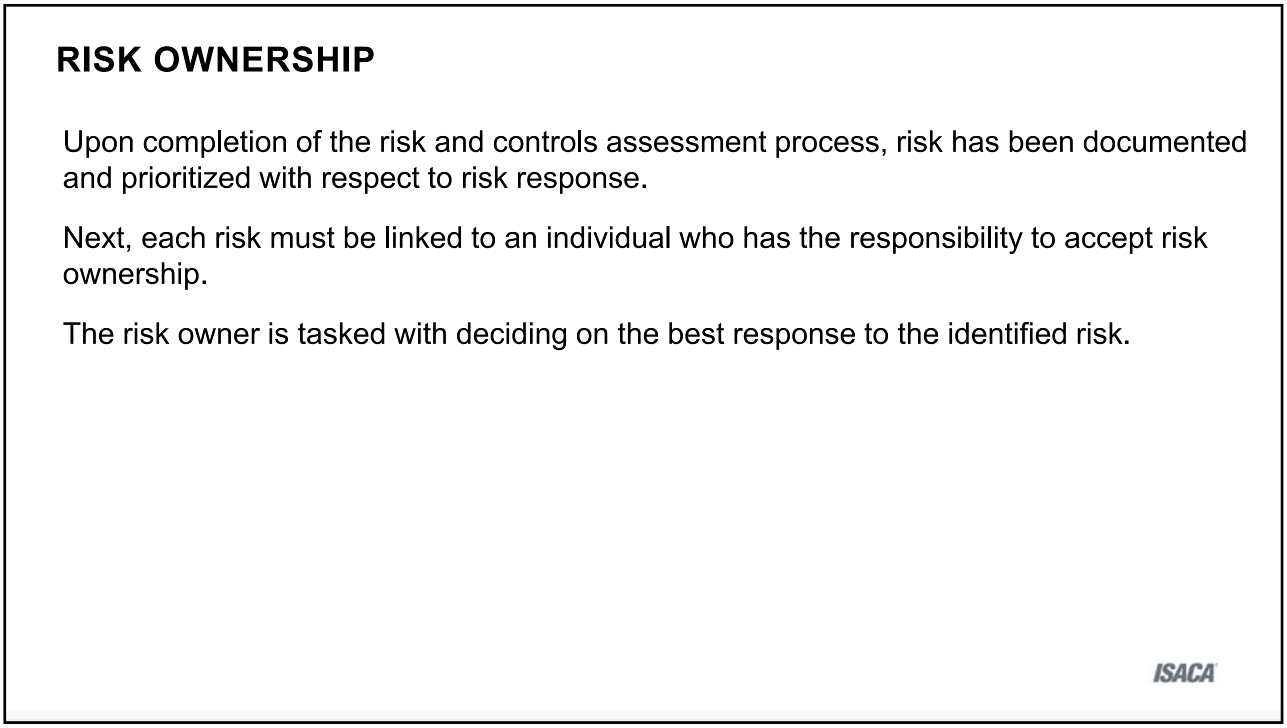
ISACA



TASK TO KNOWLEDGE STATEMENTS

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.

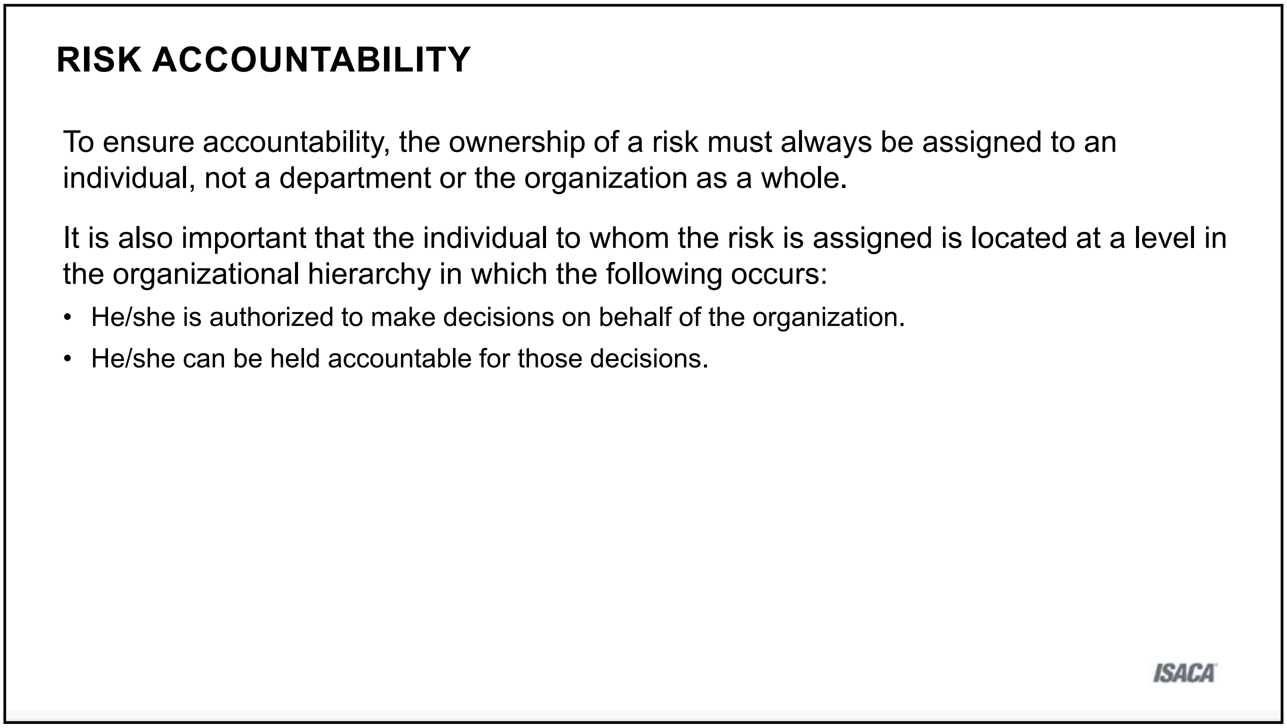


RISK OWNERSHIP

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.

TASK 2.4 SUMMARY

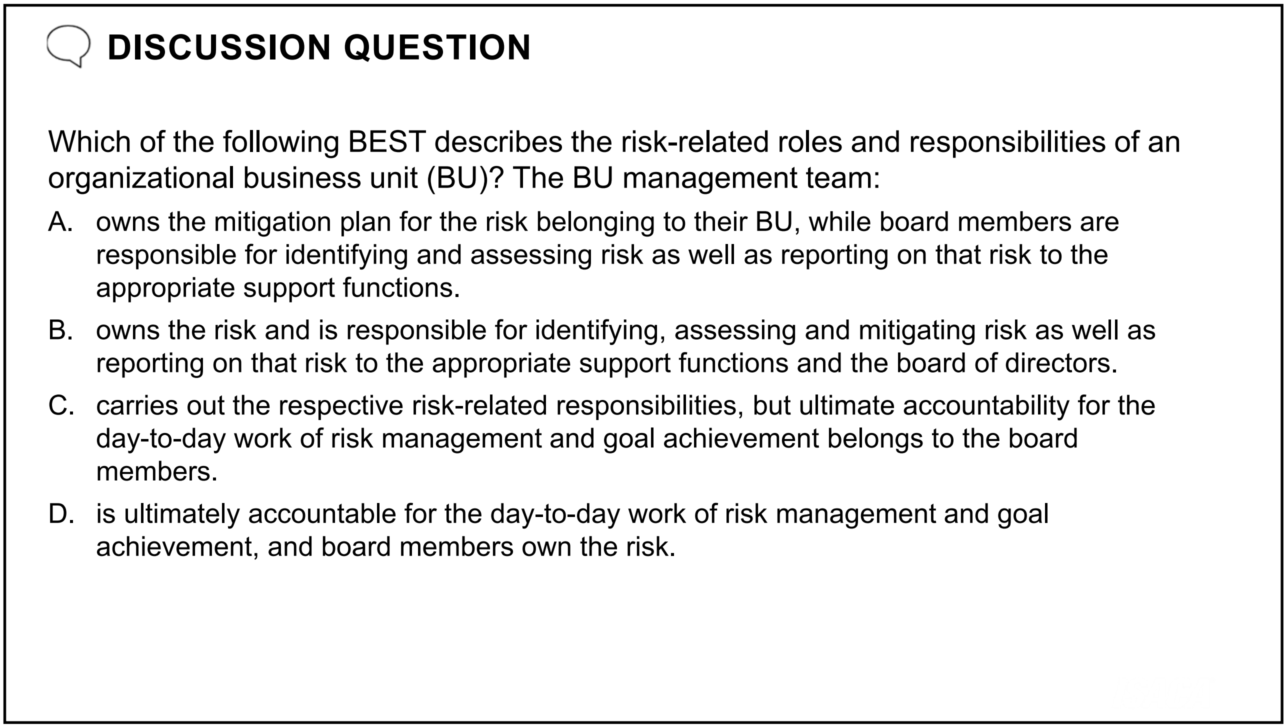
Ensure that risk ownership is assigned at the appropriate level to establish clear lines of accountability.

The IT risk management program must be overseen and supported by senior level leadership.

TASK 2.4 DISCUSSION

Who owns risk in an enterprise? For example, do you agree with the statement "Risk ownership belongs with senior leadership”?

Why or why not?



DISCUSSION QUESTION

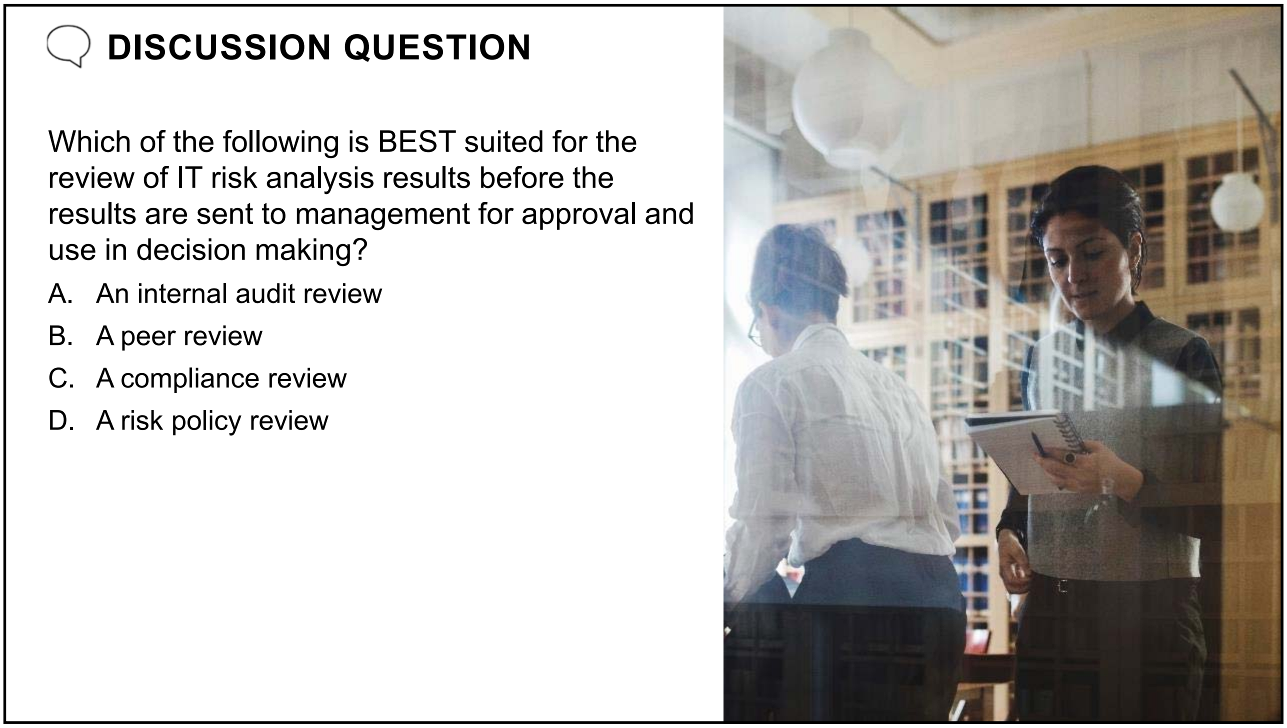
Which of the following BEST describes the risk-related roles and responsibilities of an organizational business unit (BU)? The BU management team:

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

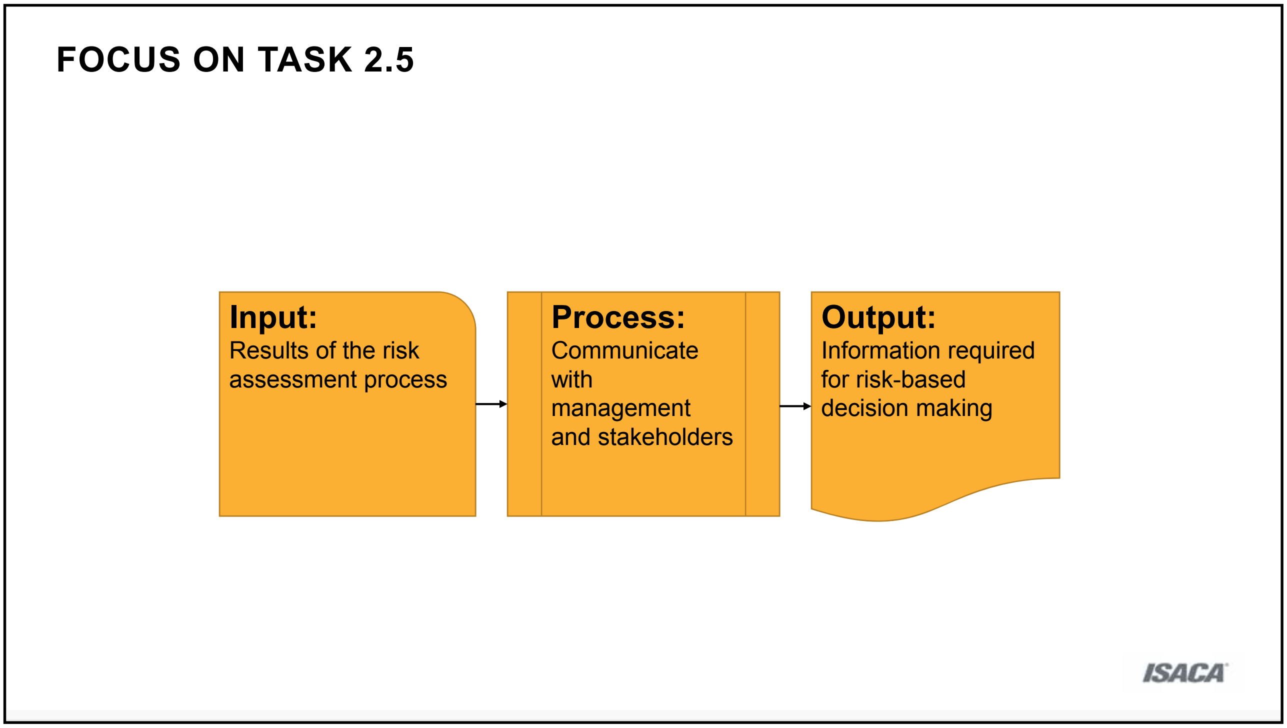
B. A peer review

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.

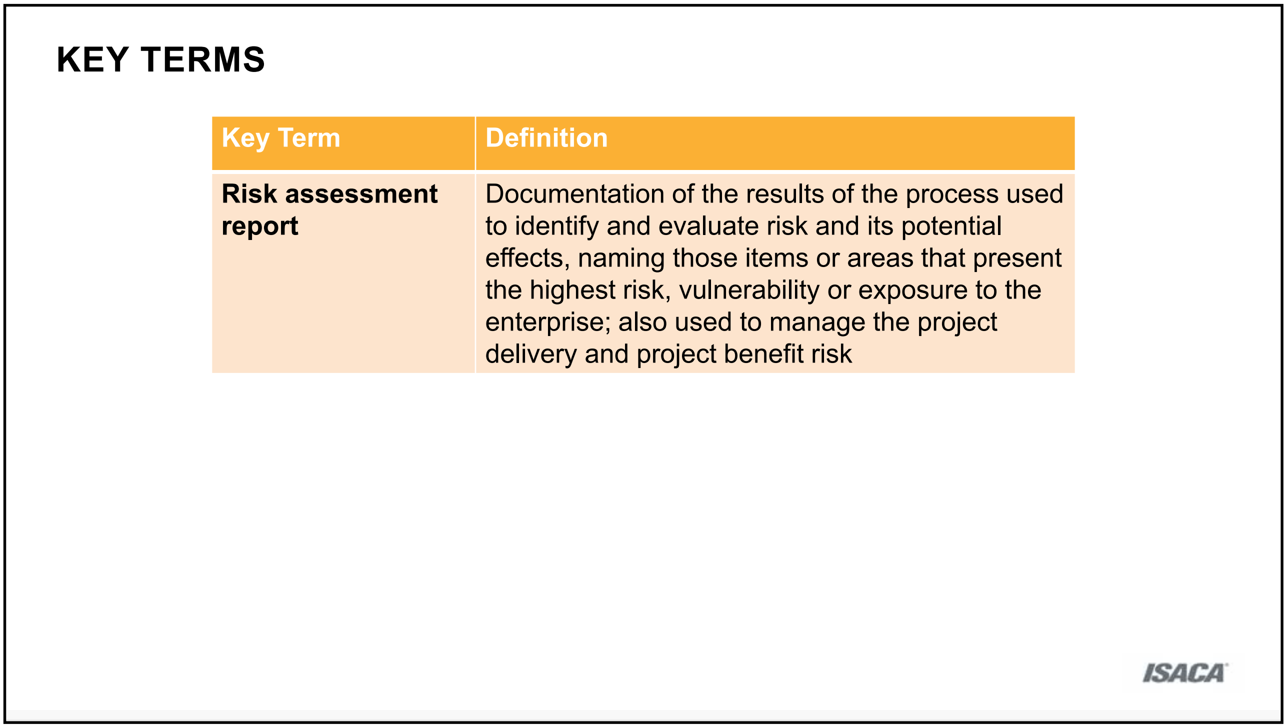


FOCUS ON TASK 2.5

Input:
Results of the risk assessment process

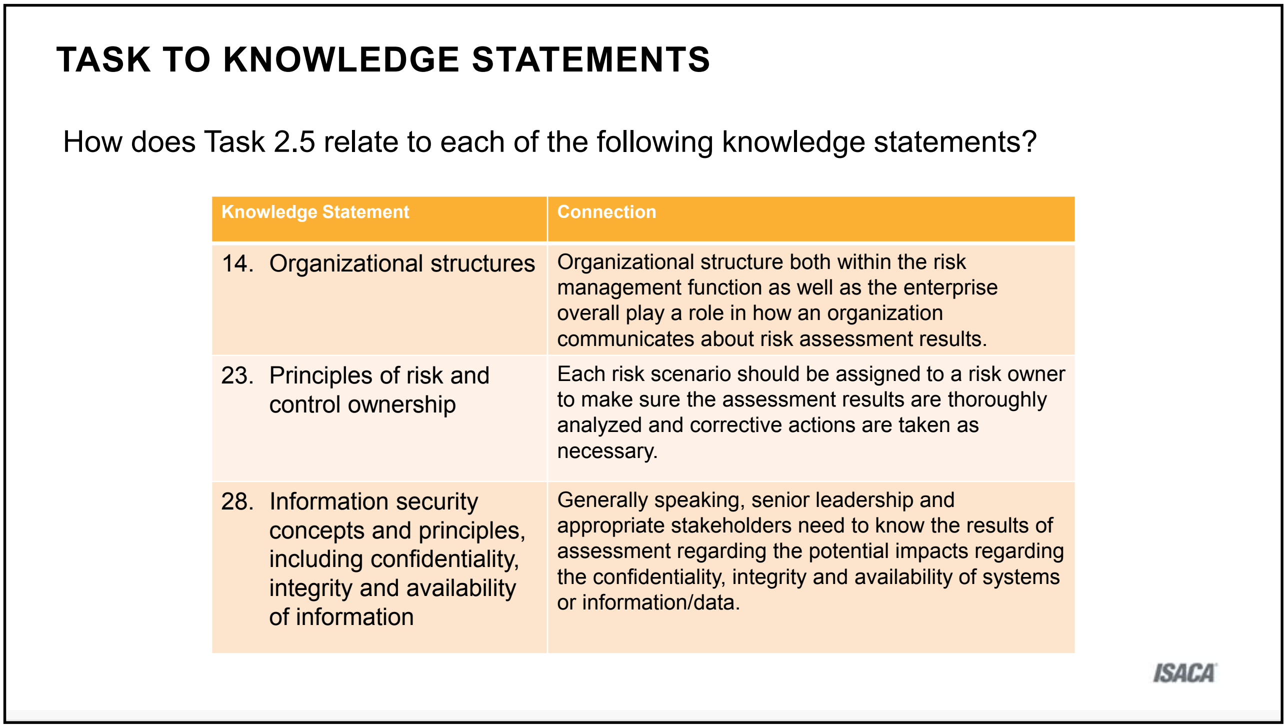
Process:
Communicate with management and stakeholders

Output:
Information required for risk-based decision making



KEY TERMS

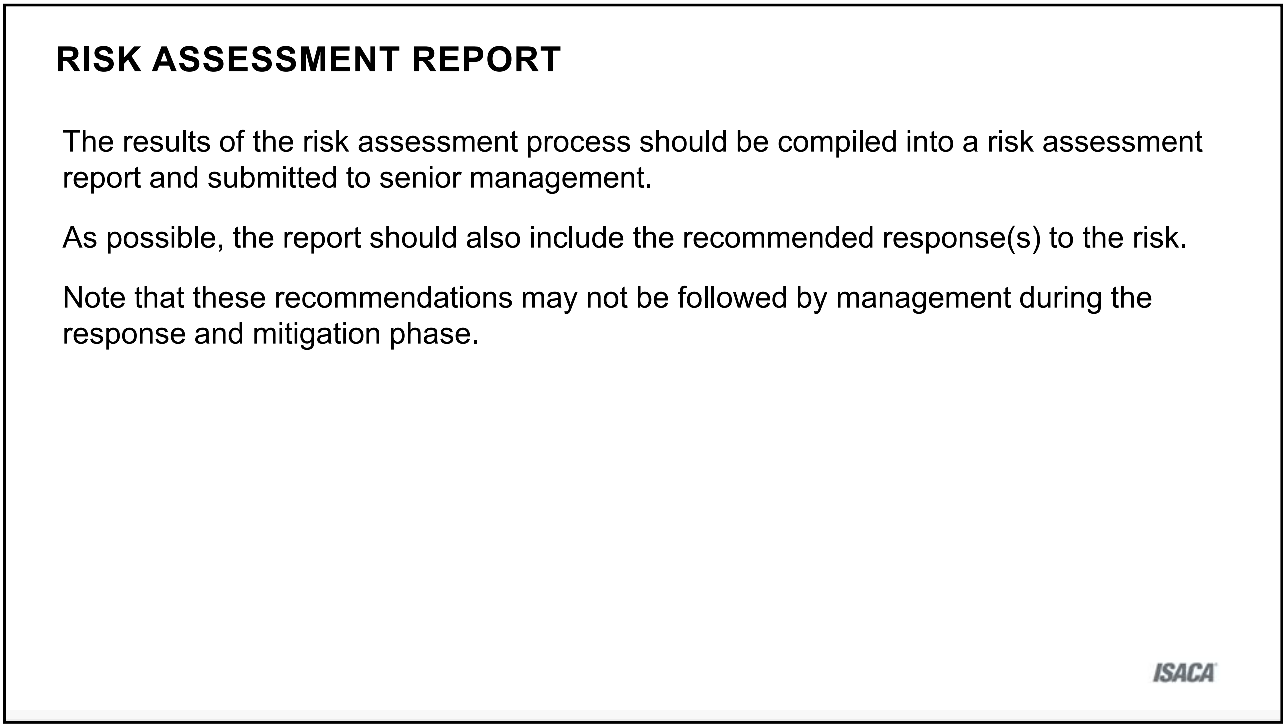
Key Term	Definition
Risk assessment report	Documentation of the results of the process used to identify and evaluate risk and its potential effects, naming those items or areas that present the highest risk, vulnerability or exposure to the enterprise; also used to manage the project delivery and project benefit risk



TASK TO KNOWLEDGE STATEMENTS

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.

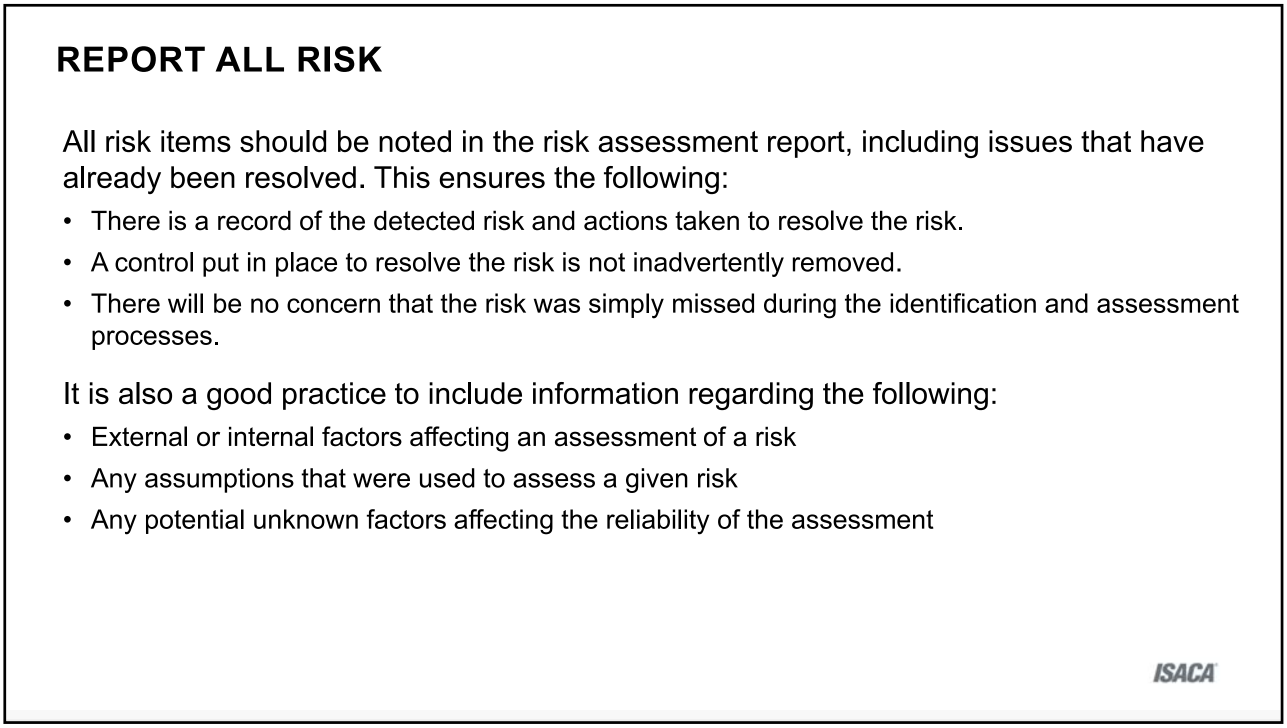


RISK ASSESSMENT REPORT

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

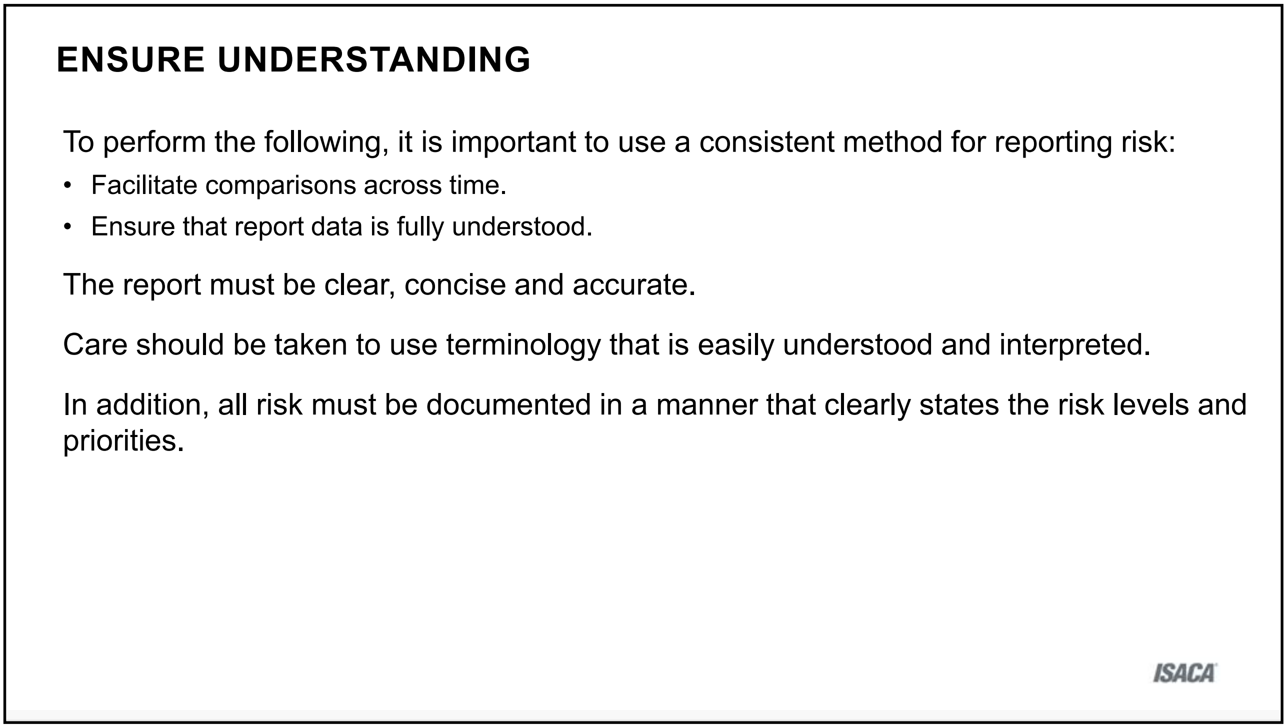
All risk items should be noted in the risk assessment report, including issues that have already been resolved. This ensures the following:

- 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

ISACA



ENSURE UNDERSTANDING

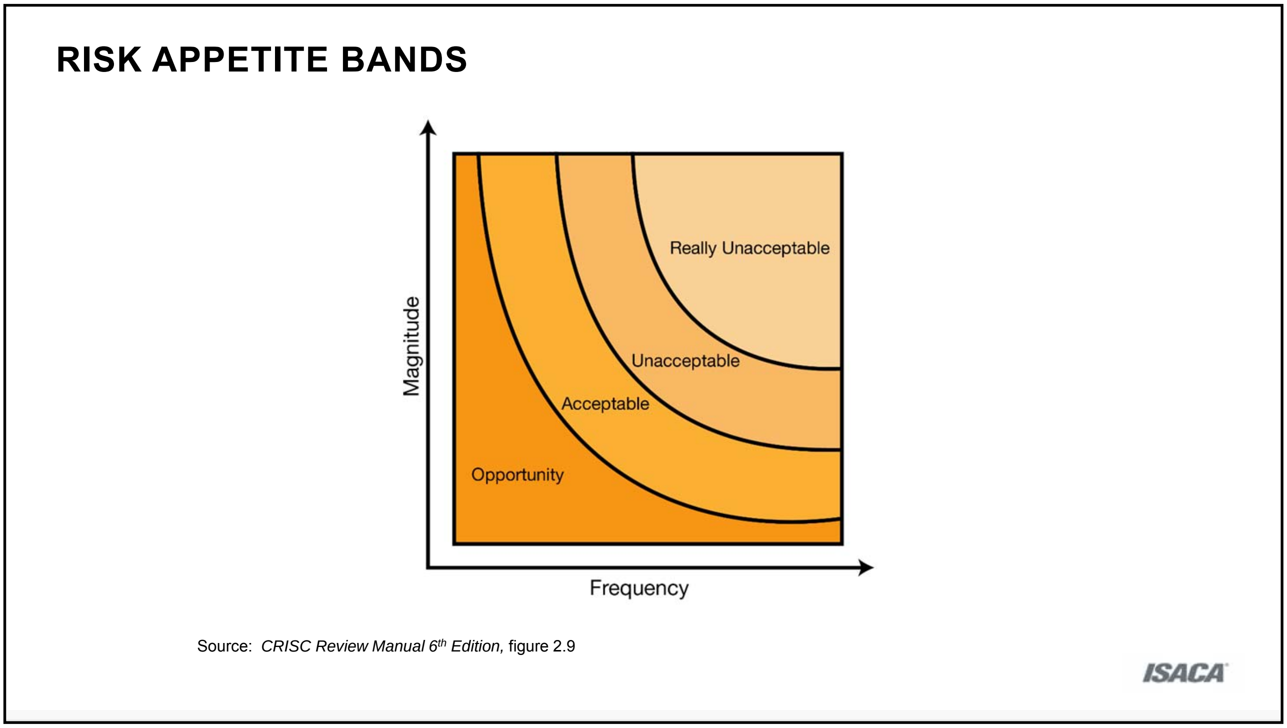
To perform the following, it is important to use a consistent method for reporting risk:

- Facilitate comparisons across time.
- Ensure that report data is fully understood.

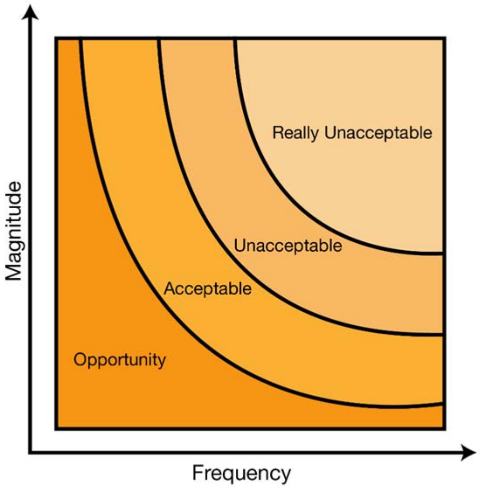
The report must be clear, concise and accurate.

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.

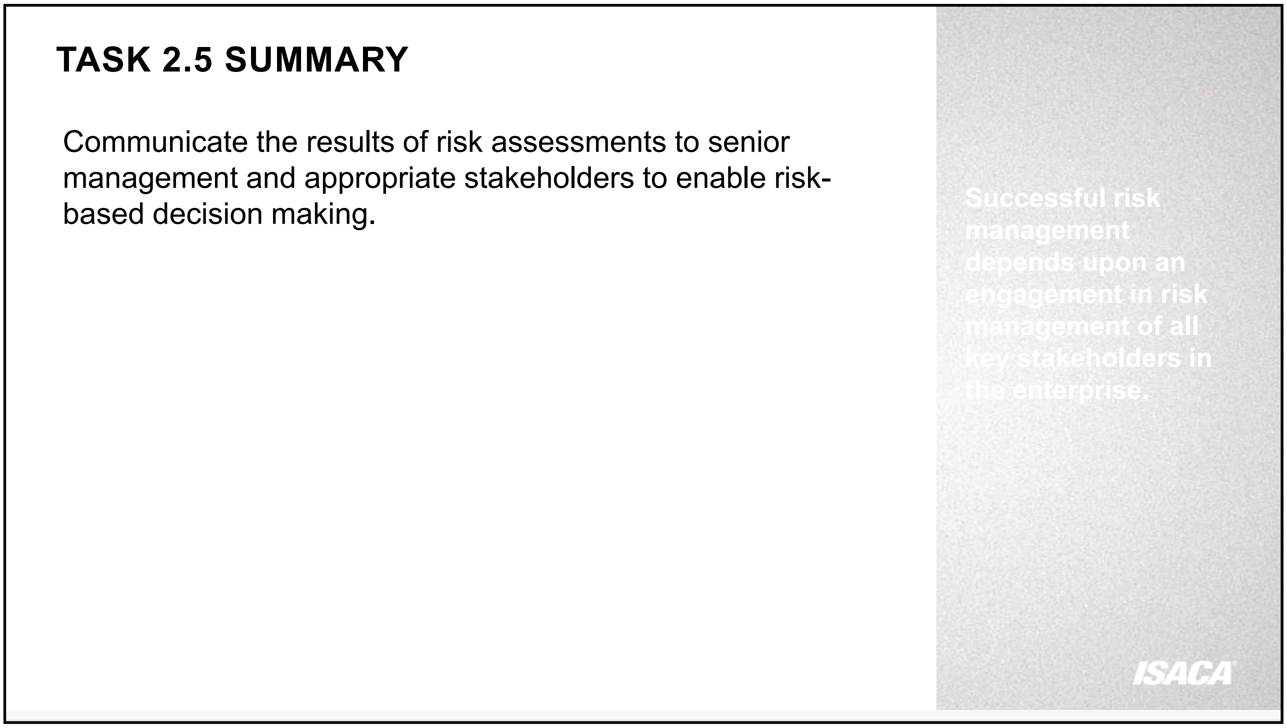


RISK APPETITE BANDS



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

ISACA



TASK 2.5 SUMMARY

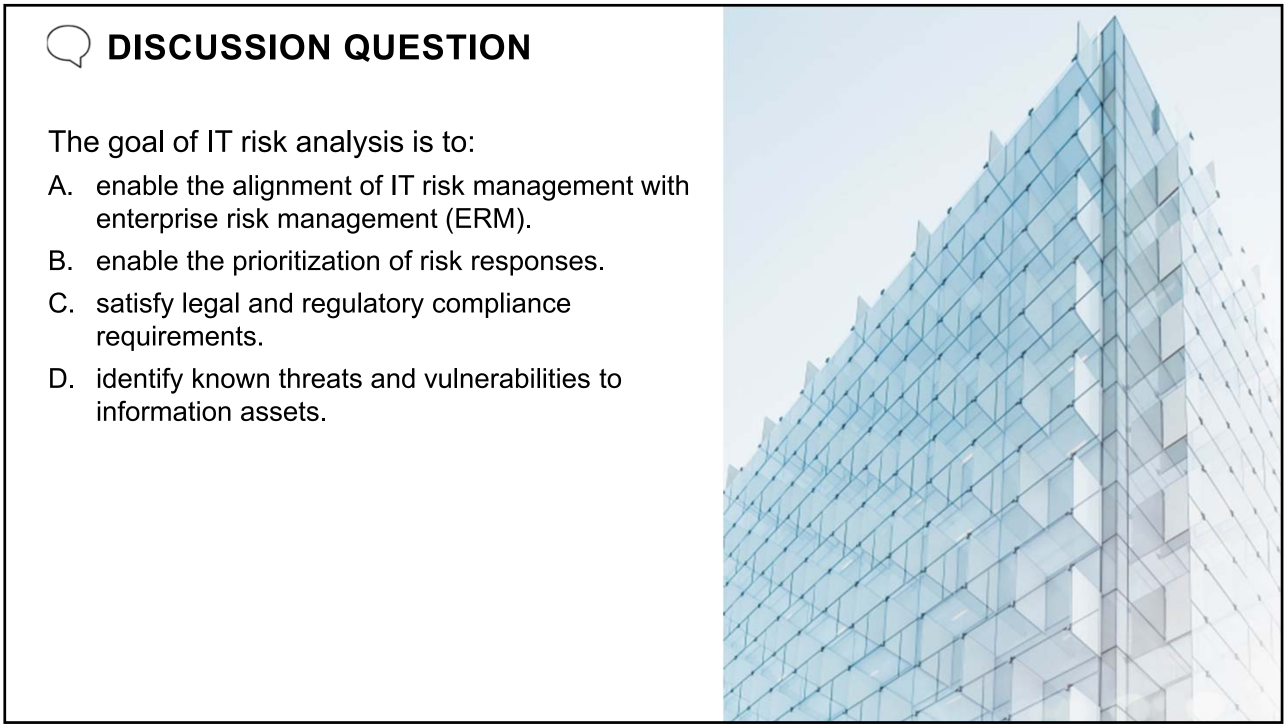
Communicate the results of risk assessments to senior management and appropriate stakeholders to enable risk-based decision making.

Successful risk management depends upon an engagement in risk management of all key stakeholders in the enterprise.

TASK 2.5 DISCUSSION

Consider the following risk situations:

- A stock trading company is using call recording equipment that runs on the Windows 2003 OS. The company has decided to purchase extended patches from Microsoft rather than upgrading to a call recorder based on a supported OS.
- A small local bank in a rural location has experienced high turnover. In response, the bank decides to outsource all IT functions to a cloud network provider.
- A company outsources the disposal of paper and computer equipment to a destruction service that picks up from the company’s loading dock in the early morning on Sundays and transports the items to a vendor site for destruction and disposal. The hiring company decides to switch vendors to one that offers onsite disposal during regular business hours.
- Comparing the three situations, which represents the best example of a risk based decision?
- Support your opinion.



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

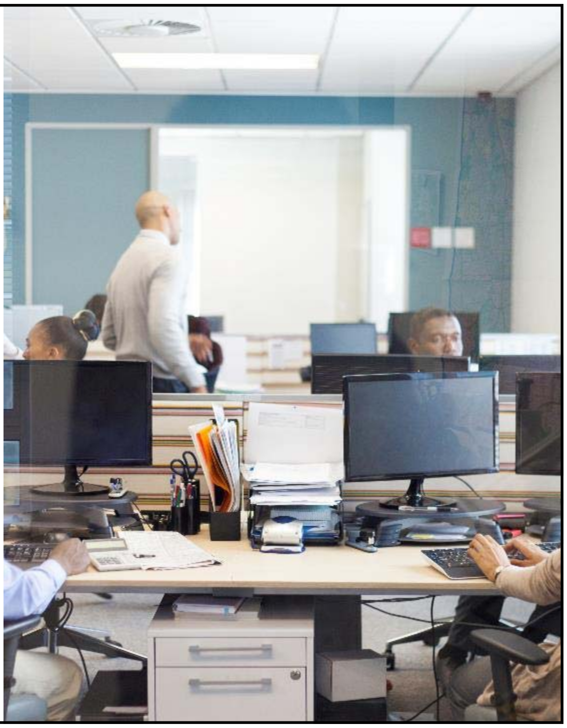
What do different risk scenarios on the same bands/curve on a risk map indicate?

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.

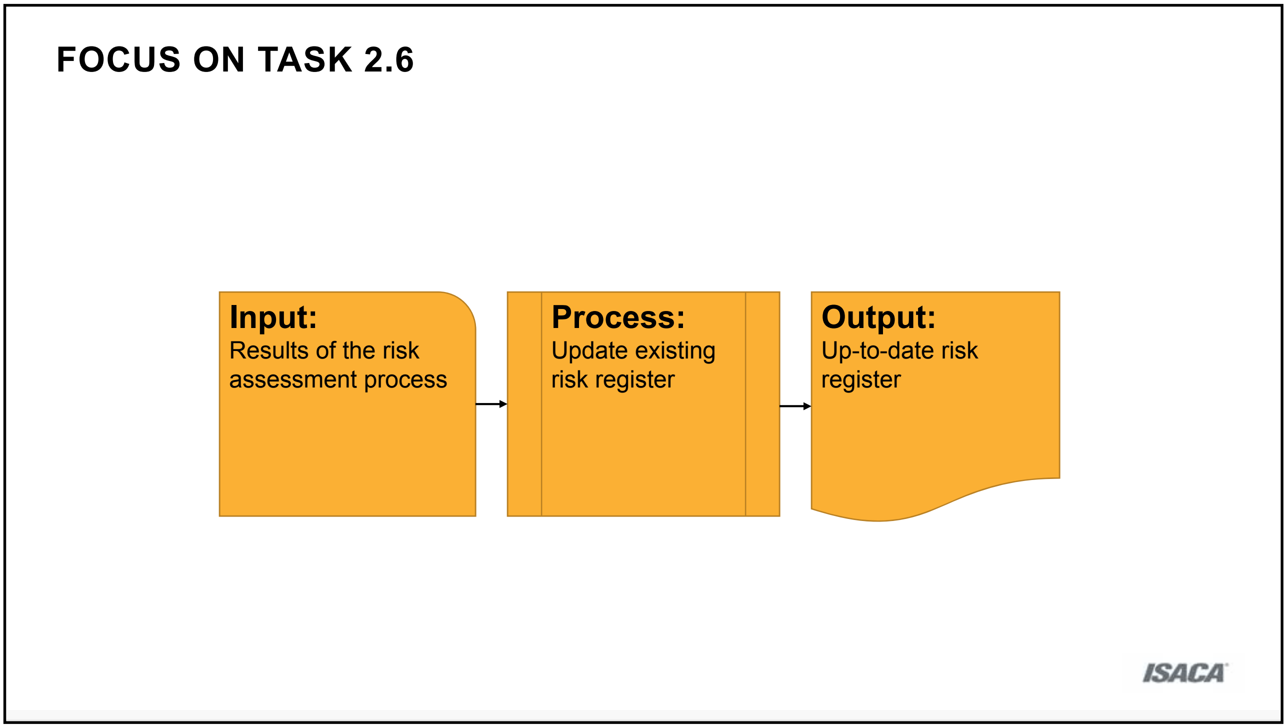
C. All risk scenarios on the same curve of a risk map require the same risk response.

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.

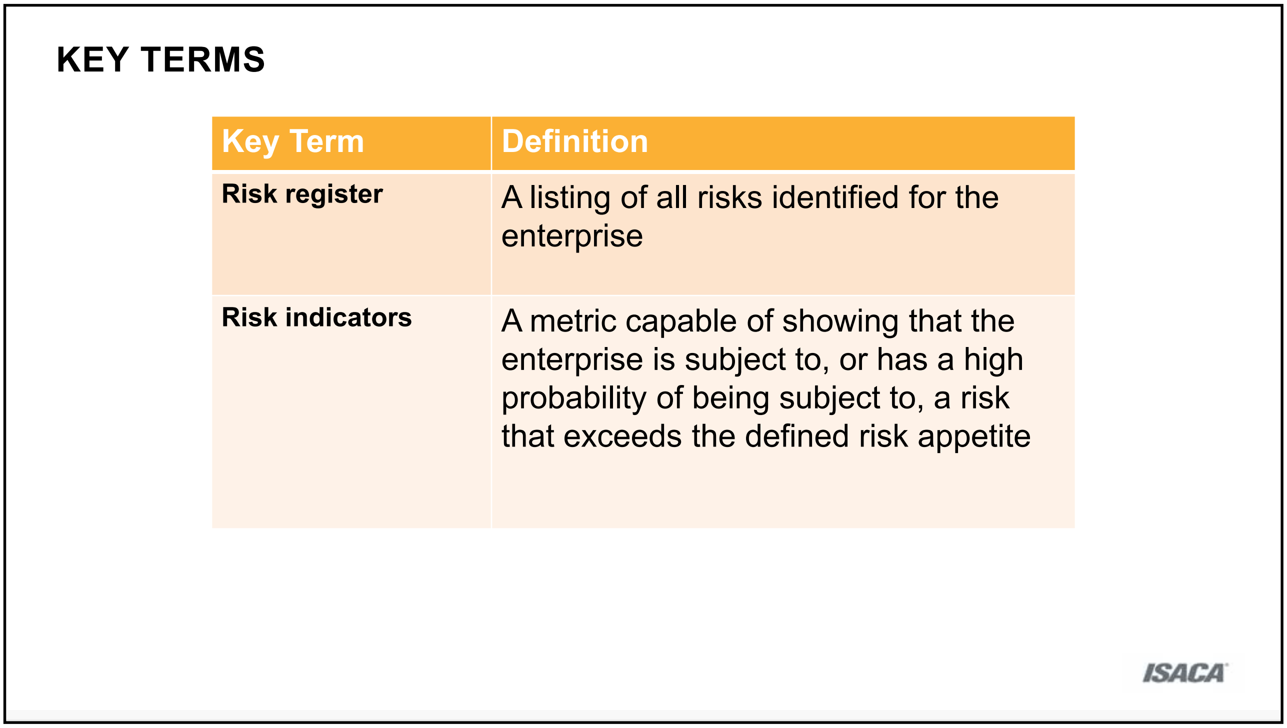


FOCUS ON TASK 2.6

Input:
Results of the risk assessment process

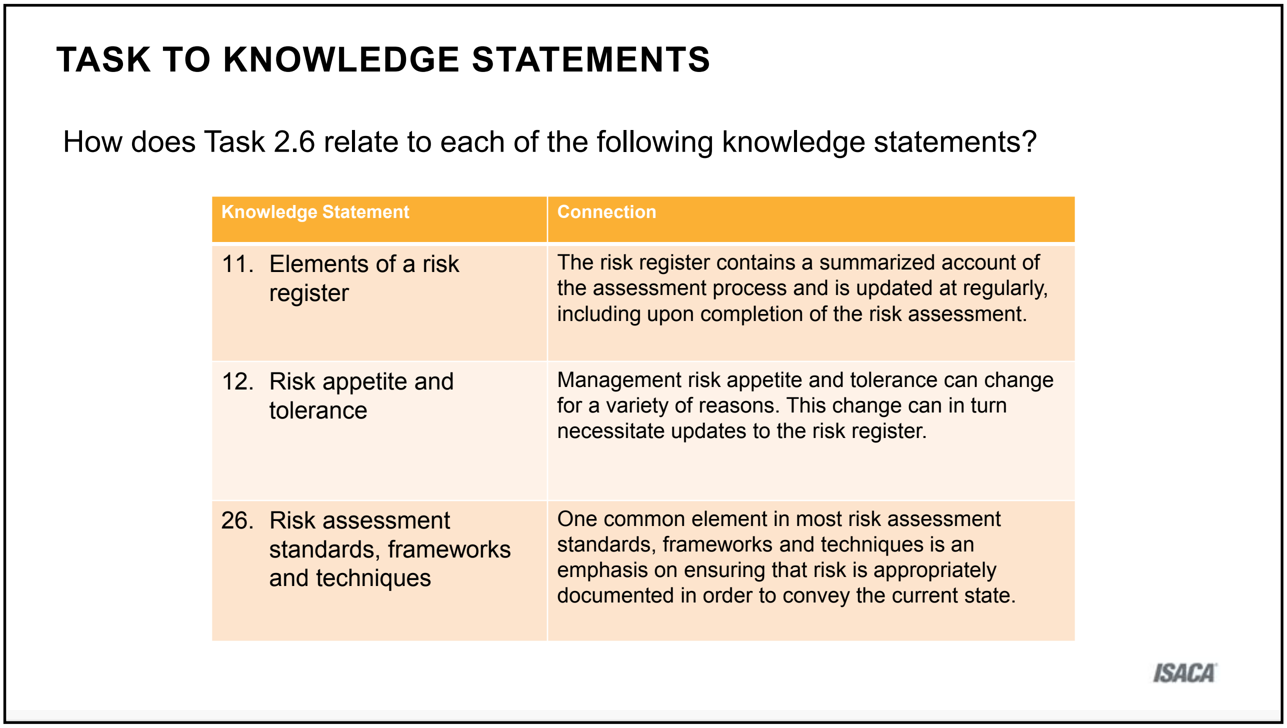
Process:
Update existing risk register

Output:
Up-to-date risk register



KEY TERMS

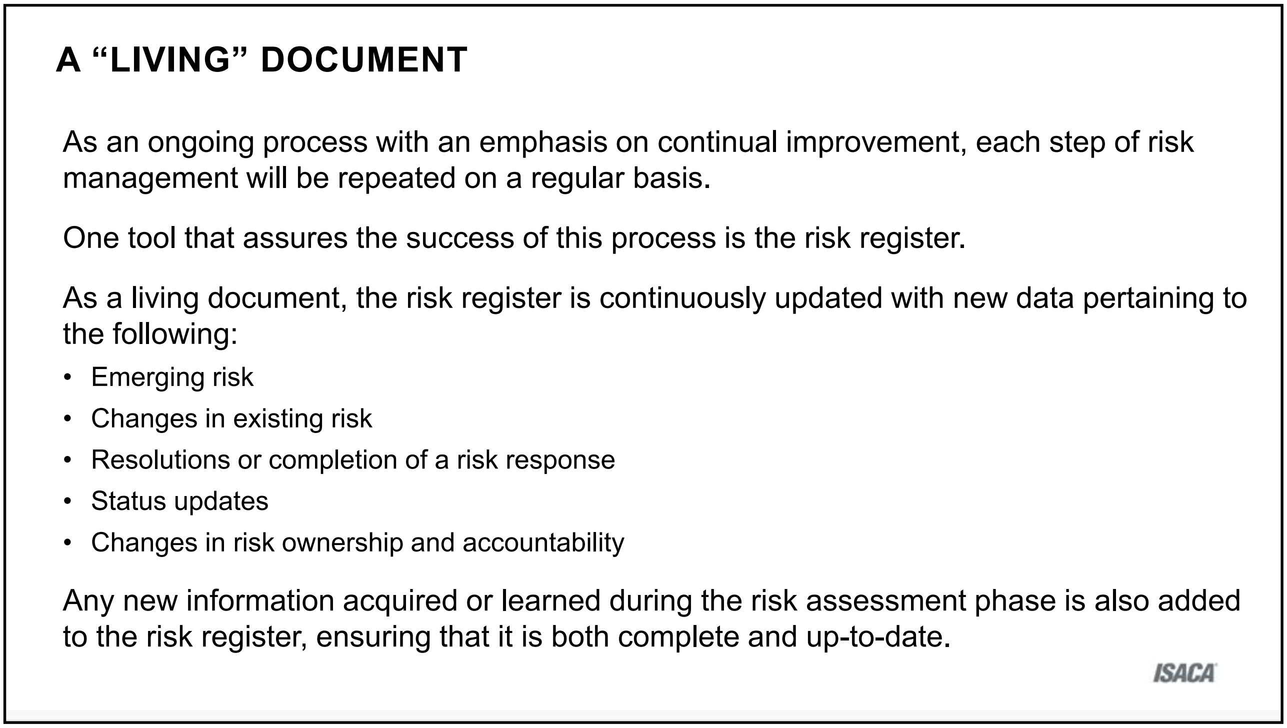
Key Term	Definition
Risk register	A listing of all risks identified for the enterprise
Risk indicators	A metric capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite



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

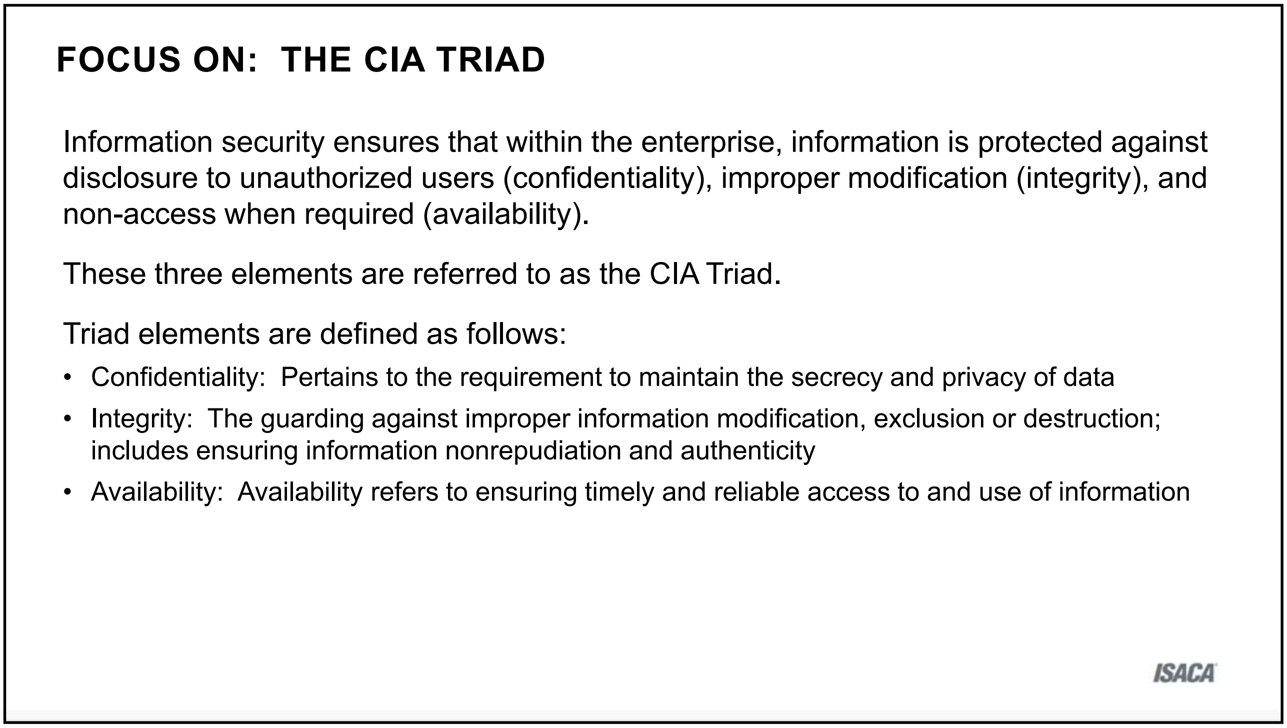
As an ongoing process with an emphasis on continual improvement, each step of risk management will be repeated on a regular basis.

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.



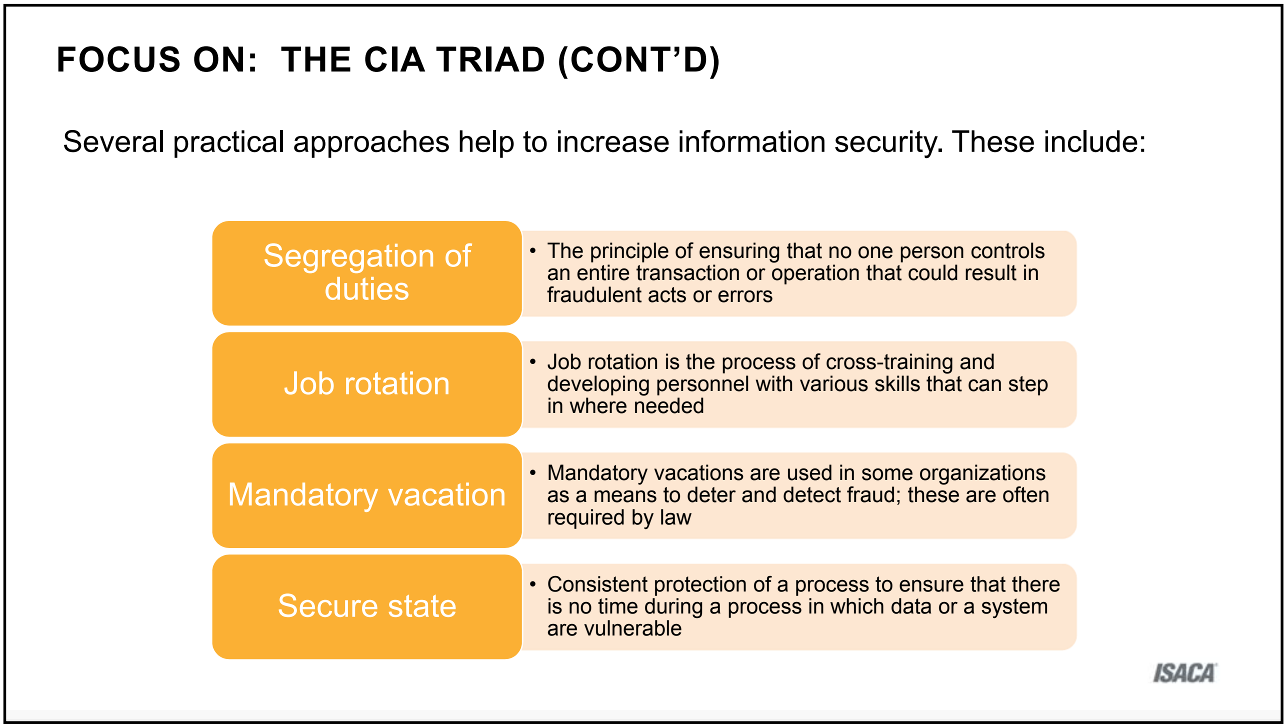
FOCUS ON: THE CIA TRIAD

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

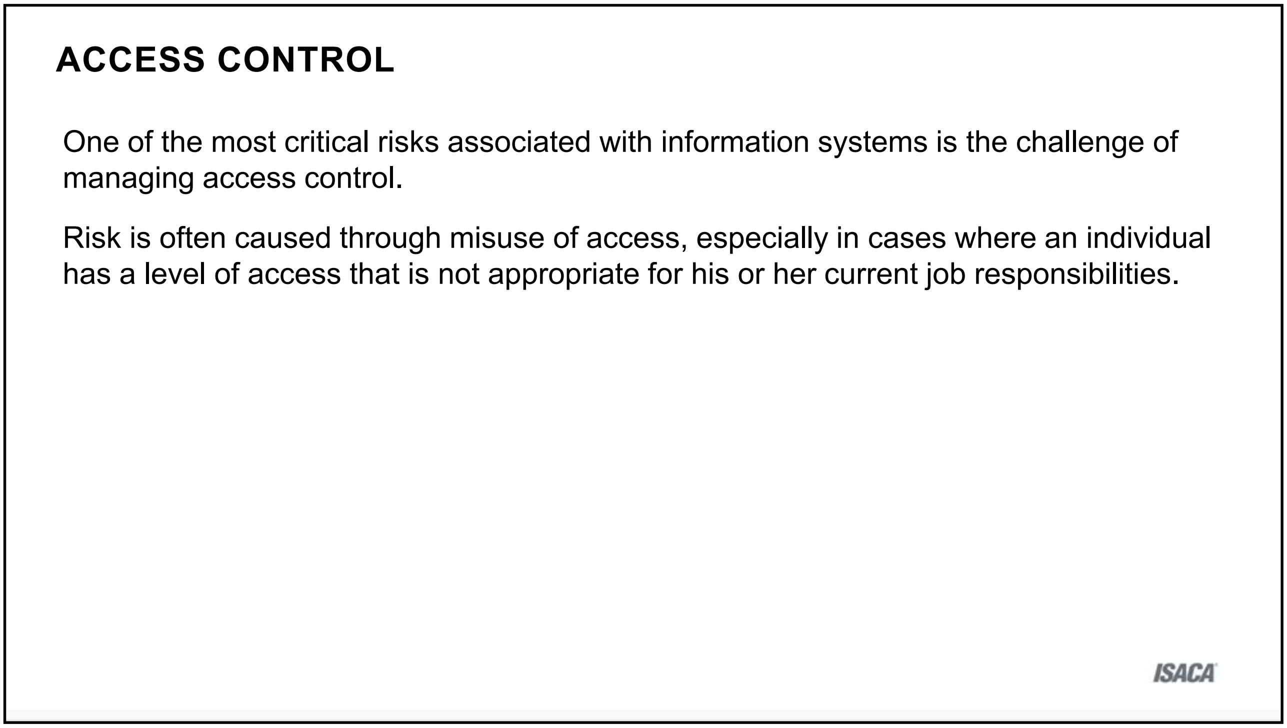
- Job rotation is the process of cross-training and developing personnel with various skills that can step in where needed

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

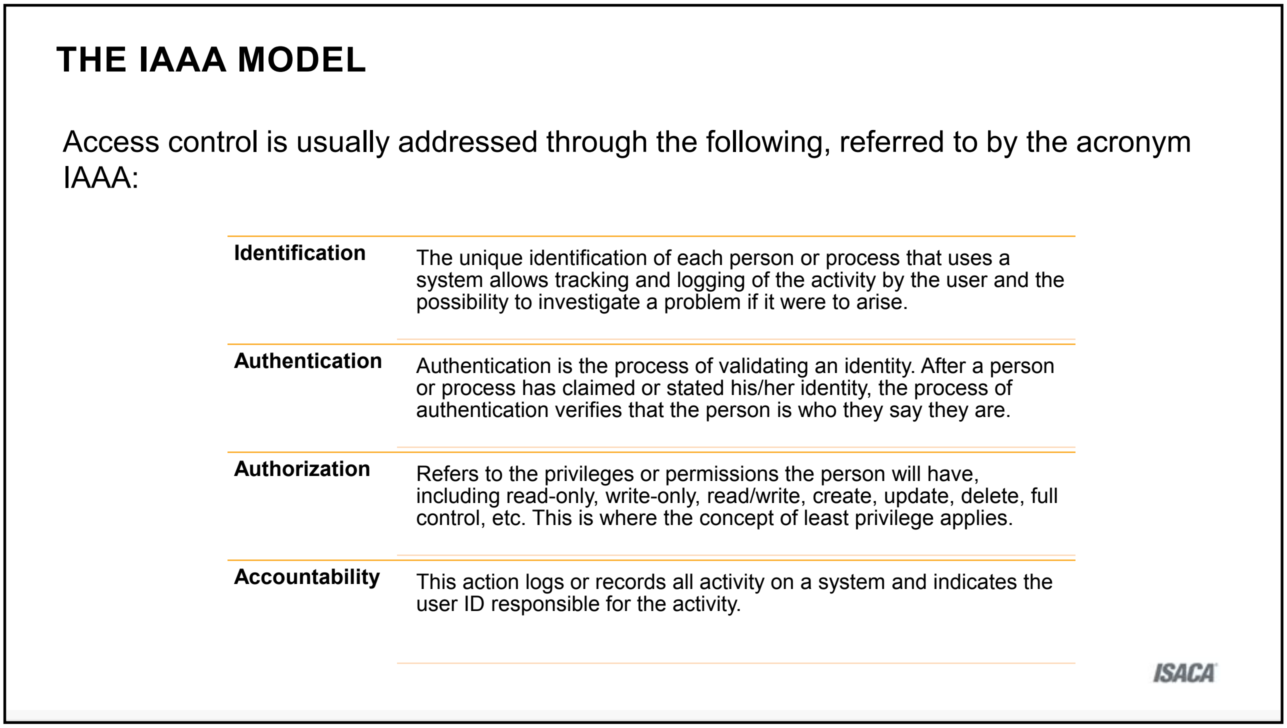
- Consistent protection of a process to ensure that there is no time during a process in which data or a system are vulnerable



ACCESS CONTROL

One of the most critical risks associated with information systems is the challenge of managing access control.

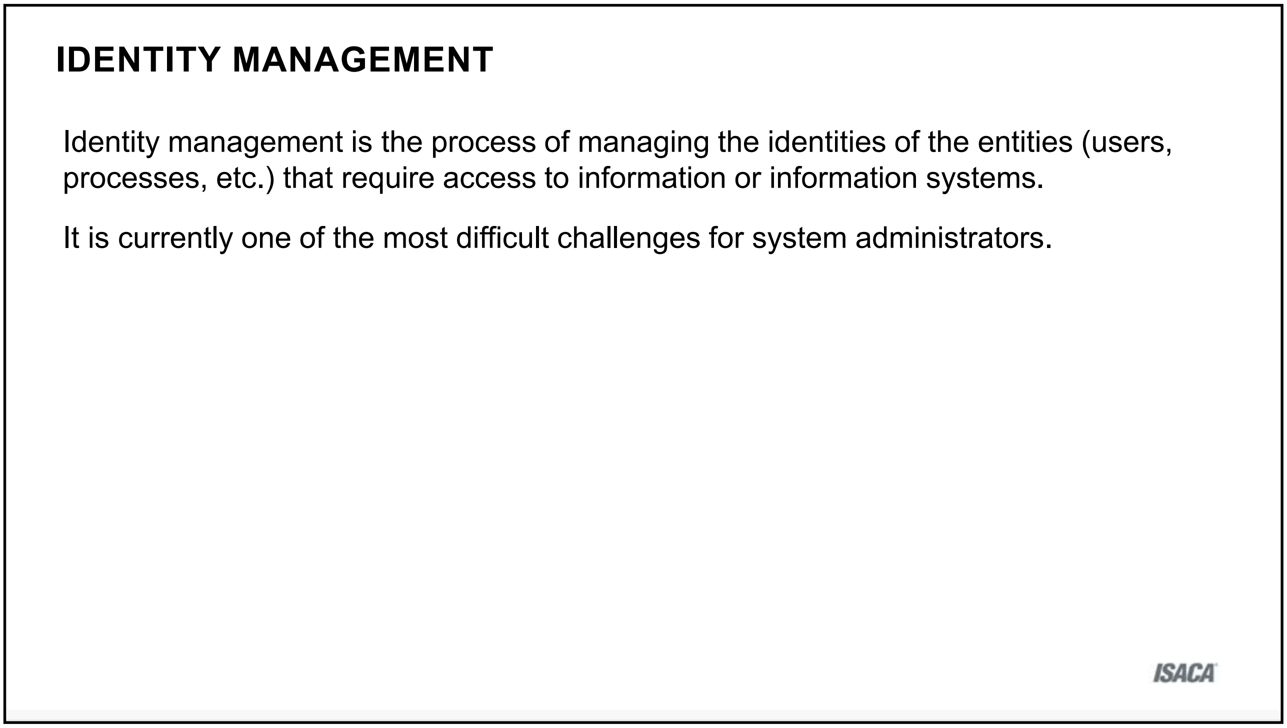
Risk is often caused through misuse of access, especially in cases where an individual has a level of access that is not appropriate for his or her current job responsibilities.



THE IAAA MODEL

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

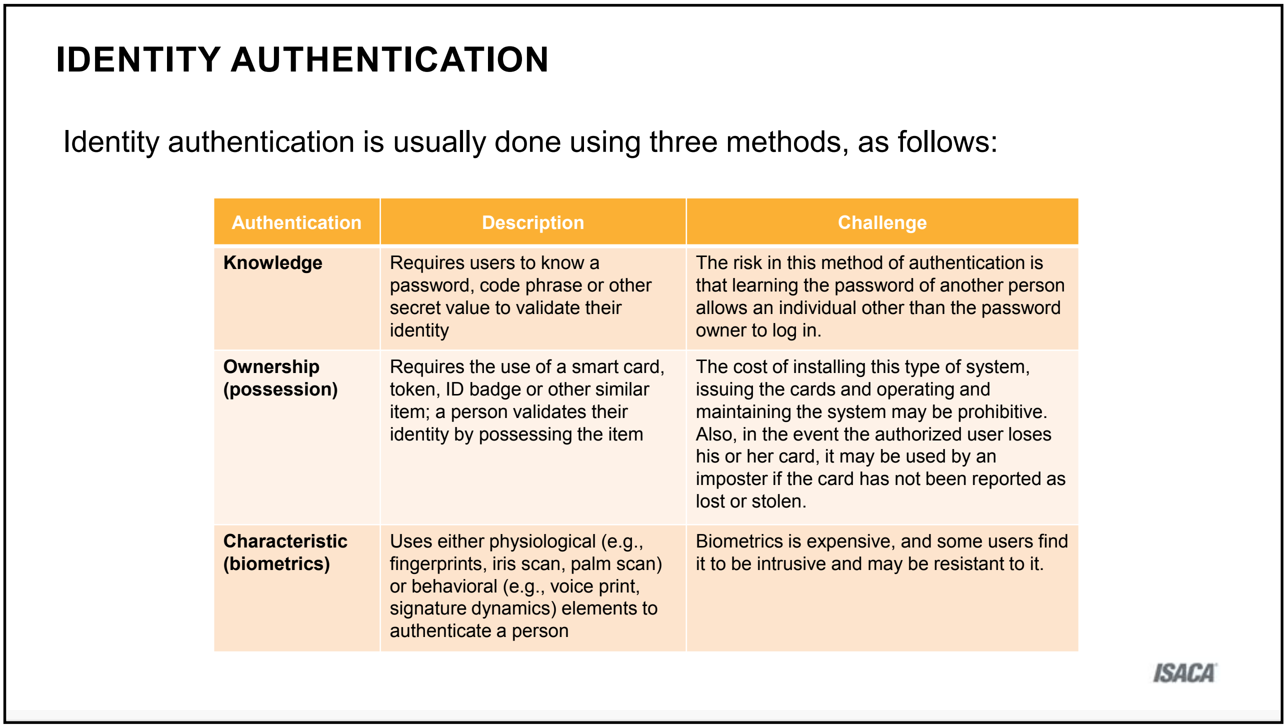
Identification	The unique identification of each person or process that uses a system allows tracking and logging of the activity by the user and the possibility to investigate a problem if it were to arise.
Authentication	Authentication is the process of validating an identity. After a person or process 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.

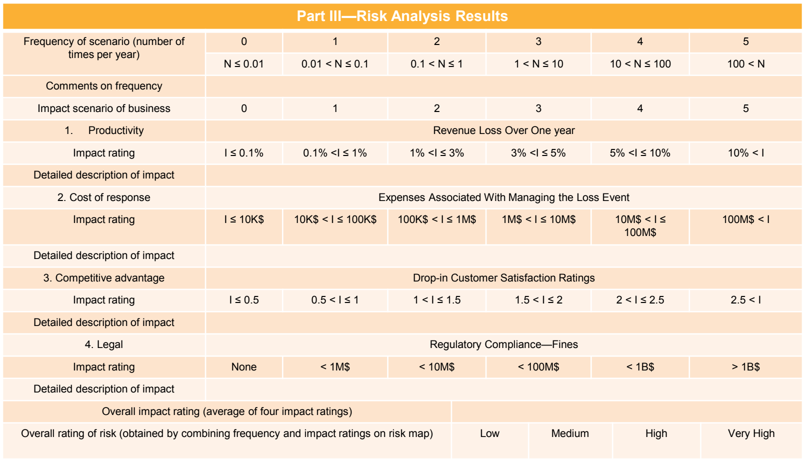
TASK 2.6 SUMMARY

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

An important task of the risk practitioner is to manage risk on a continuous, not just a one-time, basis.

TASK 2.6 ACTIVITY

Complete Part III of your risk register, adding information about your risk scenario.



Part III—Risk Analysis Results						
Frequency of scenario (number of times per year)	0	1	2	3	4	5
	N ≤ 0.01	0.01 < N ≤ 0.1	0.1 < N ≤ 1	1 < N ≤ 10	10 < N ≤ 100	100 < N
Comments on frequency						
Impact scenario of business	0	1	2	3	4	5
1. Productivity	Revenue Loss Over One year					
Impact rating	I ≤ 0.1%	0.1% <I ≤ 1%	1% <I ≤ 3%	3% <I ≤ 5%	5% <I ≤ 10%	10% < I
Detailed description of impact						
2. Cost of response	Expenses Associated With Managing the Loss Event					
Impact rating	I ≤ 10K$	10K$ < I ≤ 100K$	100K$ < I ≤ 1M$	1M$ < I ≤ 10M$	10M$ < I ≤ 100M$	100M$ < I
Detailed description of impact						
3. Competitive advantage	Drop-in Customer Satisfaction Ratings					
Impact rating	I ≤ 0.5	0.5 < I ≤ 1	1 < I ≤ 1.5	1.5 < I ≤ 2	2 < I ≤ 2.5	2.5 < I
Detailed description of impact						
4. Legal	Regulatory Compliance—Fines					
Impact rating	None	< 1M$	< 10M$	< 100M$	< 1B$	> 1B$
Detailed description of impact						
Overall impact rating (average of four impact ratings)						
Overall rating of risk (obtained by combining frequency and impact ratings on risk map)			Low	Medium	High	Very High

DISCUSSION QUESTION

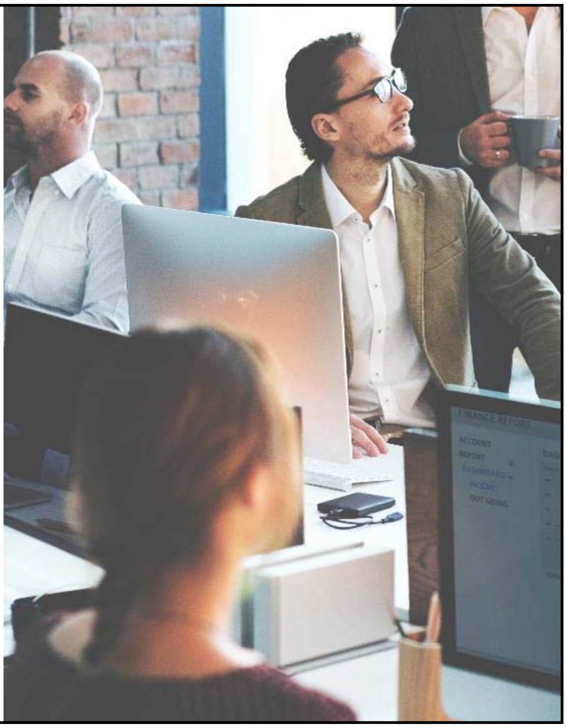
Risk assessments should be repeated at regular intervals because:

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

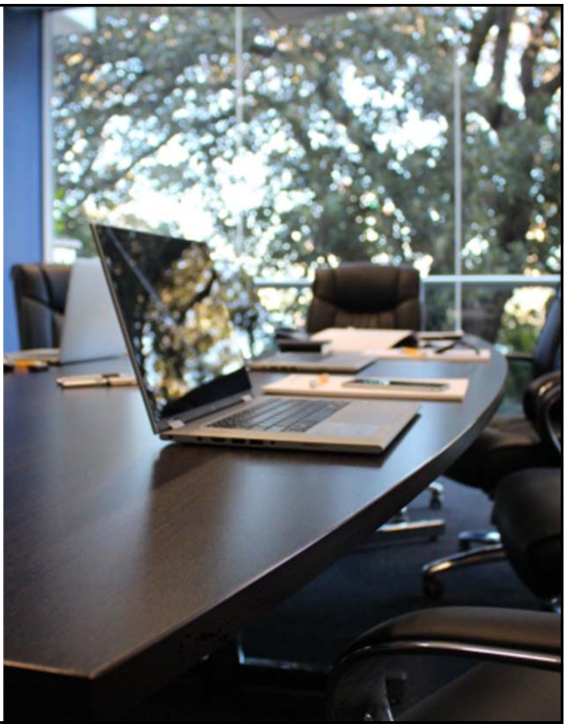
Once a risk assessment has been completed, the documented test results should be:

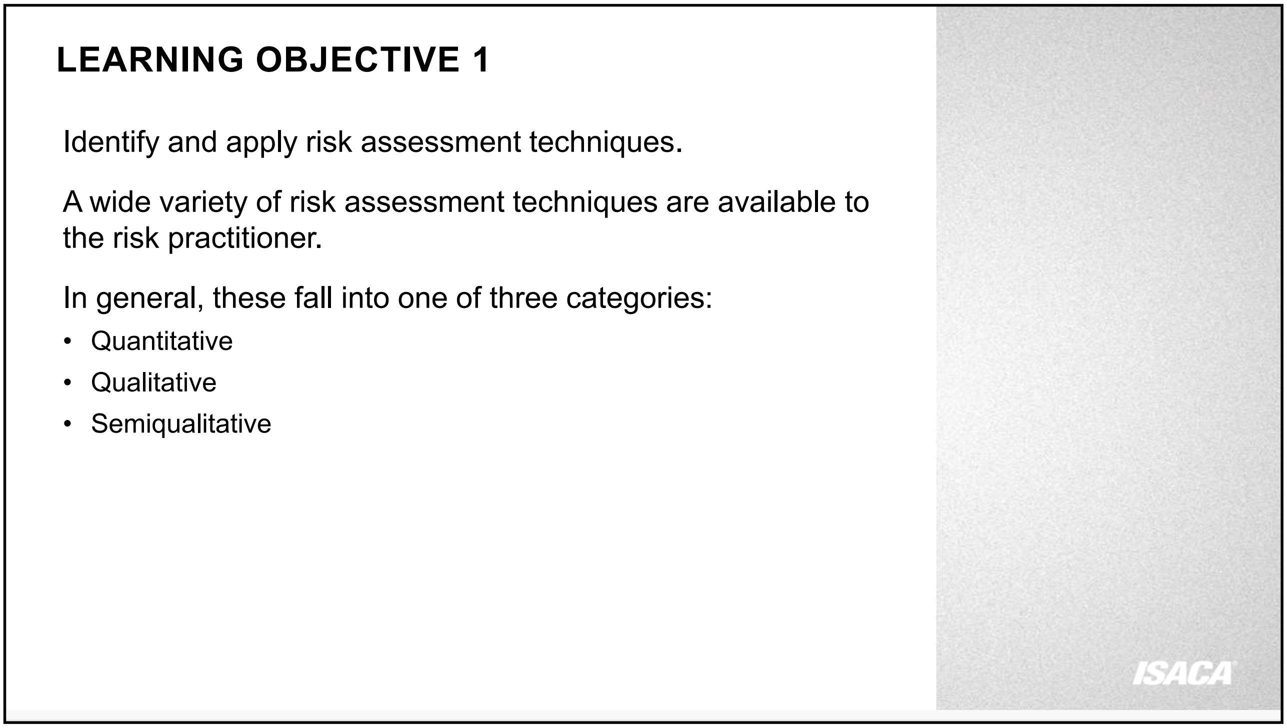
A. destroyed.

B. retained.

C. summarized.

D. published.





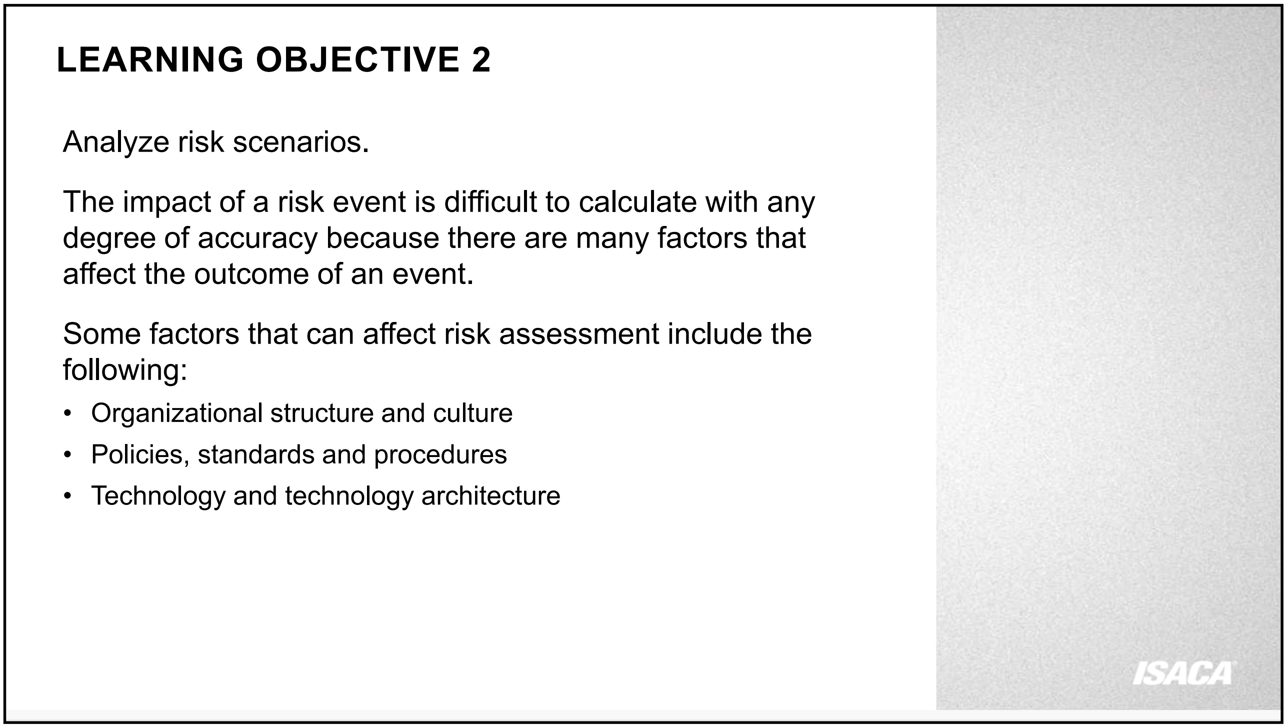
LEARNING OBJECTIVE 1

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



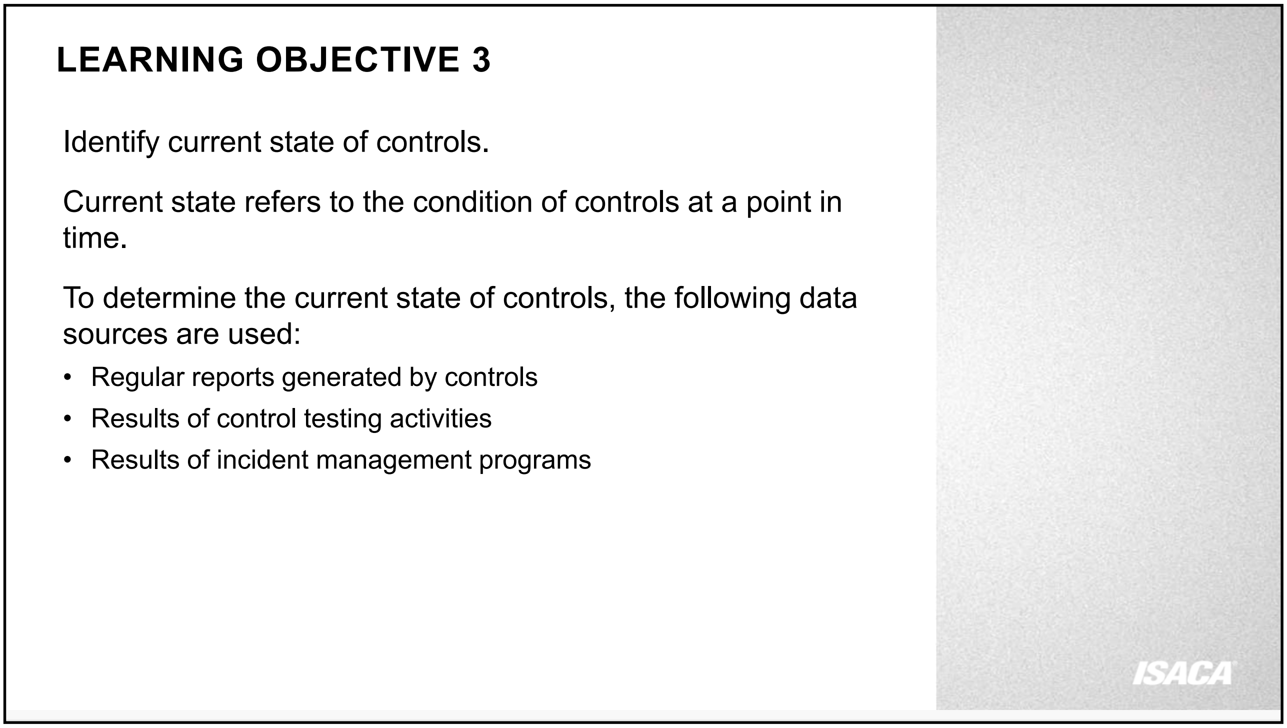
LEARNING OBJECTIVE 2

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



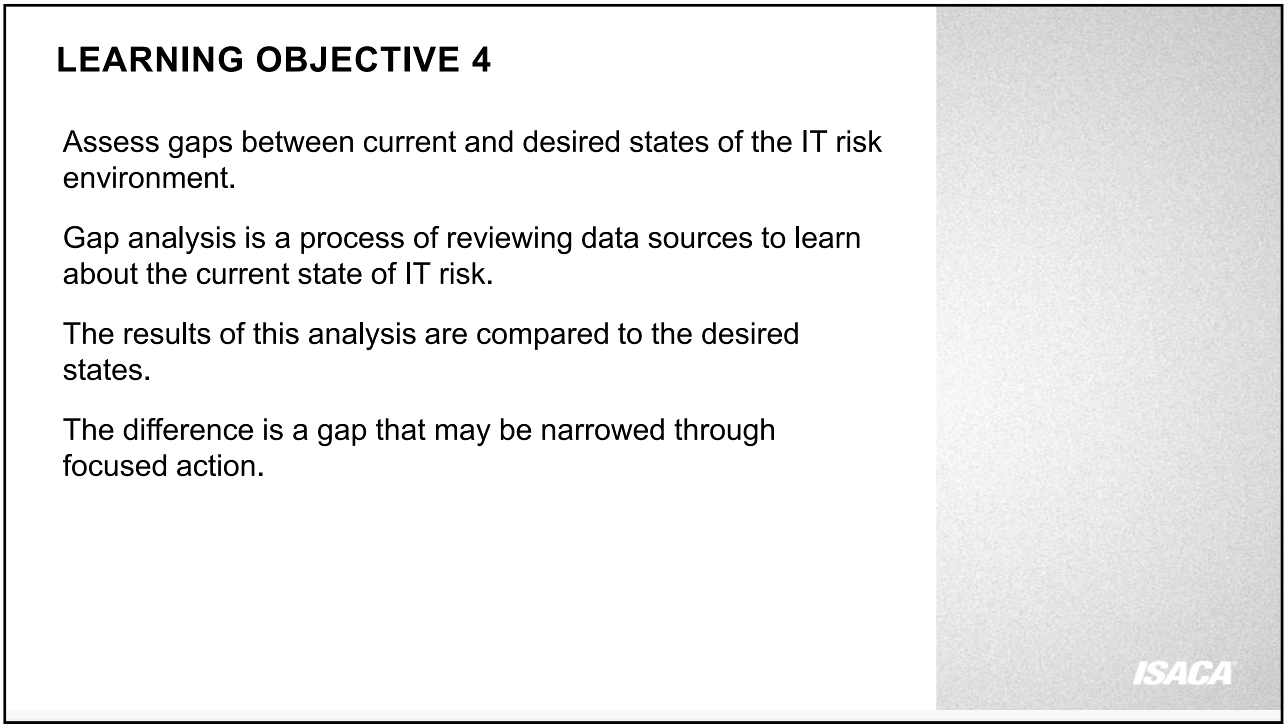
LEARNING OBJECTIVE 3

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



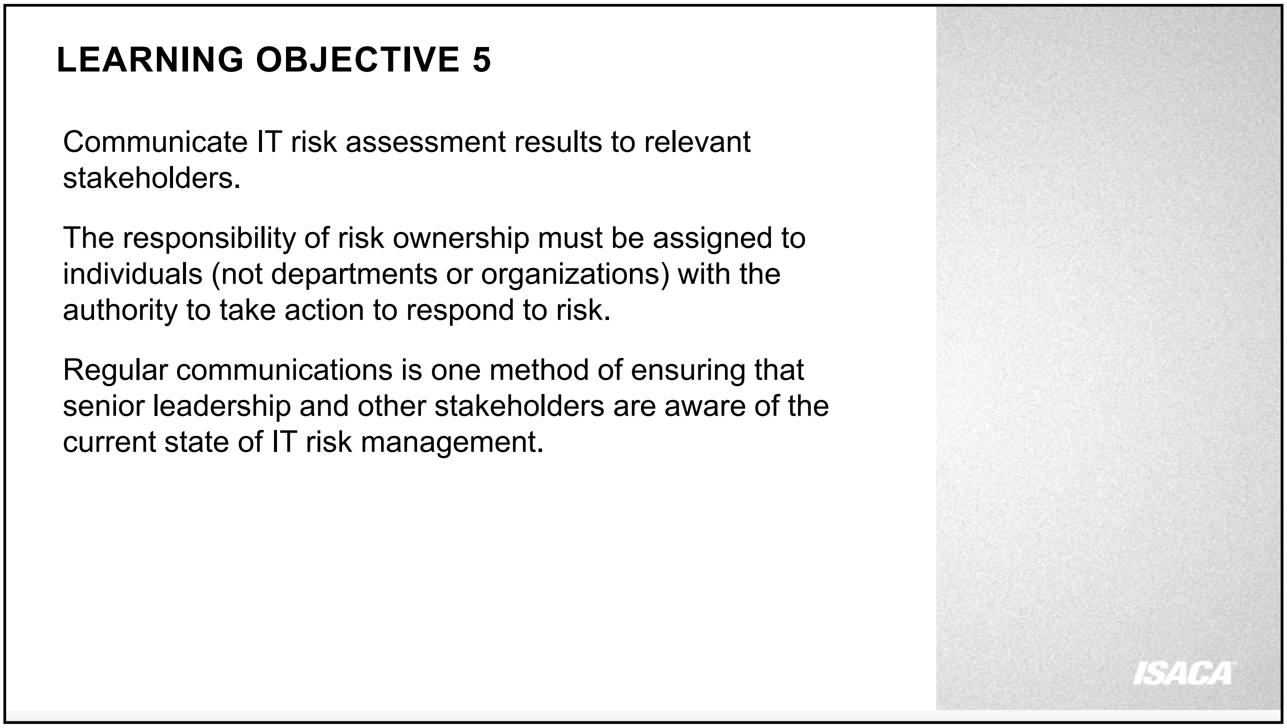
LEARNING OBJECTIVE 4

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.

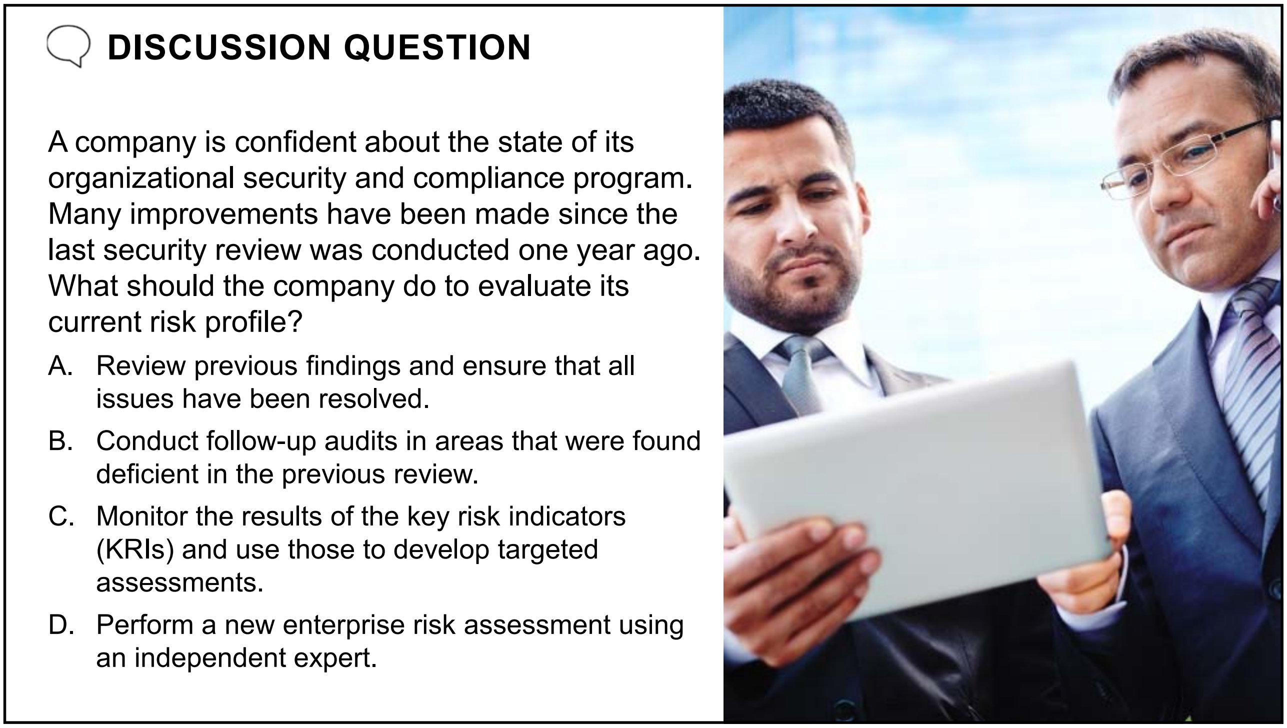


LEARNING OBJECTIVE 5

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.



DISCUSSION QUESTION

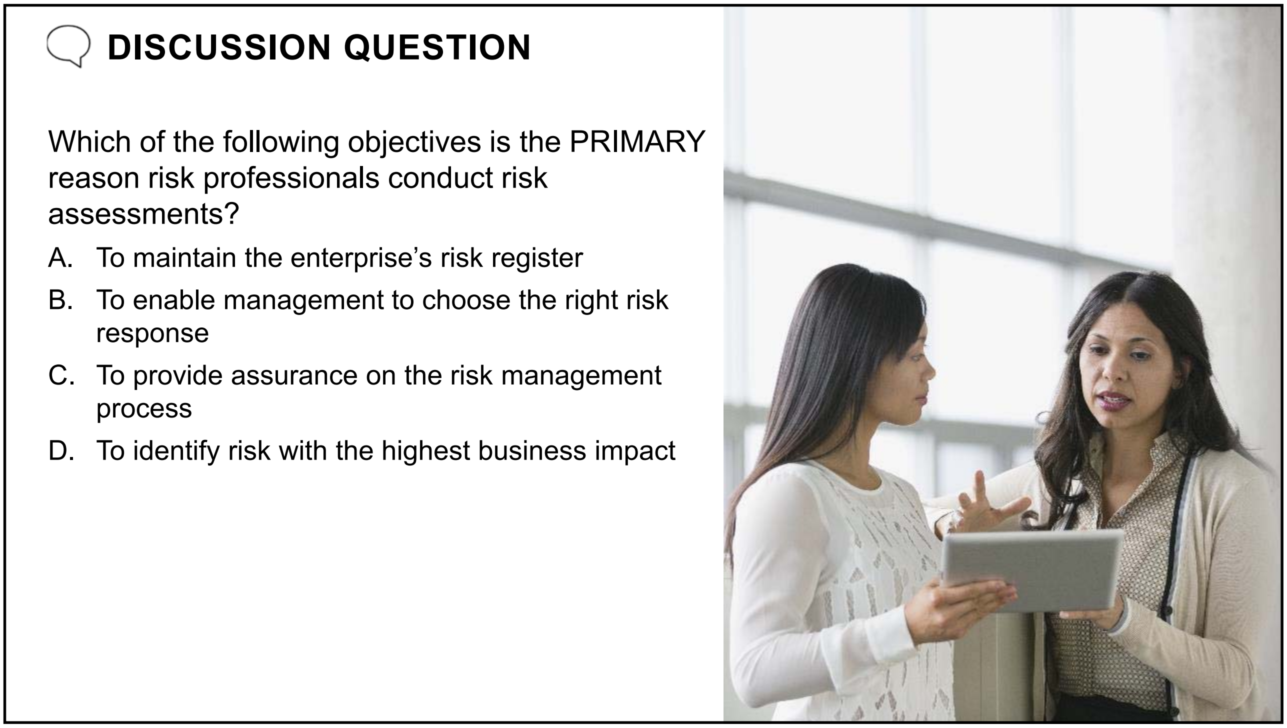
A company is confident about the state of its organizational security and compliance program. Many improvements have been made since the last security review was conducted one year ago. What should the company do to evaluate its current risk profile?

A. Review previous findings and ensure that all issues have been resolved.

B. Conduct follow-up audits in areas that were found deficient in the previous review.

C. Monitor the results of the key risk indicators (KRIs) and use those to develop targeted assessments.

D. Perform a new enterprise risk assessment using an independent expert.



DISCUSSION QUESTION

Which of the following objectives is the PRIMARY reason risk professionals conduct risk assessments?

A. To maintain the enterprise’s risk register

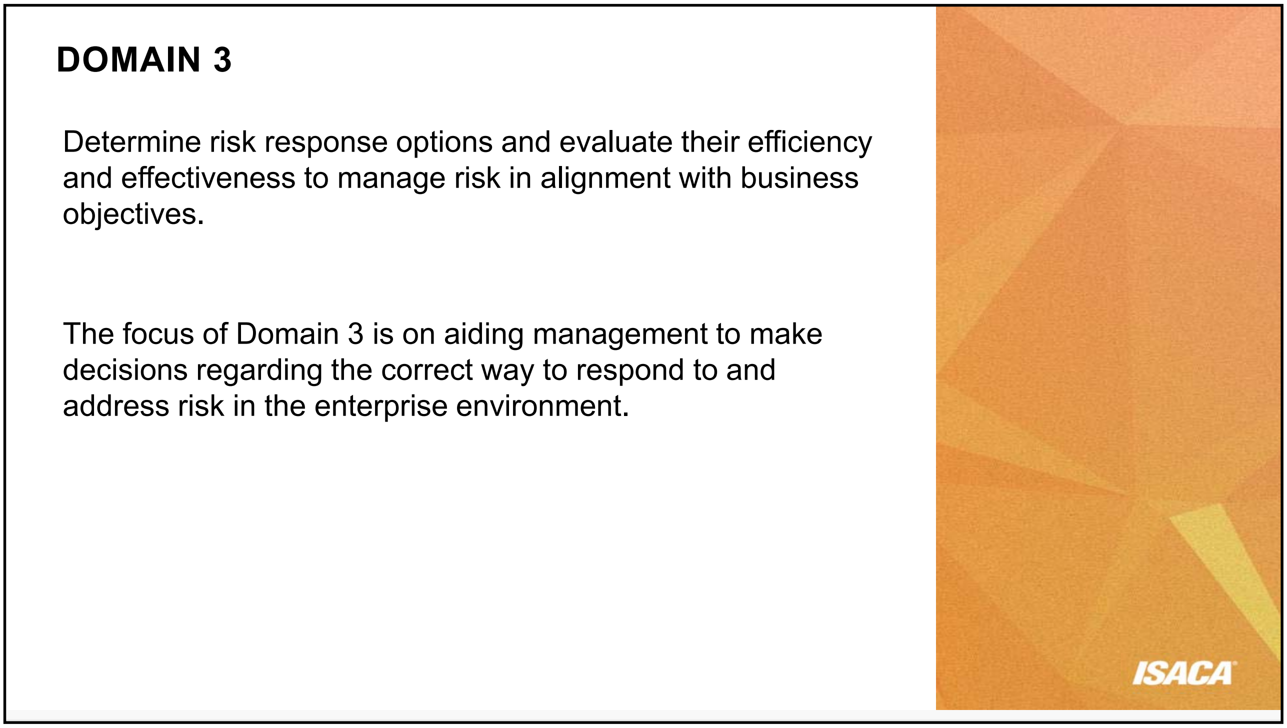
B. To enable management to choose the right risk response

C. To provide assurance on the risk management process

D. To identify risk with the highest business impact

DOMAIN 3

RISK RESPONSE AND MITIGATION



DOMAIN 3

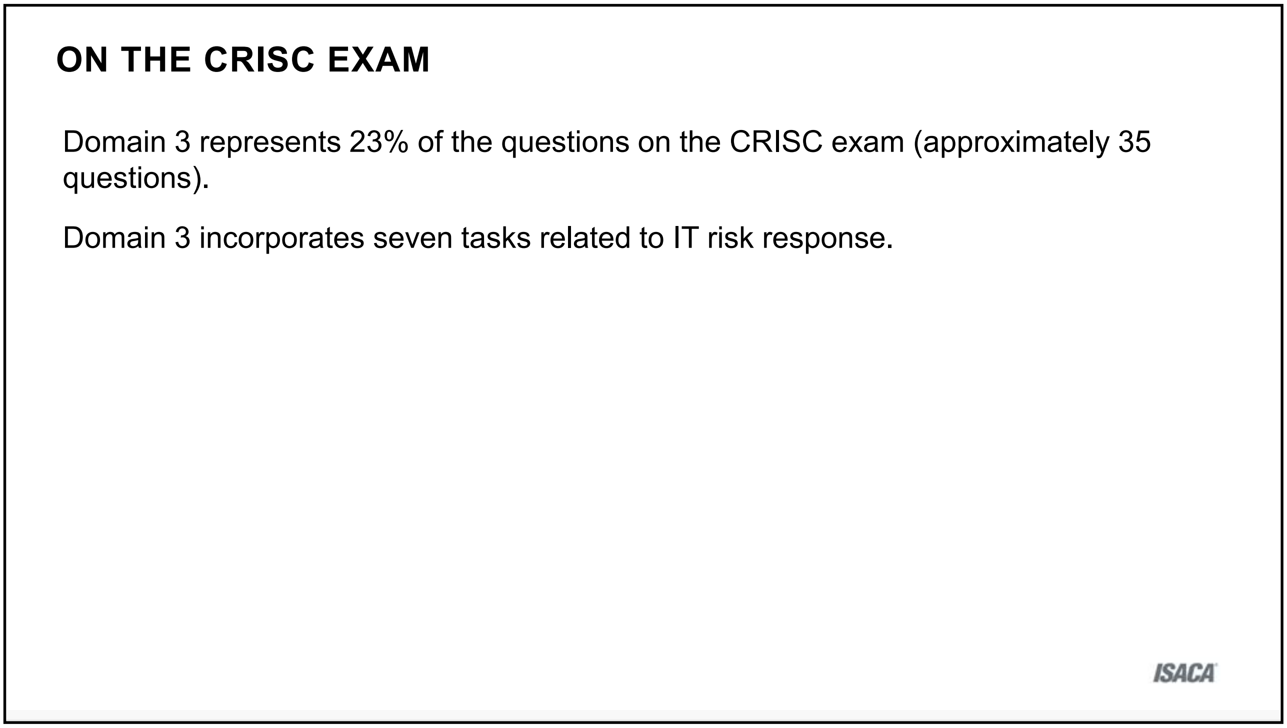
Determine risk response options and evaluate their efficiency and effectiveness to manage risk in alignment with business objectives.

The focus of Domain 3 is on aiding management to make decisions regarding the correct way to respond to and address risk in the enterprise environment.

LEARNING OBJECTIVES

The objective of this domain is to ensure that the CRISC candidate has the knowledge necessary to:

1. List the different risk response options.
2. Define various parameters for risk response selection
3. Explain how residual risk relates to inherent risk, risk appetite and risk tolerance.
4. Discuss the need for performing a cost-benefit analysis when determining a risk response.
5. Develop a risk action plan.
6. Explain the principles of risk ownership.
7. Leverage understanding of the system development life cycle (SDLC) process to implement IS controls efficiently and effectively.
8. Understand the need for control maintenance.

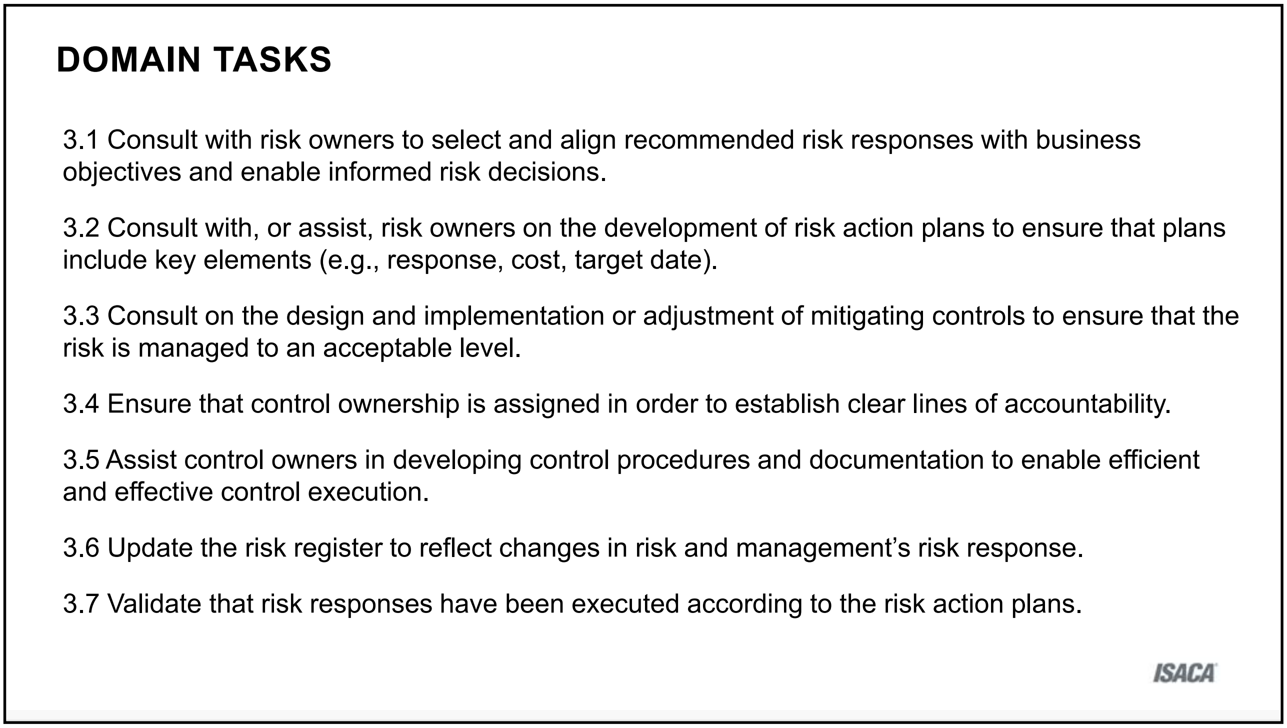


ON THE CRISC EXAM

Domain 3 represents 23% of the questions on the CRISC exam (approximately 35 questions).

Domain 3 incorporates seven tasks related to IT risk response.

ISACA



DOMAIN TASKS

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 in order to establish clear lines of accountability.

3.5 Assist control owners in developing control procedures and documentation to enable efficient and effective control execution.

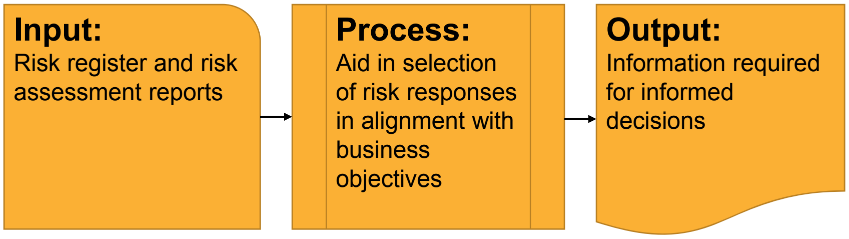
3.6 Update the risk register to reflect changes in risk and management’s risk response.

3.7 Validate that risk responses have been executed according to the risk action plans.

TASK 3.1

Consult with risk owners to select and align recommended risk responses with business objectives and enable informed risk decisions.

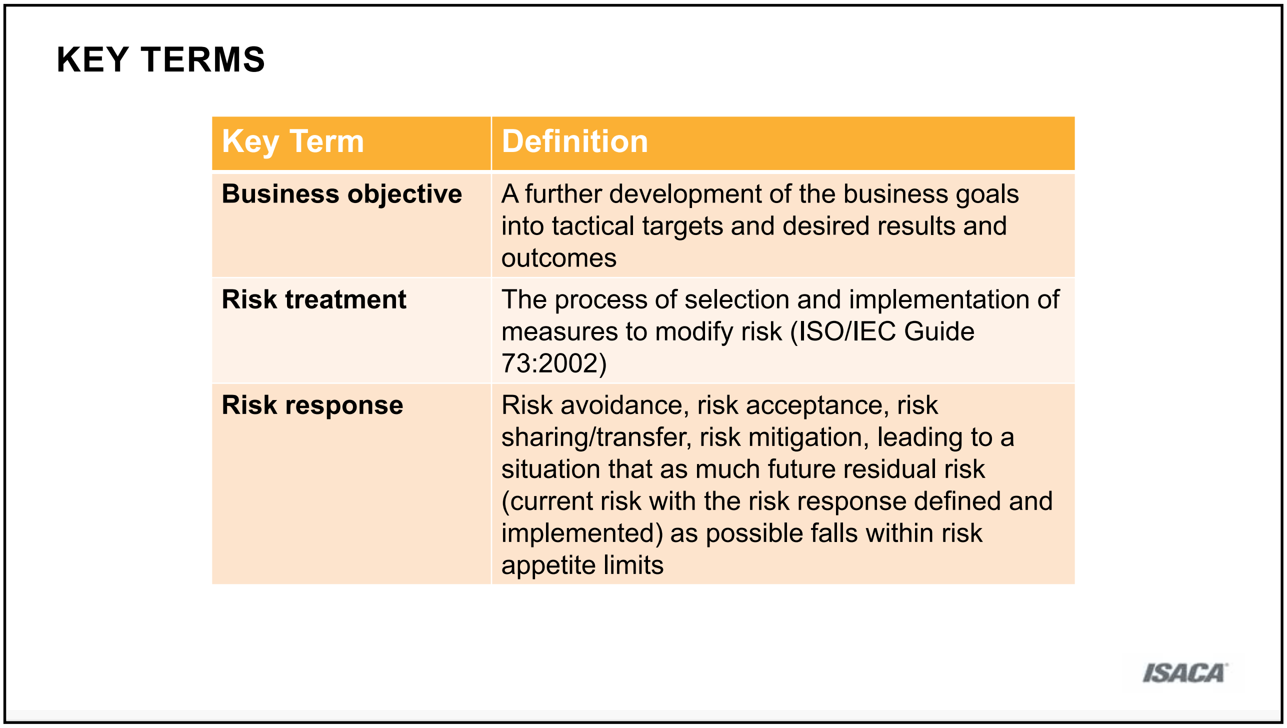
FOCUS ON TASK 3.1



Input:
Risk register and risk assessment reports

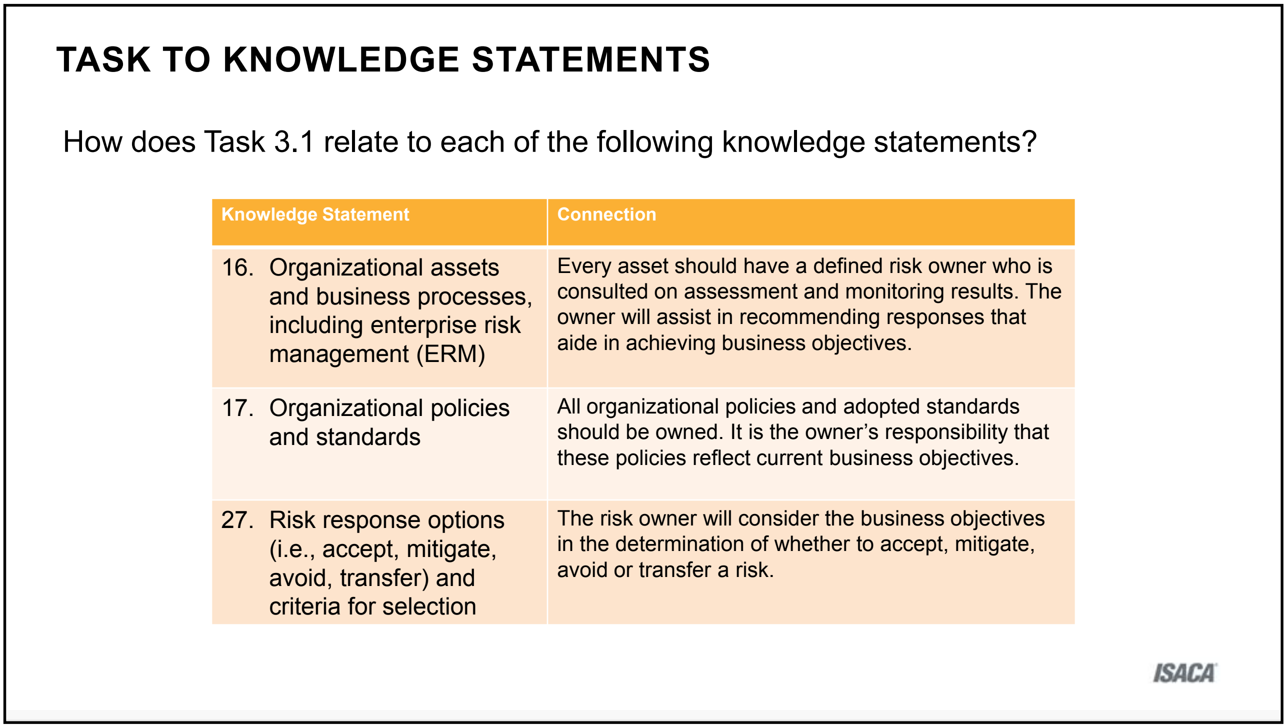
Process:
Aid in selection of risk responses in alignment with business objectives

Output:
Information required for informed decisions



KEY TERMS

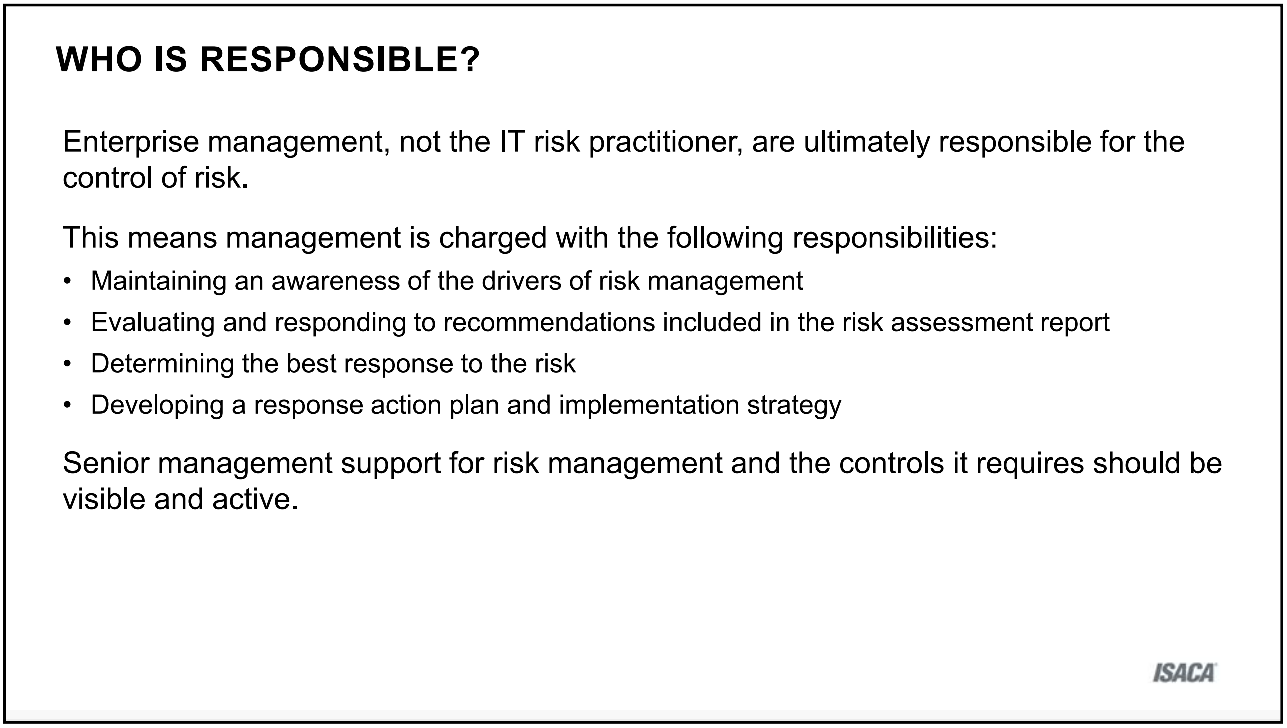
Key Term	Definition
Business objective	A further development of the business goals into tactical targets and desired results and outcomes
Risk treatment	The process of selection and implementation of measures to modify risk (ISO/IEC Guide 73:2002)
Risk response	Risk avoidance, risk acceptance, risk sharing/transfer, risk mitigation, leading to a situation that as much future residual risk (current risk with the risk response defined and implemented) as possible falls within risk appetite limits



TASK TO KNOWLEDGE STATEMENTS

How does Task 3.1 relate to each of the following knowledge statements?

Knowledge Statement	Connection
16. Organizational assets and business processes, including enterprise risk management (ERM)	Every asset should have a defined risk owner who is consulted on assessment and monitoring results. The owner will assist in recommending responses that aide in achieving business objectives.
17. Organizational policies and standards	All organizational policies and adopted standards should be owned. It is the owner's responsibility that these policies reflect current business objectives.
27. Risk response options (i.e., accept, mitigate, avoid, transfer) and criteria for selection	The risk owner will consider the business objectives in the determination of whether to accept, mitigate, avoid or transfer a risk.



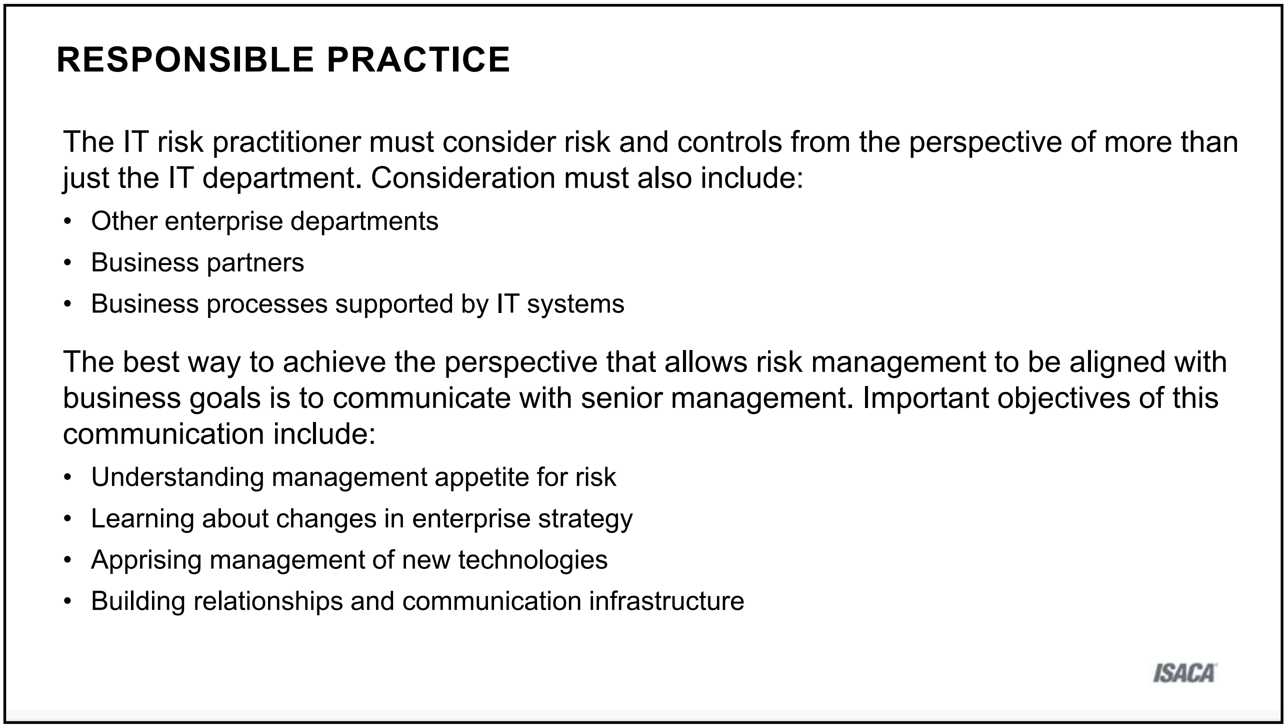
WHO IS RESPONSIBLE?

Enterprise management, not the IT risk practitioner, are ultimately responsible for the control of risk.

This means management is charged with the following responsibilities:

- Maintaining an awareness of the drivers of risk management
- Evaluating and responding to recommendations included in the risk assessment report
- Determining the best response to the risk
- Developing a response action plan and implementation strategy

Senior management support for risk management and the controls it requires should be visible and active.



RESPONSIBLE PRACTICE

The IT risk practitioner must consider risk and controls from the perspective of more than just the IT department. Consideration must also include:

- Other enterprise departments
- Business partners
- Business processes supported by IT systems

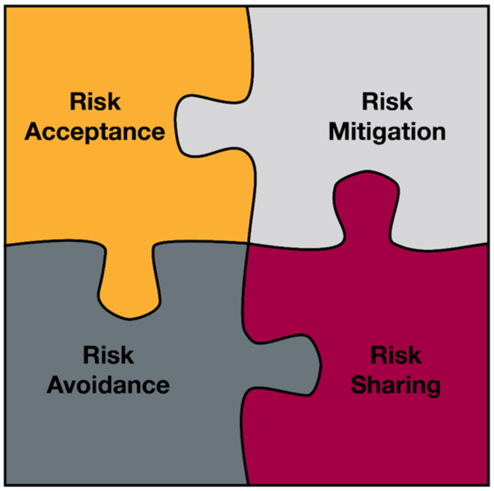
The best way to achieve the perspective that allows risk management to be aligned with business goals is to communicate with senior management. Important objectives of this communication include:

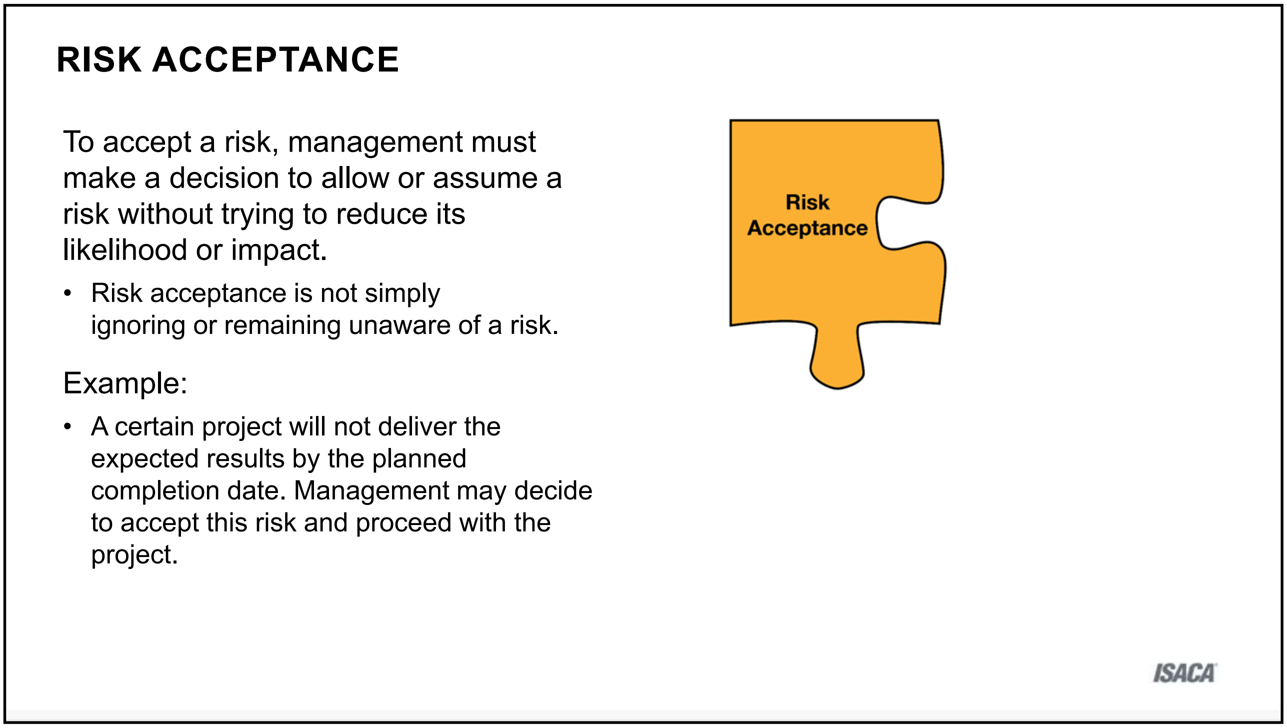
- Understanding management appetite for risk
- Learning about changes in enterprise strategy
- Apprising management of new technologies
- Building relationships and communication infrastructure

RISK TREATMENTS

The purpose of responding to risk is to bring risk in line with the defined risk appetite for the enterprise.

There are four commonly accepted categories of risk responses or "treatments."





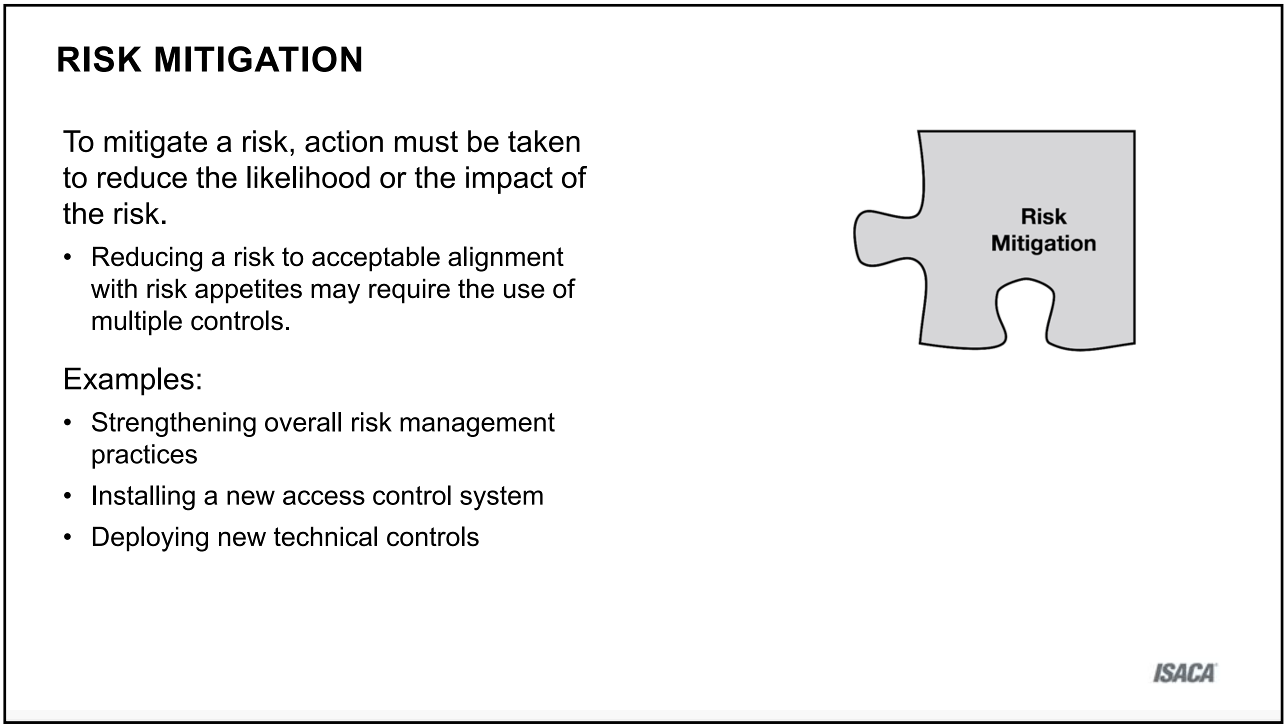
RISK ACCEPTANCE

To accept a risk, management must make a decision to allow or assume a risk without trying to reduce its likelihood or impact.

- Risk acceptance is not simply ignoring or remaining unaware of a risk.

Example:

- A certain project will not deliver the expected results by the planned completion date. Management may decide to accept this risk and proceed with the project.



RISK MITIGATION

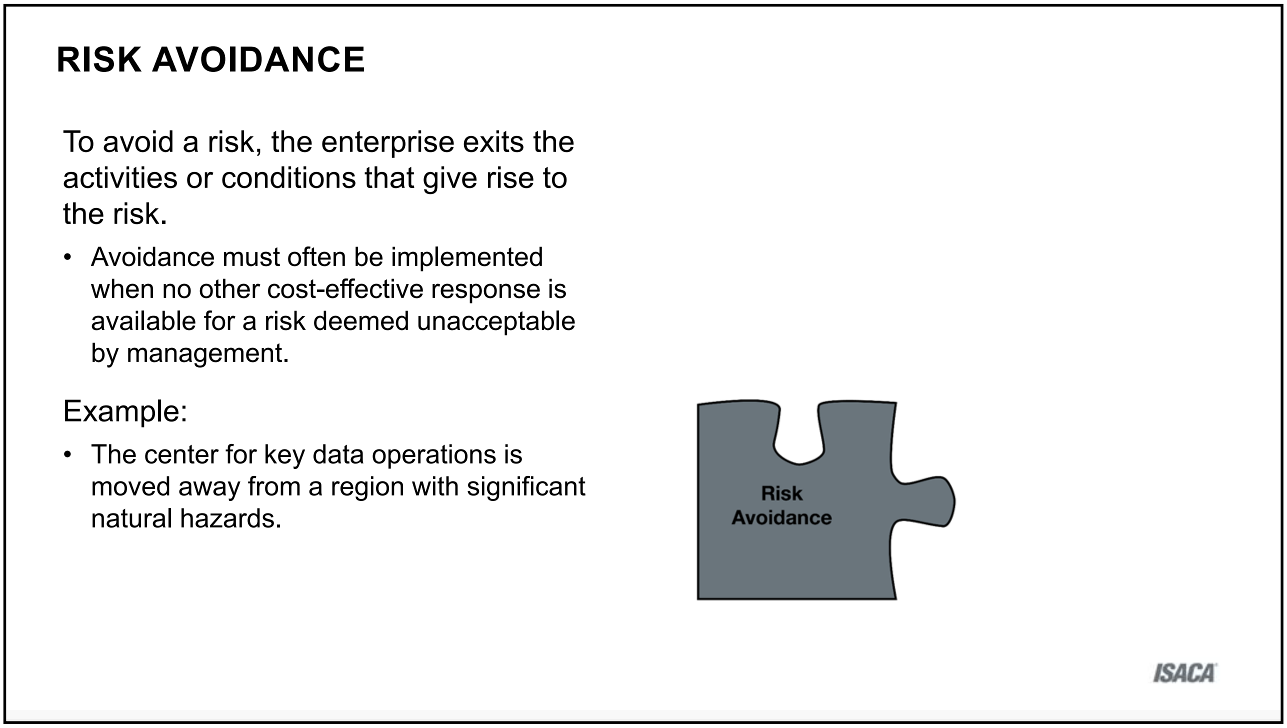
To mitigate a risk, action must be taken to reduce the likelihood or the impact of the risk.

- Reducing a risk to acceptable alignment with risk appetites may require the use of multiple controls.

Examples:

- Strengthening overall risk management practices
- Installing a new access control system
- Deploying new technical controls

Risk
Mitigation



RISK AVOIDANCE

To avoid a risk, the enterprise exits the activities or conditions that give rise to the risk.

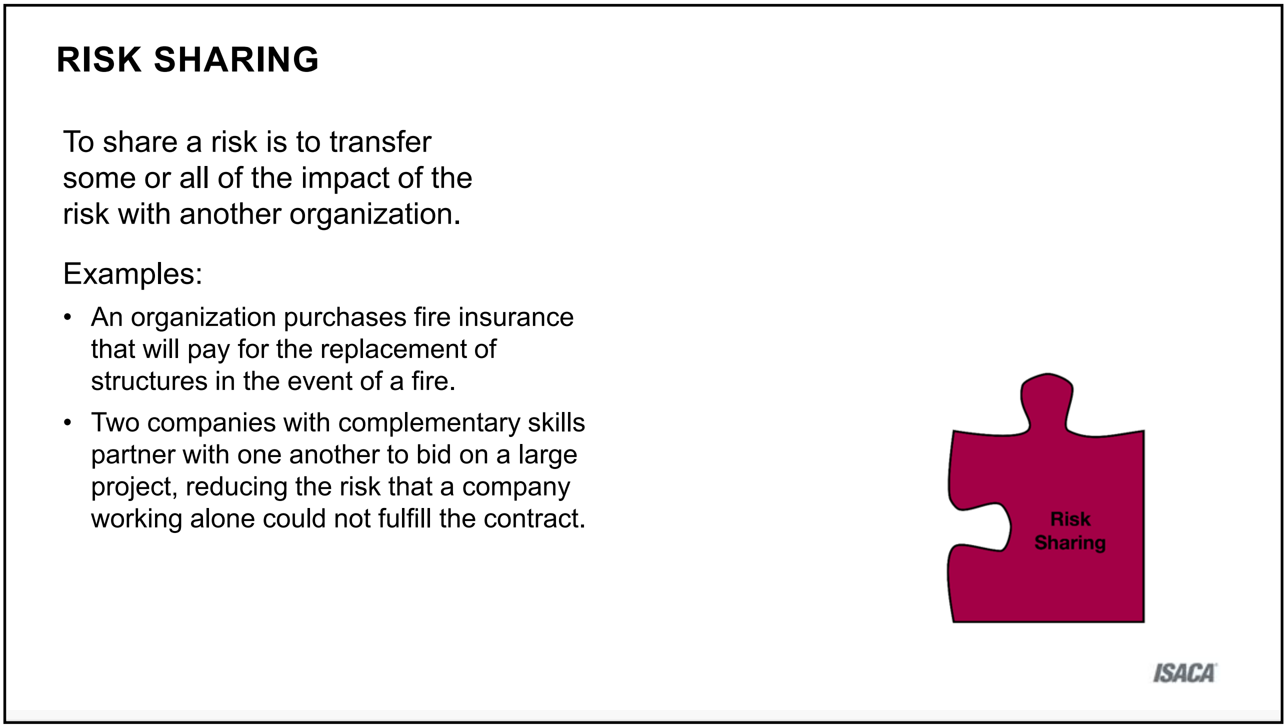
- Avoidance must often be implemented when no other cost-effective response is available for a risk deemed unacceptable by management.

Example:

- The center for key data operations is moved away from a region with significant natural hazards.

Risk Avoidance

ISACA



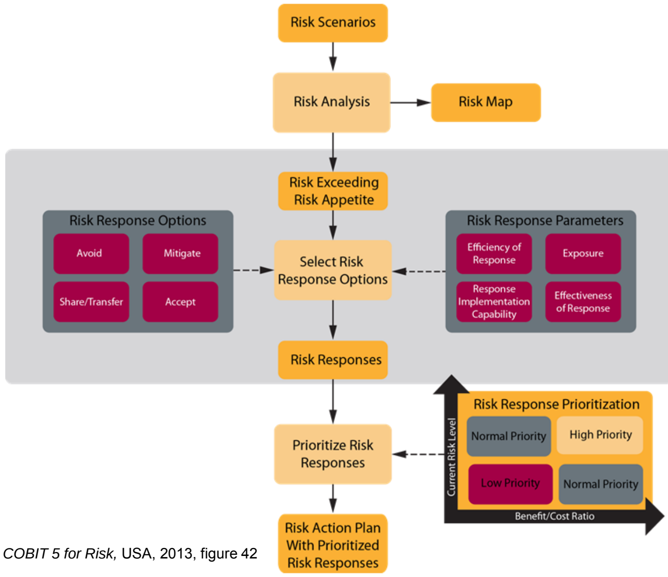
RISK SHARING

To share a risk is to transfer some or all of the impact of the risk with another organization.

Examples:

- An organization purchases fire insurance that will pay for the replacement of structures in the event of a fire.
- Two companies with complementary skills partner with one another to bid on a large project, reducing the risk that a company working alone could not fulfill the contract.

RISK RESPONSE PROCESS



Risk Scenarios

Risk Analysis

Risk Map

Risk Exceeding Risk Appetite

Risk Response Options

Avoid

Mitigate

Share/Transfer

Accept

Select Risk Response Options

Risk Response Parameters

Efficiency of Response

Exposure

Response Implementation Capability

Effectiveness of Response

Risk Responses

Prioritize Risk Responses

Risk Response Prioritization

Current Risk Level

Normal Priority

High Priority

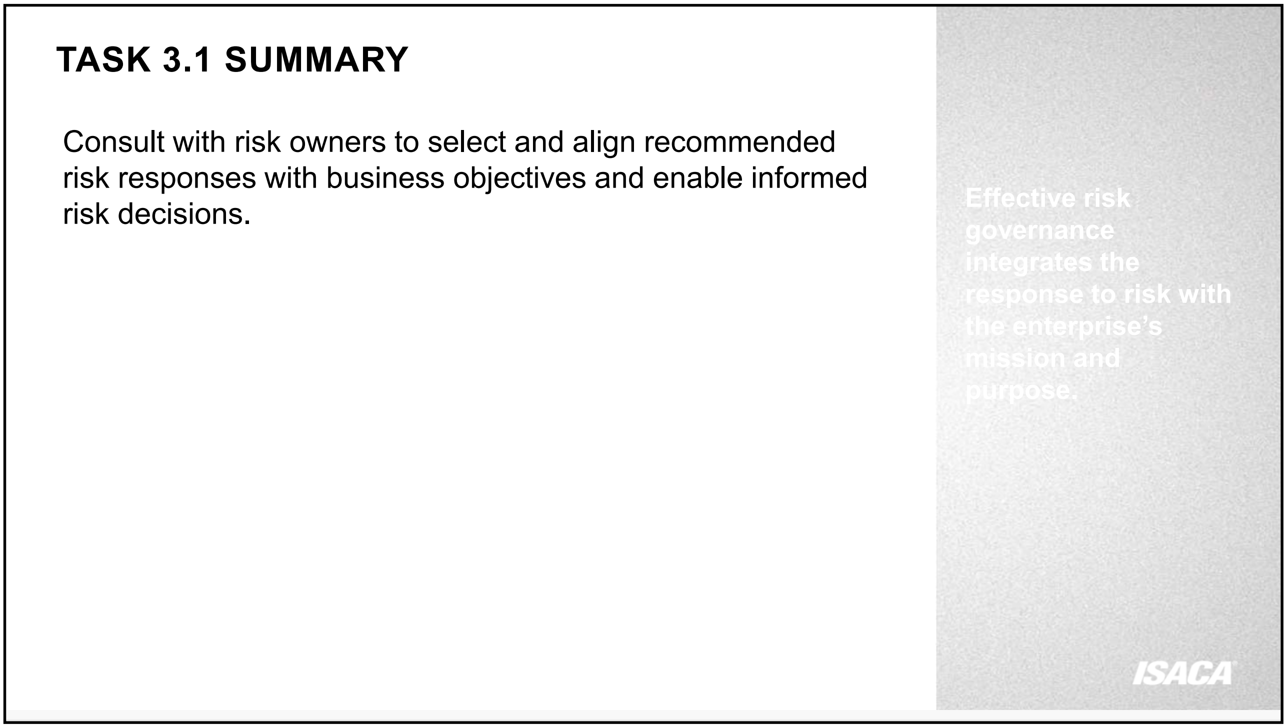
Low Priority

Normal Priority

Benefit/Cost Ratio

Risk Action Plan With Prioritized Risk Responses

Source: ISACA, *COBIT 5 for Risk*, USA, 2013, figure 42



TASK 3.1 SUMMARY

Consult with risk owners to select and align recommended risk responses with business objectives and enable informed risk decisions.

Effective risk governance integrates the response to risk with the enterprise's mission and purpose.

TASK 3.1 DISCUSSION

Review the following situation, then answer the question below.

Business Objective:

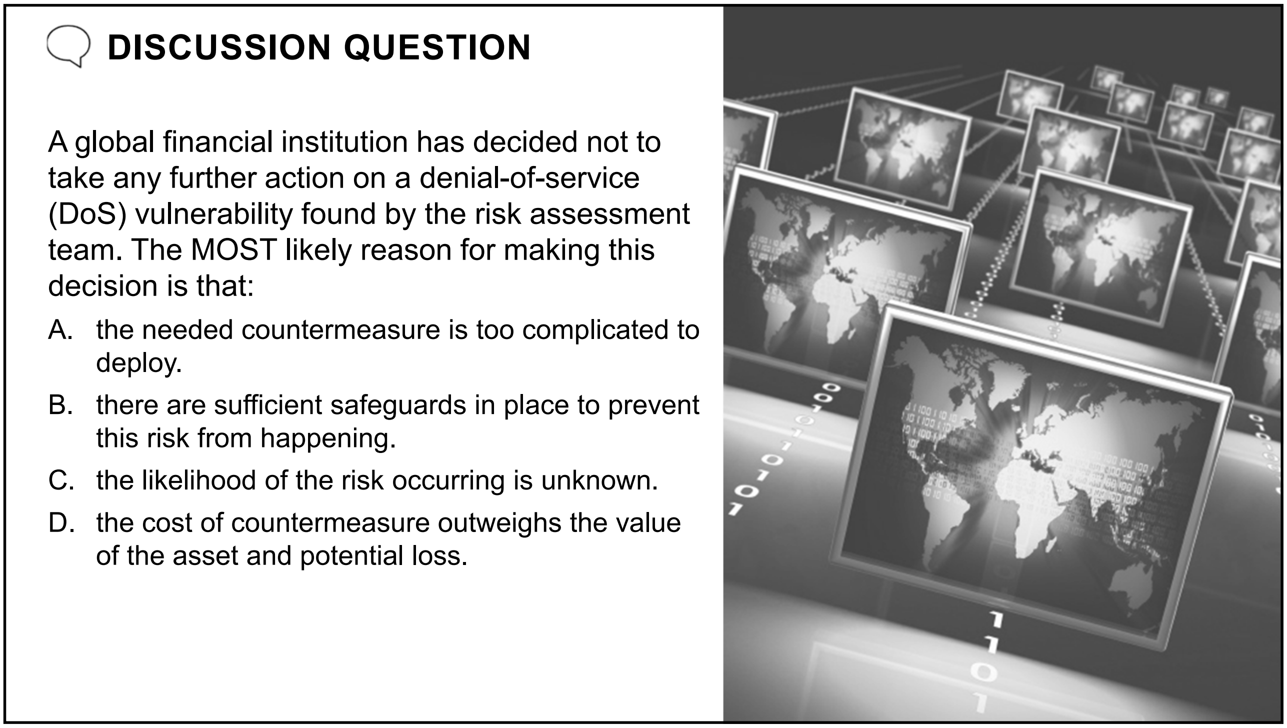
- Ensure the confidentiality, integrity and availability of our clients' personally identifying information (PII).

Output From Risk Evaluation:

- Clients' personally identifiable information is stored in a SQL 7 database that is not encrypted at rest.

Possible Risk Response Options:

- Upgrade from SQL7 to SQL8 Server
- Add a process of everyone with access to this information to annually sign a non-disclosure agreement and attend training on how to protect PII information
- Outsource the process that contains PII information to a 3rd party
- Which response best ensures that the business objective will be achieved? Support your opinion.



DISCUSSION QUESTION

A global financial institution has decided not to take any further action on a denial-of-service (DoS) vulnerability found by the risk assessment team. The MOST likely reason for making this decision is that:

A. the needed countermeasure is too complicated to deploy.

B. there are sufficient safeguards in place to prevent this risk from happening.

C. the likelihood of the risk occurring is unknown.

D. the cost of countermeasure outweighs the value of the asset and potential loss.

DISCUSSION QUESTION

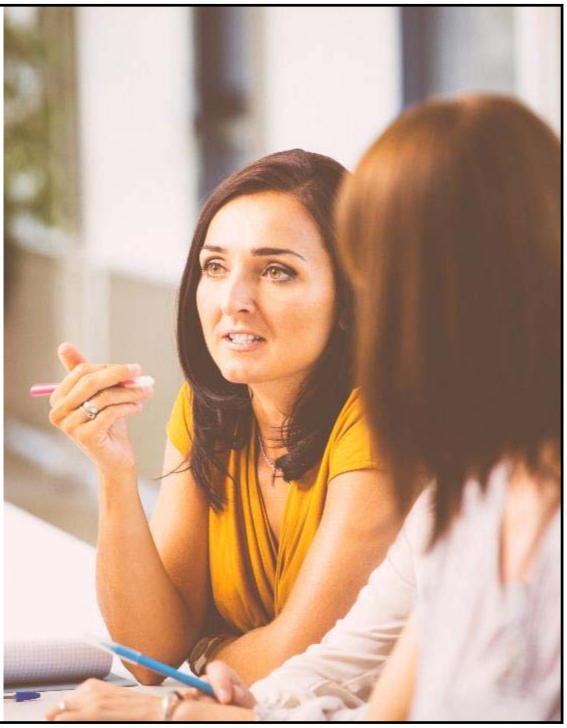
A risk response report includes recommendations for:

A. acceptance.

B. assessment.

C. evaluation.

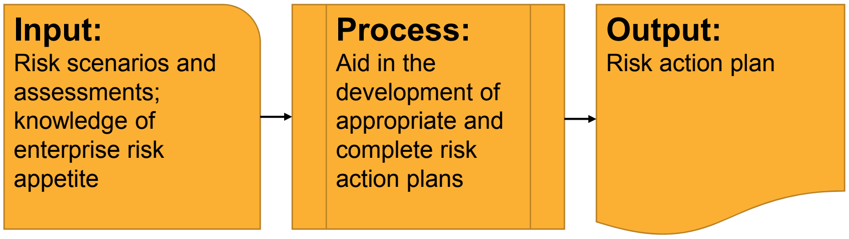
D. quantification.



TASK 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).

FOCUS ON TASK 3.2

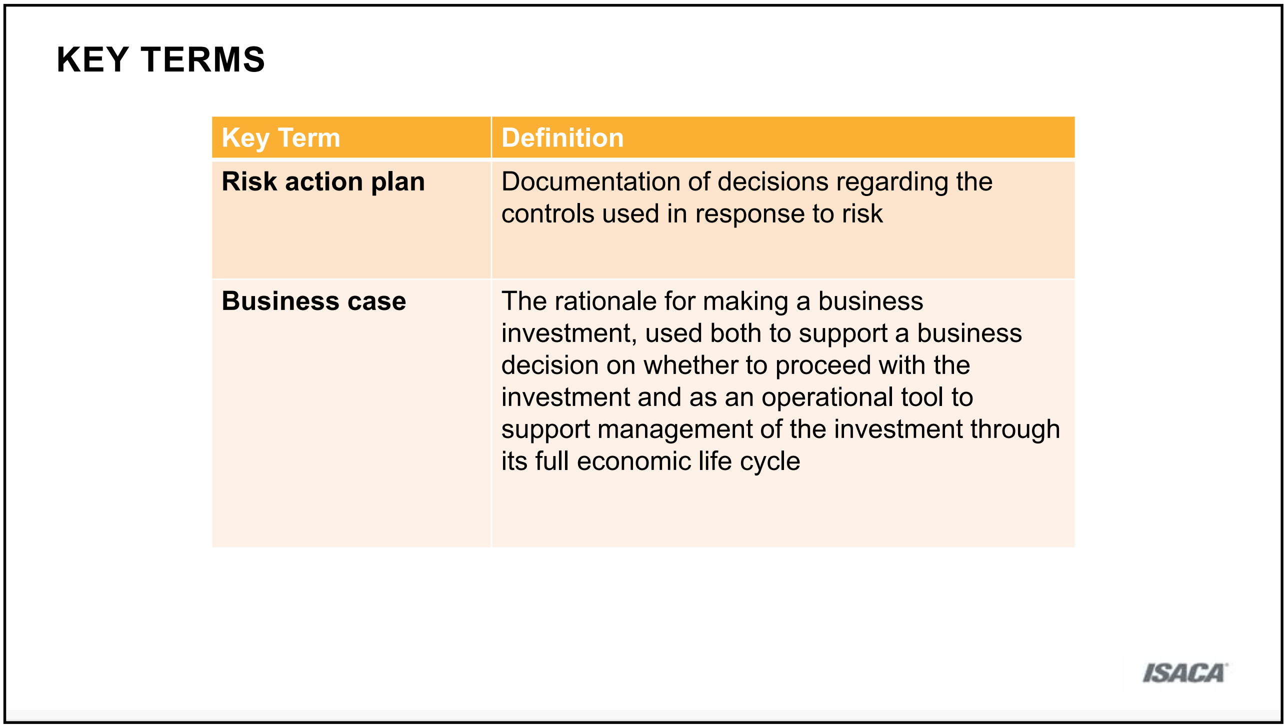


Input:
Risk scenarios and assessments; knowledge of enterprise risk appetite

Process:
Aid in the development of appropriate and complete risk action plans

Output:
Risk action plan

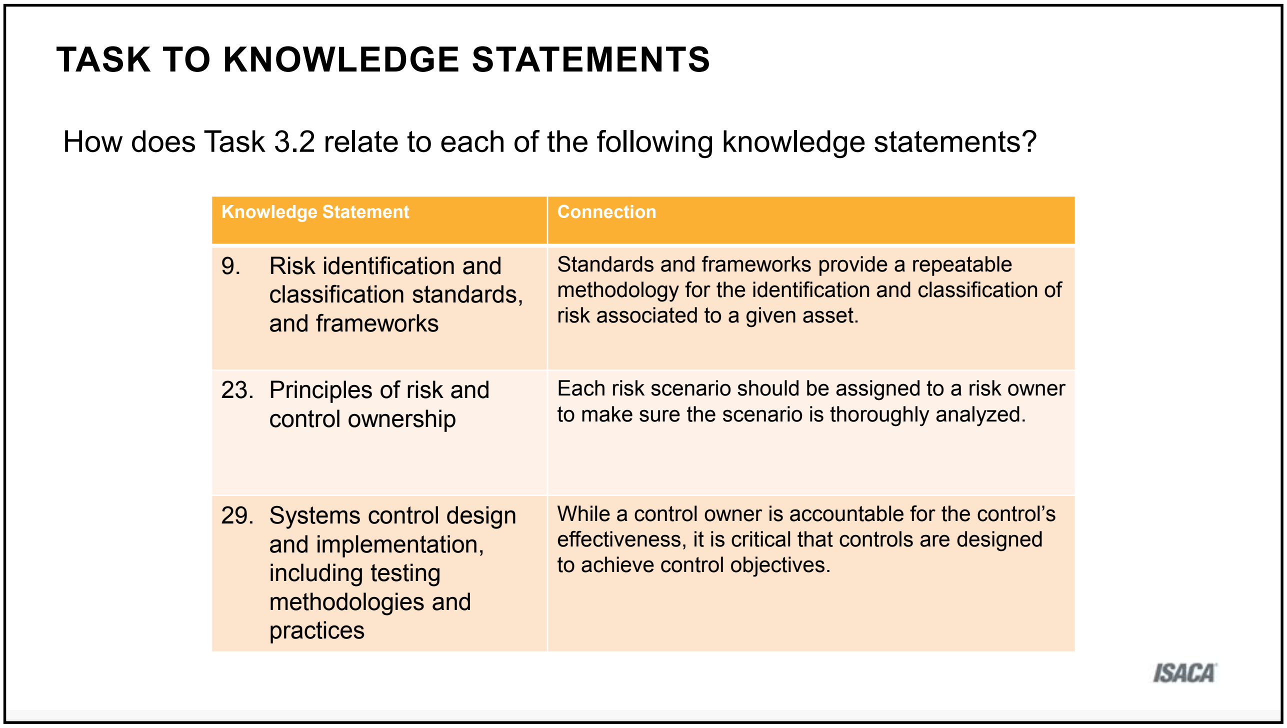
ISACA



KEY TERMS

Key Term	Definition
Risk action plan	Documentation of decisions regarding the controls used in response to risk
Business case	The rationale for making a business investment, used both to support a business decision on whether to proceed with the investment and as an operational tool to support management of the investment through its full economic life cycle

ISACA

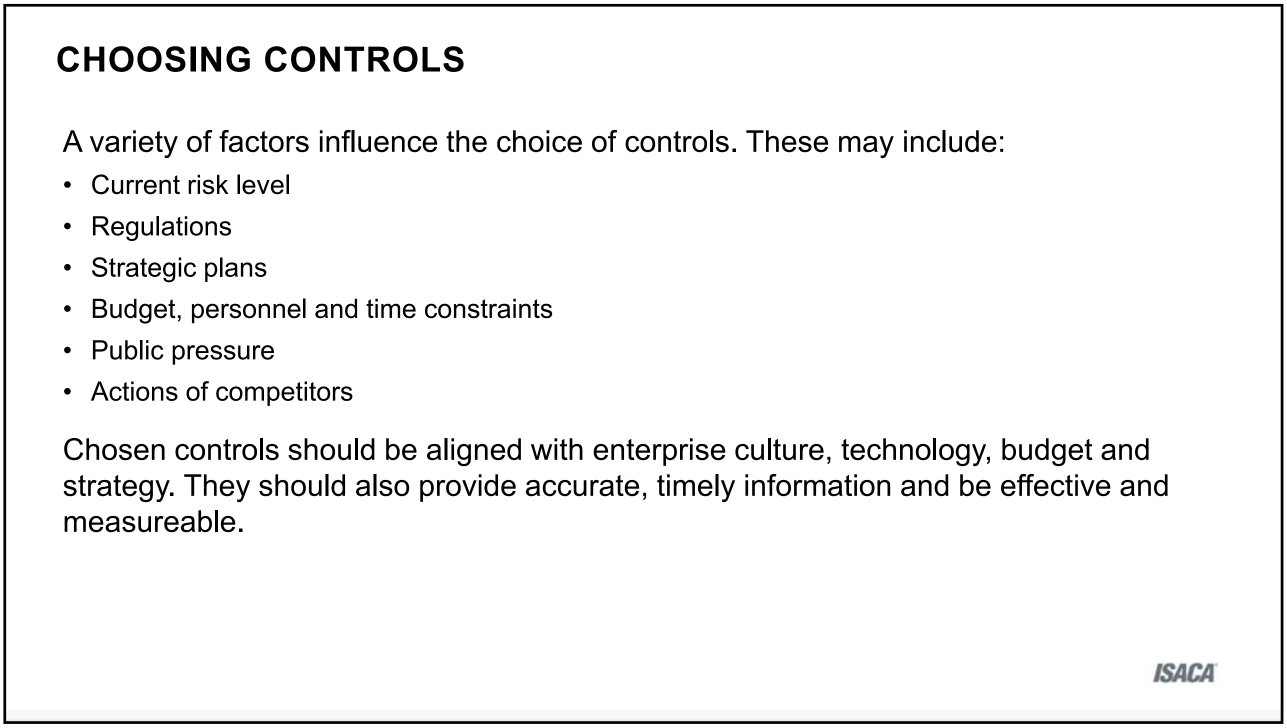


TASK TO KNOWLEDGE STATEMENTS

How does Task 3.2 relate to each of the following knowledge statements?

Knowledge Statement	Connection
9. Risk identification and classification standards, and frameworks	Standards and frameworks provide a repeatable methodology for the identification and classification of risk associated to a given asset.
23. Principles of risk and control ownership	Each risk scenario should be assigned to a risk owner to make sure the scenario is thoroughly analyzed.
29. Systems control design and implementation, including testing methodologies and practices	While a control owner is accountable for the control's effectiveness, it is critical that controls are designed to achieve control objectives.

ISACA

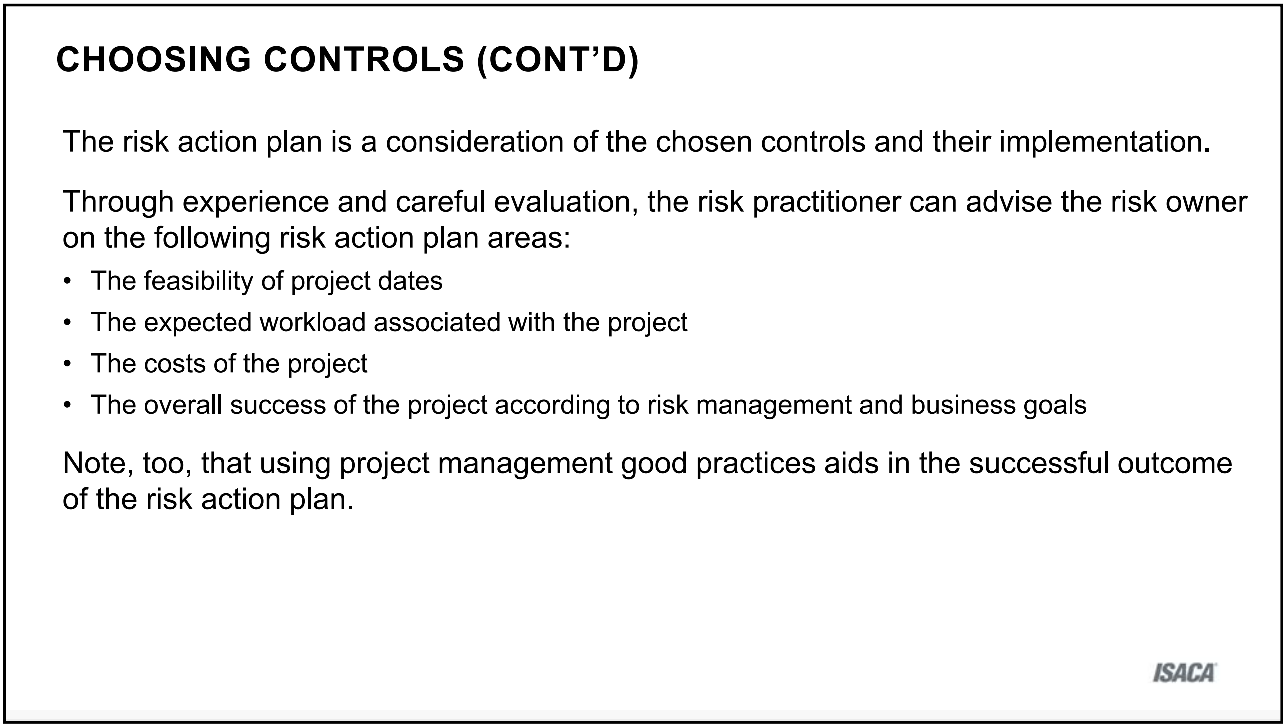


CHOOSING CONTROLS

A variety of factors influence the choice of controls. These may include:

- Current risk level
- Regulations
- Strategic plans
- Budget, personnel and time constraints
- Public pressure
- Actions of competitors

Chosen controls should be aligned with enterprise culture, technology, budget and strategy. They should also provide accurate, timely information and be effective and measureable.



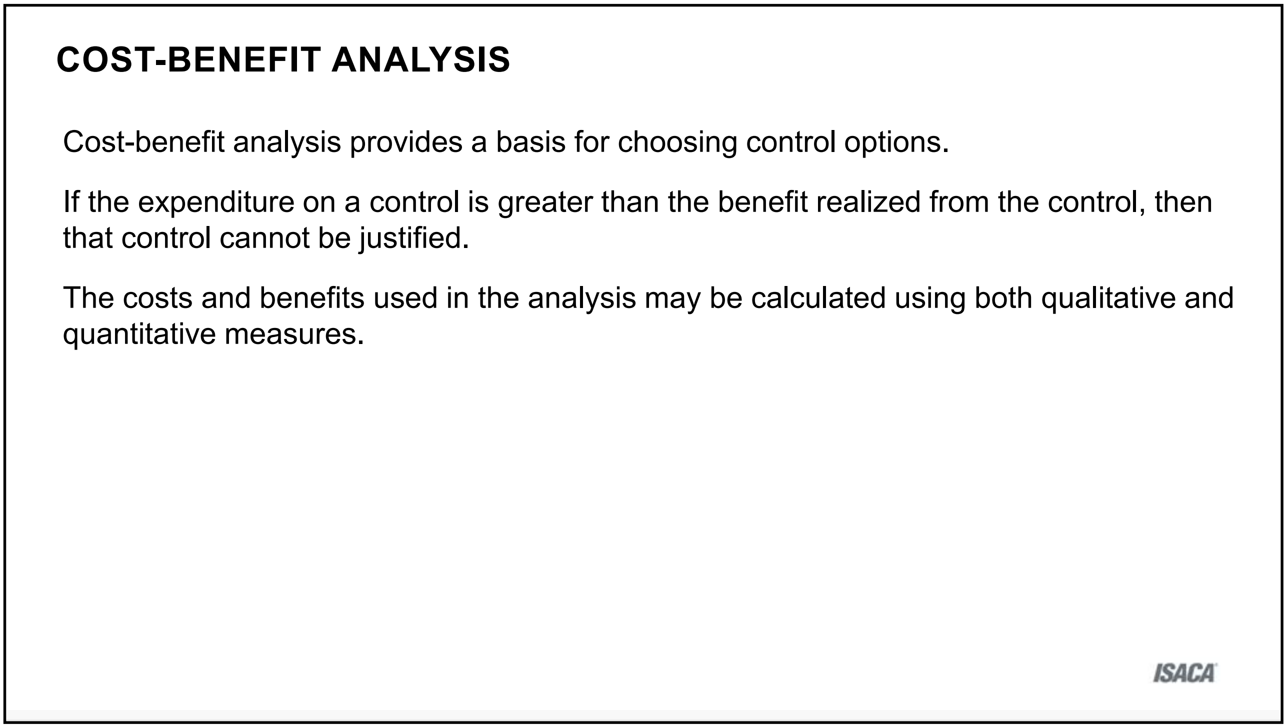
CHOOSING CONTROLS (CONT'D)

The risk action plan is a consideration of the chosen controls and their implementation.

Through experience and careful evaluation, the risk practitioner can advise the risk owner on the following risk action plan areas:

- The feasibility of project dates
- The expected workload associated with the project
- The costs of the project
- The overall success of the project according to risk management and business goals

Note, too, that using project management good practices aids in the successful outcome of the risk action plan.

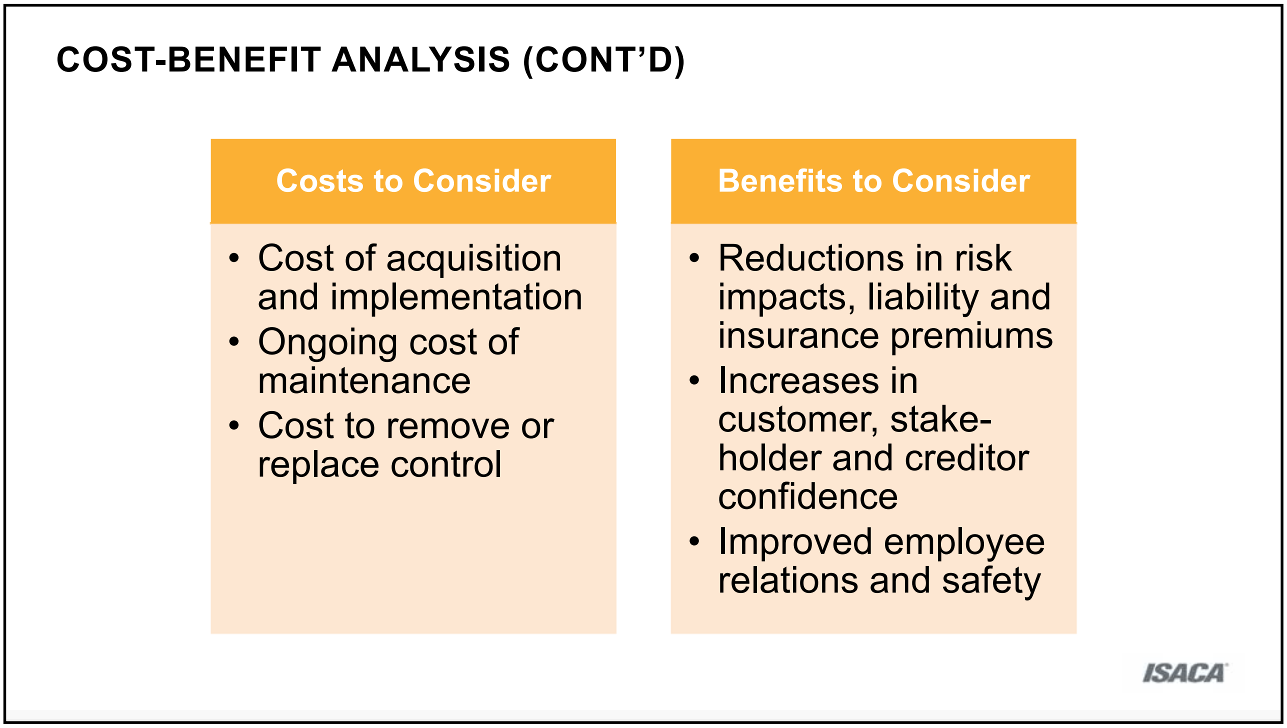


COST-BENEFIT ANALYSIS

Cost-benefit analysis provides a basis for choosing control options.

If the expenditure on a control is greater than the benefit realized from the control, then that control cannot be justified.

The costs and benefits used in the analysis may be calculated using both qualitative and quantitative measures.



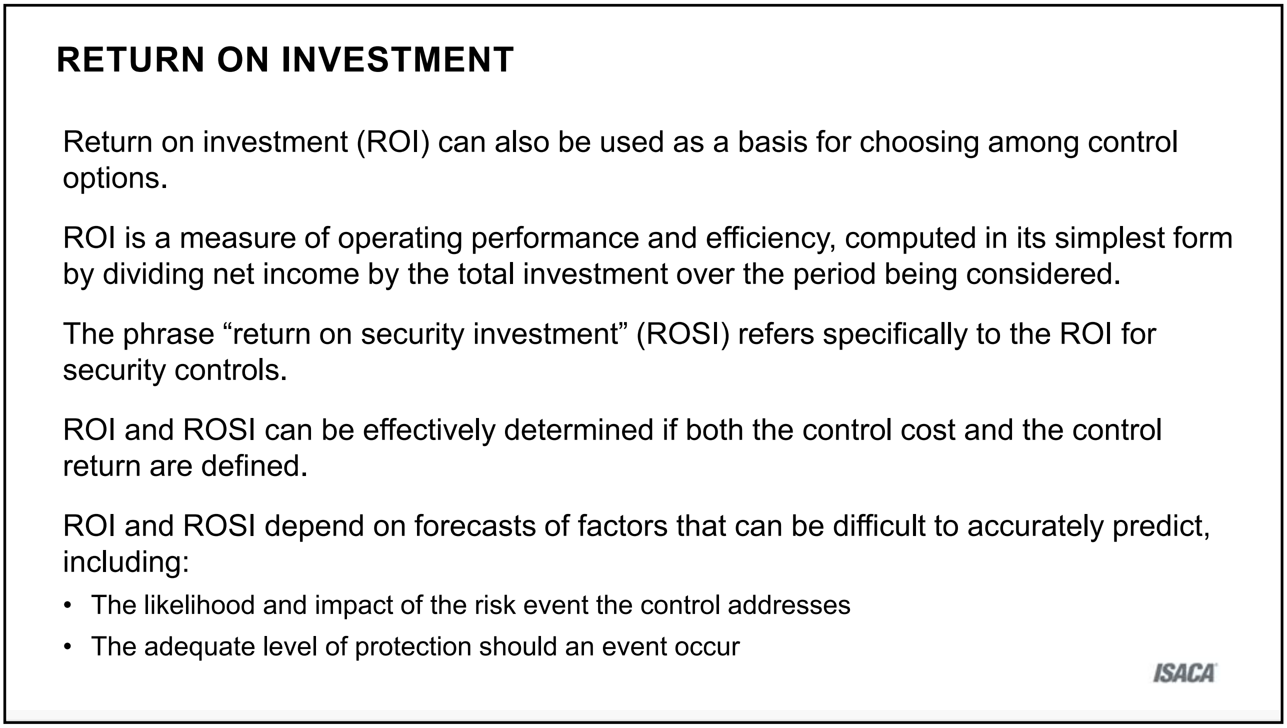
COST-BENEFIT ANALYSIS (CONT’D)

Costs to Consider

- Cost of acquisition and implementation
- Ongoing cost of maintenance
- Cost to remove or replace control

Benefits to Consider

- Reductions in risk impacts, liability and insurance premiums
- Increases in customer, stake-holder and creditor confidence
- Improved employee relations and safety



RETURN ON INVESTMENT

Return on investment (ROI) can also be used as a basis for choosing among control options.

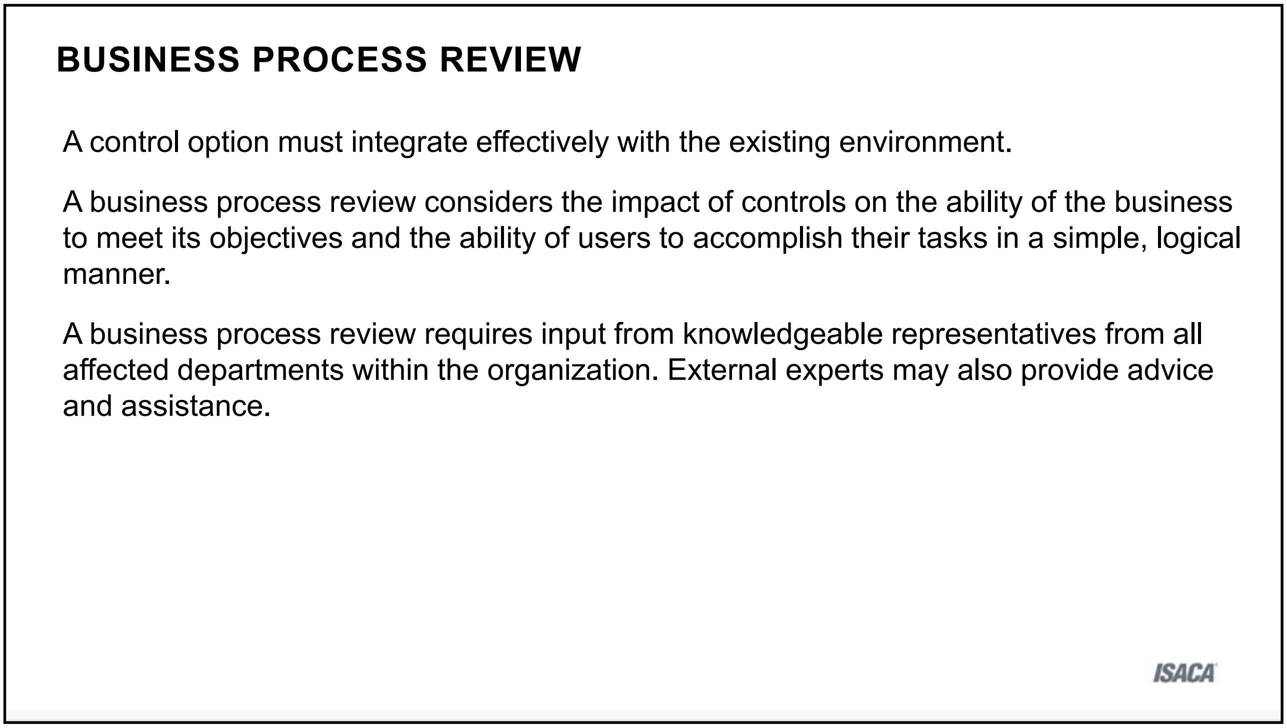
ROI is a measure of operating performance and efficiency, computed in its simplest form by dividing net income by the total investment over the period being considered.

The phrase “return on security investment” (ROSI) refers specifically to the ROI for security controls.

ROI and ROSI can be effectively determined if both the control cost and the control return are defined.

ROI and ROSI depend on forecasts of factors that can be difficult to accurately predict, including:

- The likelihood and impact of the risk event the control addresses
- The adequate level of protection should an event occur

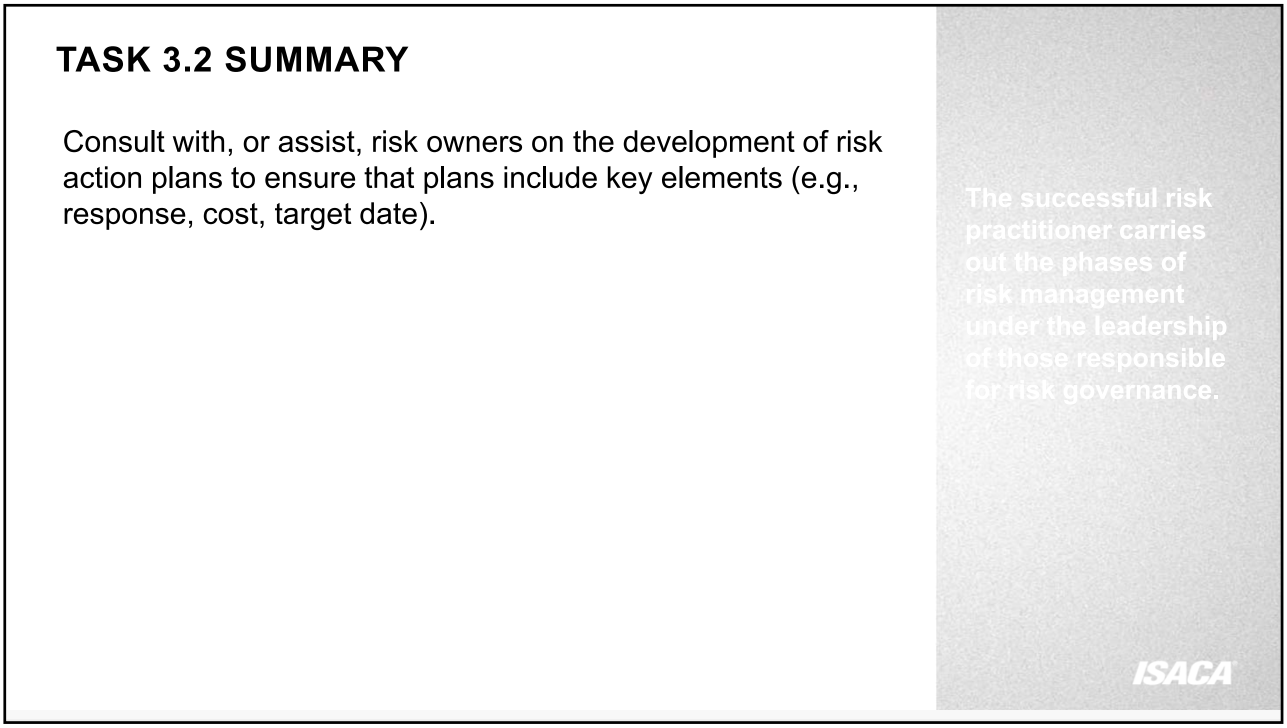


BUSINESS PROCESS REVIEW

A control option must integrate effectively with the existing environment.

A business process review considers the impact of controls on the ability of the business to meet its objectives and the ability of users to accomplish their tasks in a simple, logical manner.

A business process review requires input from knowledgeable representatives from all affected departments within the organization. External experts may also provide advice and assistance.



TASK 3.2 SUMMARY

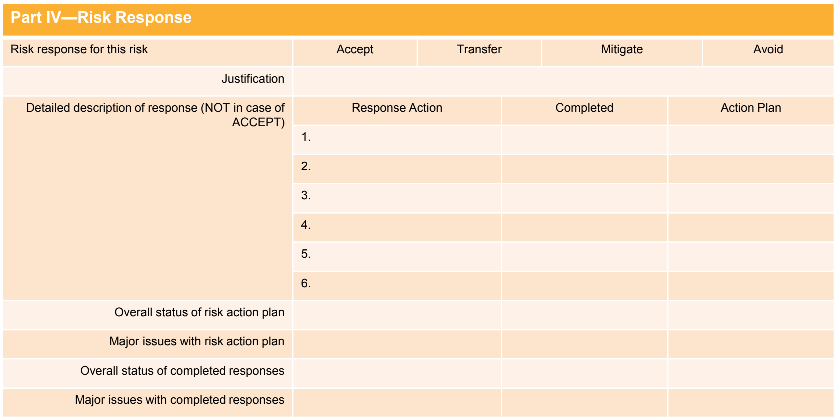
Consult with, or assist, risk owners on the development of risk action plans to ensure that plans include key elements (e.g., response, cost, target date).

The successful risk practitioner carries out the phases of risk management under the leadership of those responsible for risk governance.

ISACA

TASK 3.2 ACTIVITY

Develop the risk action plan by completing Part IV of the risk register for your scenario.



Part IV—Risk Response				
Risk response for this risk	Accept	Transfer	Mitigate	Avoid
Justification				
Detailed description of response (NOT in case of ACCEPT)	Response Action	Completed	Action Plan	
	1.			
	2.			
	3.			
	4.			
	5.			
	6.			
Overall status of risk action plan				
Major issues with risk action plan				
Overall status of completed responses				
Major issues with completed responses				

DISCUSSION QUESTION

It is MOST important for risk mitigation to:

A. eliminate threats and vulnerabilities.

B. reduce the likelihood of risk occurrence.

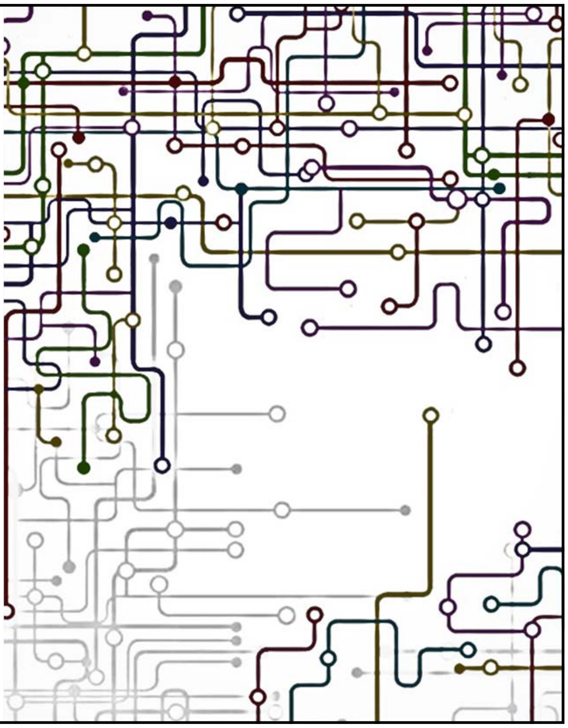
C. reduce risk within acceptable cost.

D. reduce inherent risk to zero.

DISCUSSION QUESTION

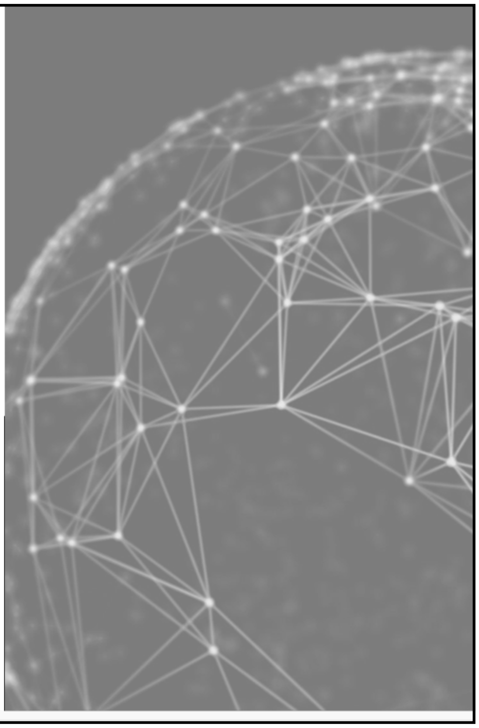
Which type of cost incurred is used when leveraging existing network cabling for an IT project?

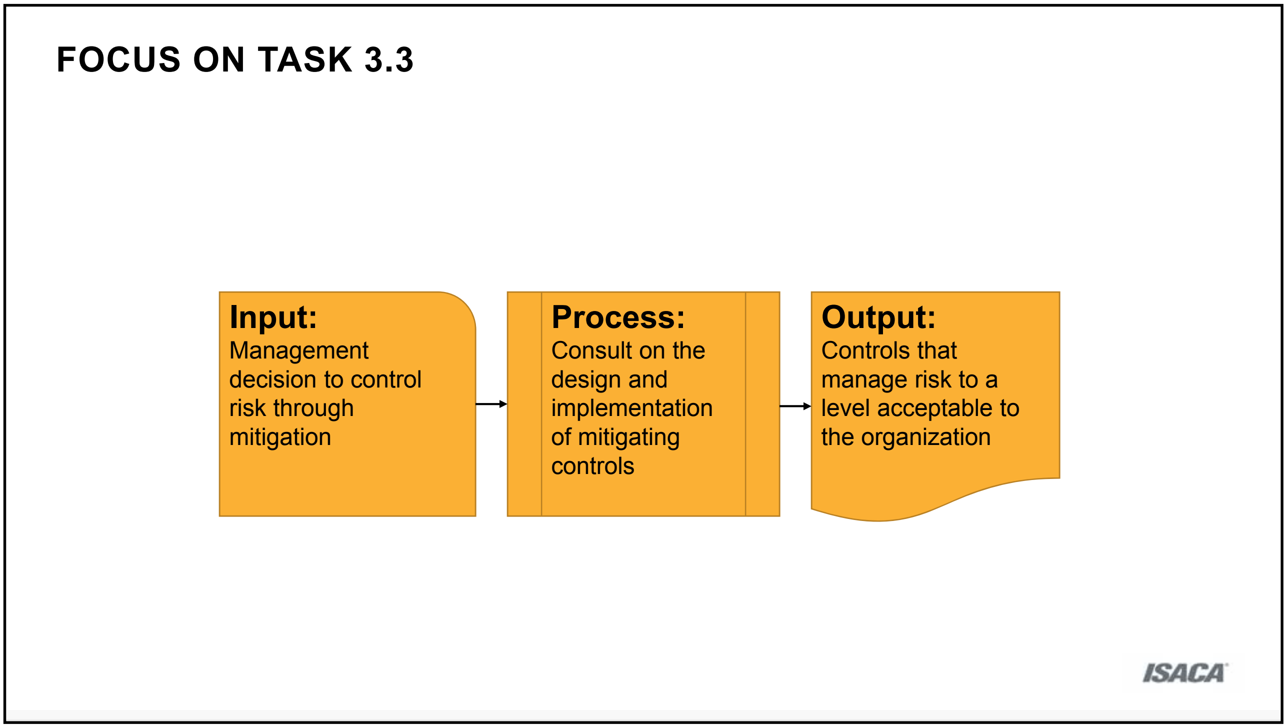
A. Indirect cost
B. Infrastructure cost
C. Project cost
D. Maintenance cost



TASK 3.3

Consult on the design and implementation or adjustment of mitigating controls to ensure that the risk is managed to an acceptable level.



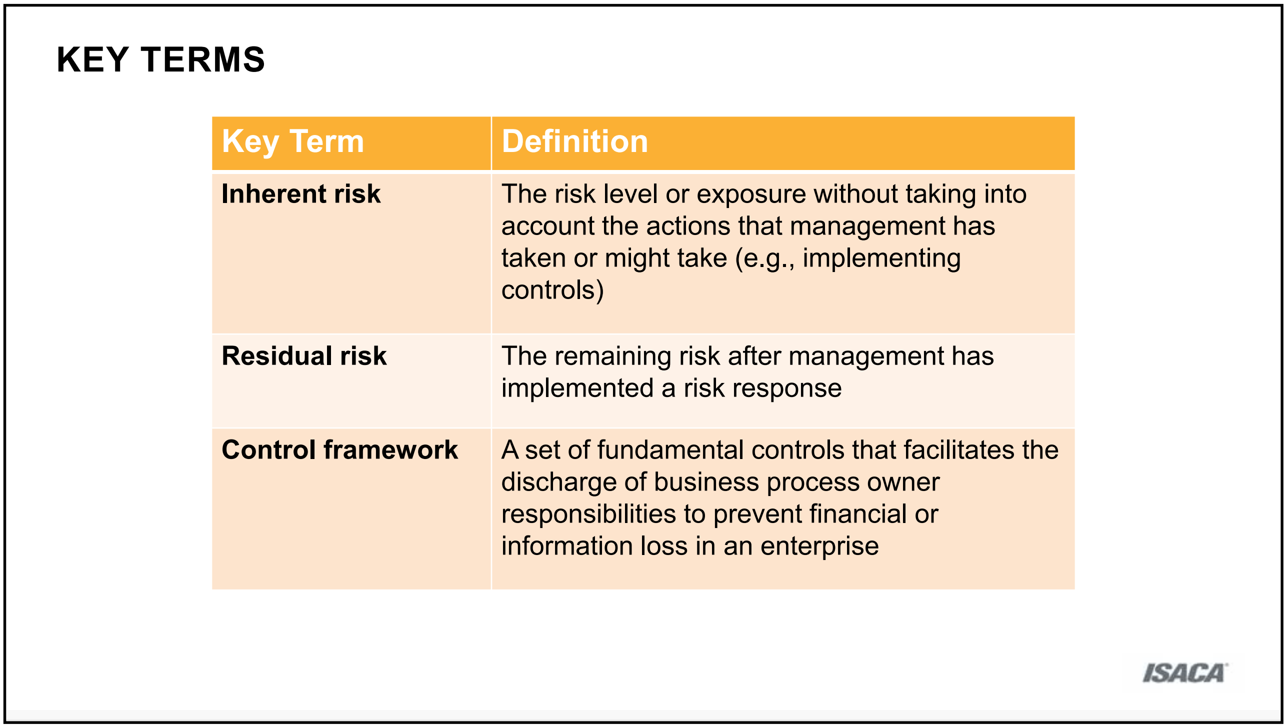


FOCUS ON TASK 3.3

Input:
Management decision to control risk through mitigation

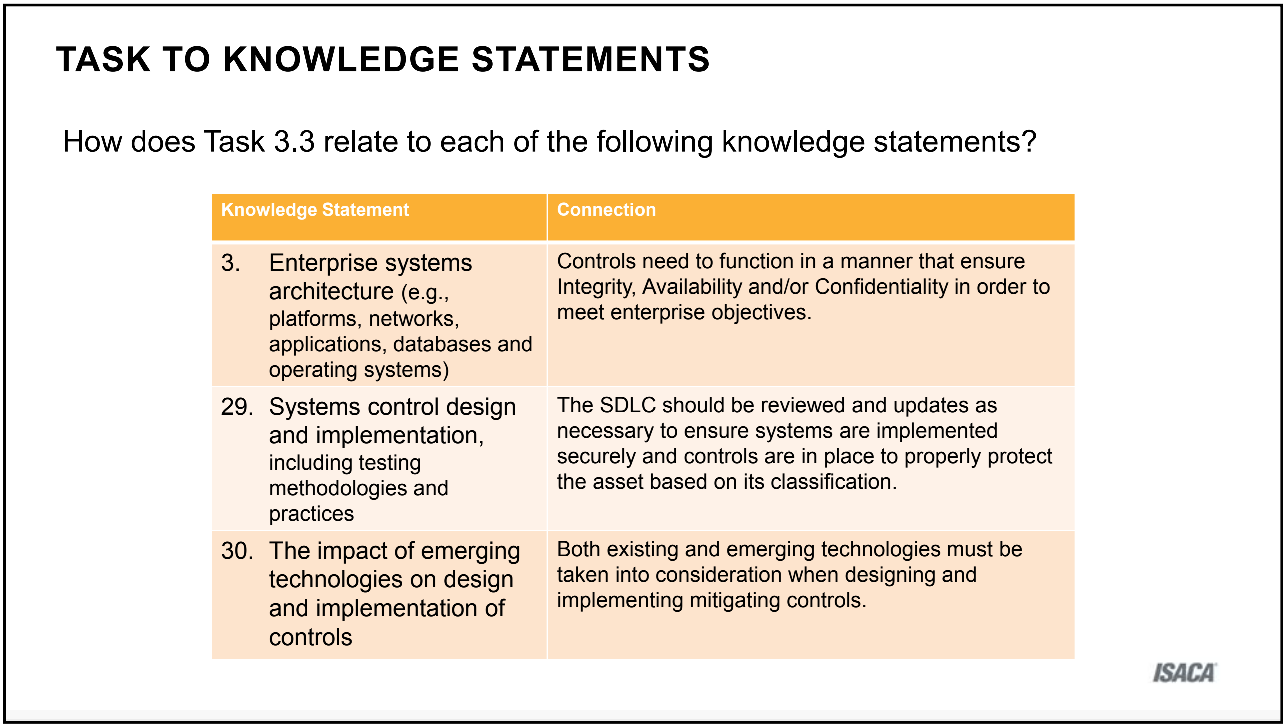
Process:
Consult on the design and implementation of mitigating controls

Output:
Controls that manage risk to a level acceptable to the organization



KEY TERMS

Key Term	Definition
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
Control framework	A set of fundamental controls that facilitates the discharge of business process owner responsibilities to prevent financial or information loss in an enterprise

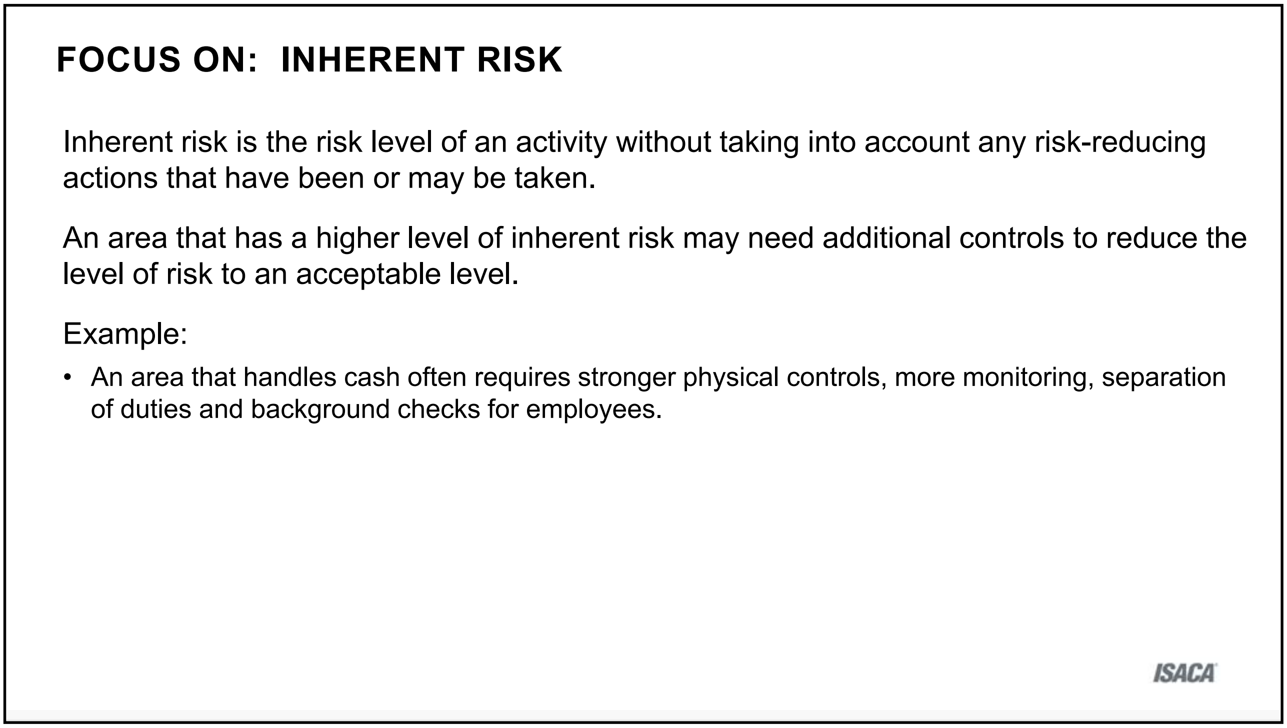


TASK TO KNOWLEDGE STATEMENTS

How does Task 3.3 relate to each of the following knowledge statements?

Knowledge Statement	Connection
3. Enterprise systems architecture (e.g., platforms, networks, applications, databases and operating systems)	Controls need to function in a manner that ensure Integrity, Availability and/or Confidentiality in order to meet enterprise objectives.
29. Systems control design and implementation, including testing methodologies and practices	The SDLC should be reviewed and updates as necessary to ensure systems are implemented securely and controls are in place to properly protect the asset based on its classification.
30. The impact of emerging technologies on design and implementation of controls	Both existing and emerging technologies must be taken into consideration when designing and implementing mitigating controls.

ISACA



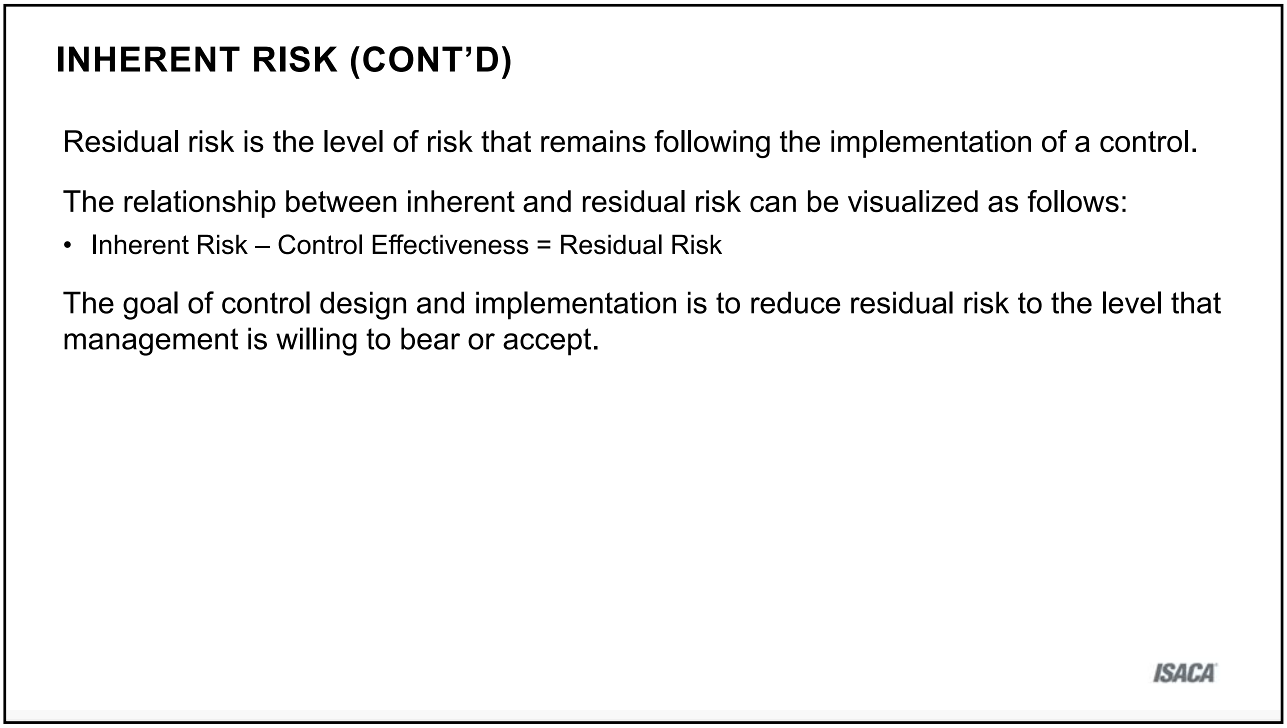
FOCUS ON: INHERENT RISK

Inherent risk is the risk level of an activity without taking into account any risk-reducing actions that have been or may be taken.

An area that has a higher level of inherent risk may need additional controls to reduce the level of risk to an acceptable level.

Example:

- An area that handles cash often requires stronger physical controls, more monitoring, separation of duties and background checks for employees.



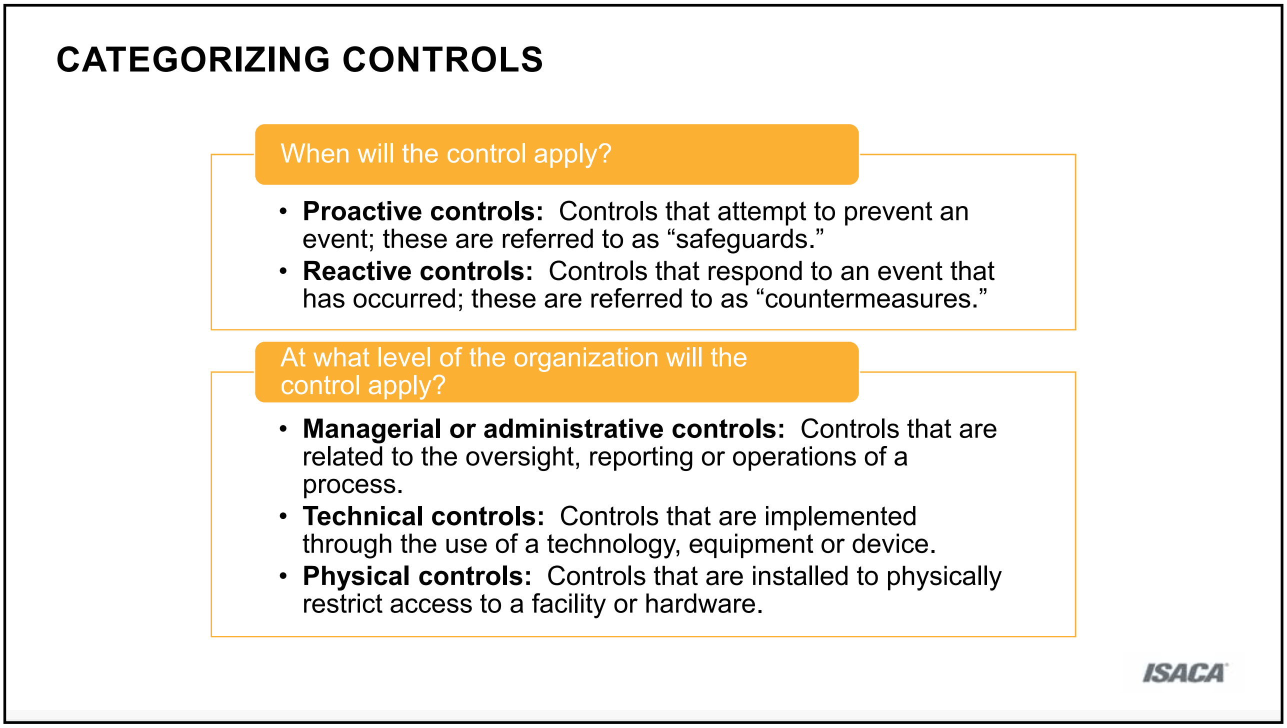
INHERENT RISK (CONT'D)

Residual risk is the level of risk that remains following the implementation of a control.

The relationship between inherent and residual risk can be visualized as follows:

- Inherent Risk – Control Effectiveness = Residual Risk

The goal of control design and implementation is to reduce residual risk to the level that management is willing to bear or accept.



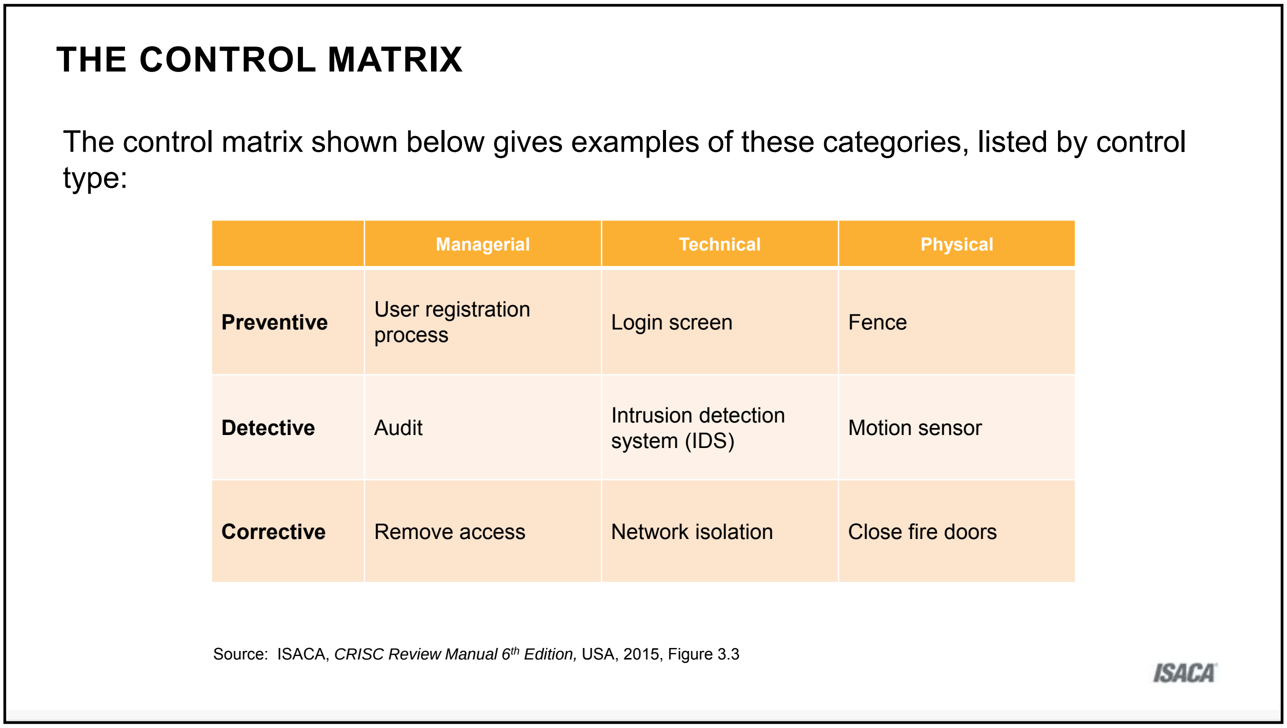
CATEGORIZING CONTROLS

When will the control apply?

- **Proactive controls:** Controls that attempt to prevent an event; these are referred to as "safeguards."
- **Reactive controls:** Controls that respond to an event that has occurred; these are referred to as "countermeasures."

At what level of the organization will the control apply?

- **Managerial or administrative controls:** Controls that are related to the oversight, reporting or operations of a process.
- **Technical controls:** Controls that are implemented through the use of a technology, equipment or device.
- **Physical controls:** Controls that are installed to physically restrict access to a facility or hardware.



THE CONTROL MATRIX

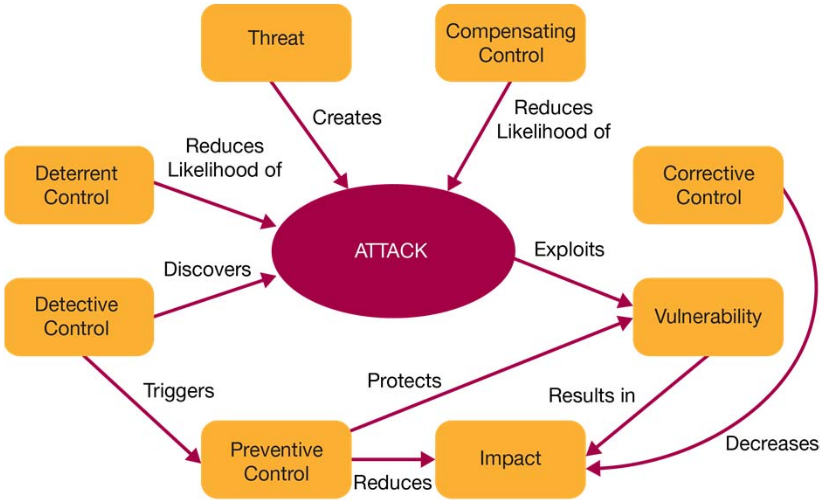
The control matrix shown below gives examples of these categories, listed by control type:

	Managerial	Technical	Physical
Preventive	User registration process	Login screen	Fence
Detective	Audit	Intrusion detection system (IDS)	Motion sensor
Corrective	Remove access	Network isolation	Close fire doors

Source: ISACA, *CRISC Review Manual 6th Edition,* USA, 2015, Figure 3.3

ISACA

CONTROL INTERDEPENDENCIES



Threat

Compensating Control

Creates

Reduces Likelihood of

Reduces Likelihood of

Deterrent Control

Corrective Control

ATTACK

Exploits

Discovers

Detective Control

Vulnerability

Triggers

Protects

Results in

Decreases

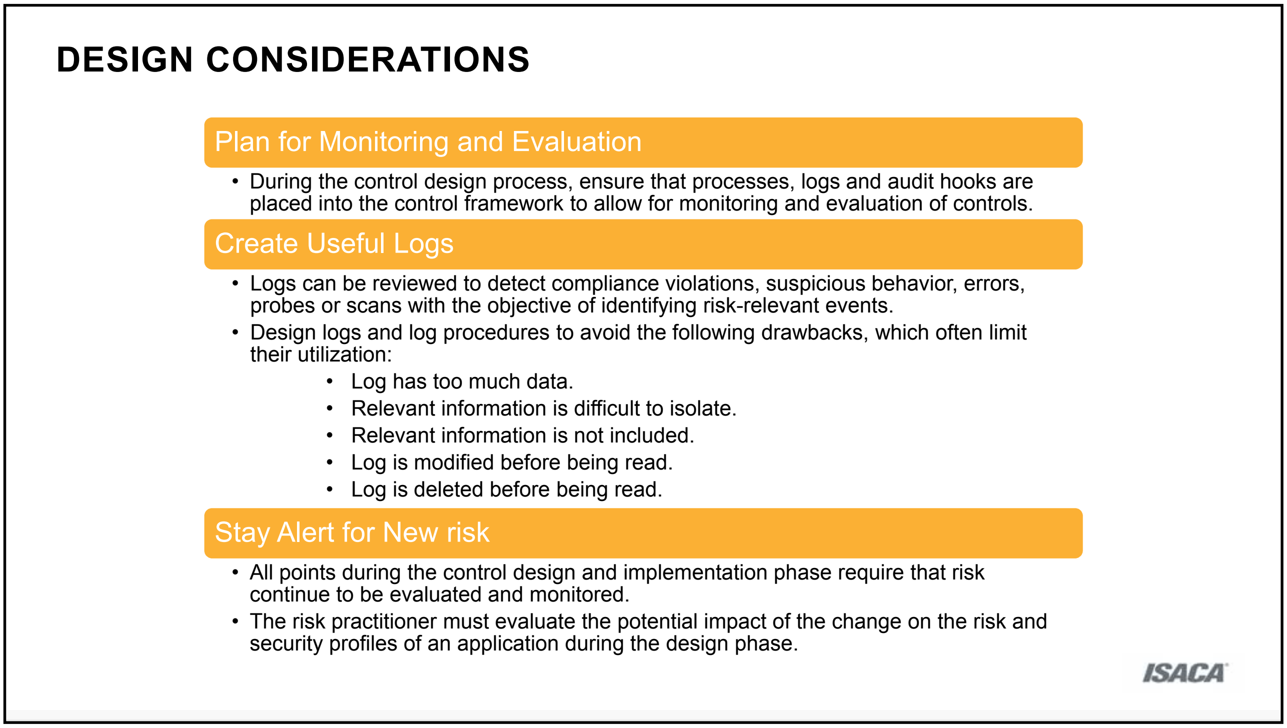
Preventive Control

Impact

Reduces

Source: ISACA, *CRISC Review Manual 6th Edition*, figure 3.4

ISACA



DESIGN CONSIDERATIONS

Plan for Monitoring and Evaluation

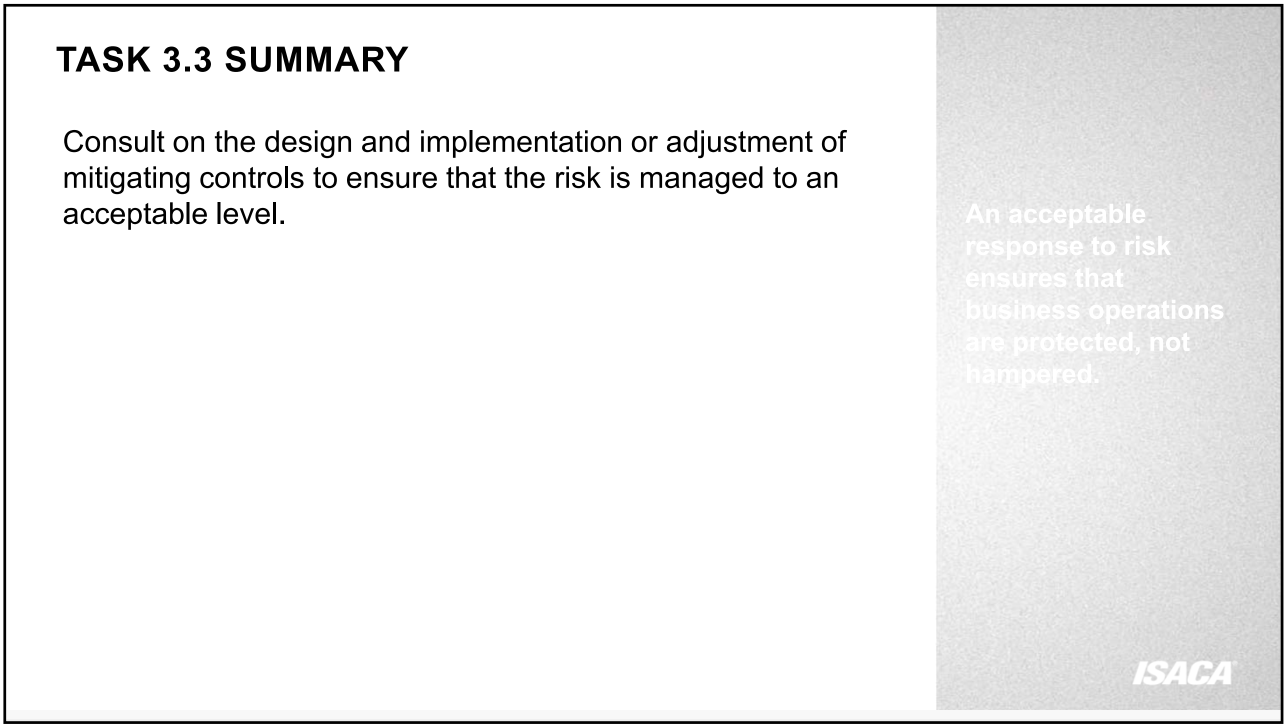
- During the control design process, ensure that processes, logs and audit hooks are placed into the control framework to allow for monitoring and evaluation of controls.

Create Useful Logs

- Logs can be reviewed to detect compliance violations, suspicious behavior, errors, probes or scans with the objective of identifying risk-relevant events.
- Design logs and log procedures to avoid the following drawbacks, which often limit their utilization:
    - Log has too much data.
    - Relevant information is difficult to isolate.
    - Relevant information is not included.
    - Log is modified before being read.
    - Log is deleted before being read.

Stay Alert for New risk

- All points during the control design and implementation phase require that risk continue to be evaluated and monitored.
- The risk practitioner must evaluate the potential impact of the change on the risk and security profiles of an application during the design phase.



TASK 3.3 SUMMARY

Consult on the design and implementation or adjustment of mitigating controls to ensure that the risk is managed to an acceptable level.

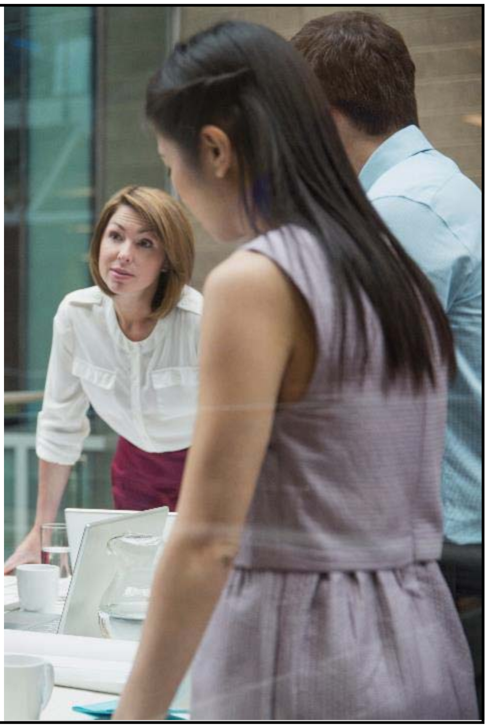
An acceptable response to risk ensures that business operations are protected, not hampered.

TASK 3.3 ACTIVITY

Name a typical control found in an IT environment.

How might the design of this control be altered for improved effectiveness?

What changes would improve its implementation?



DISCUSSION QUESTION

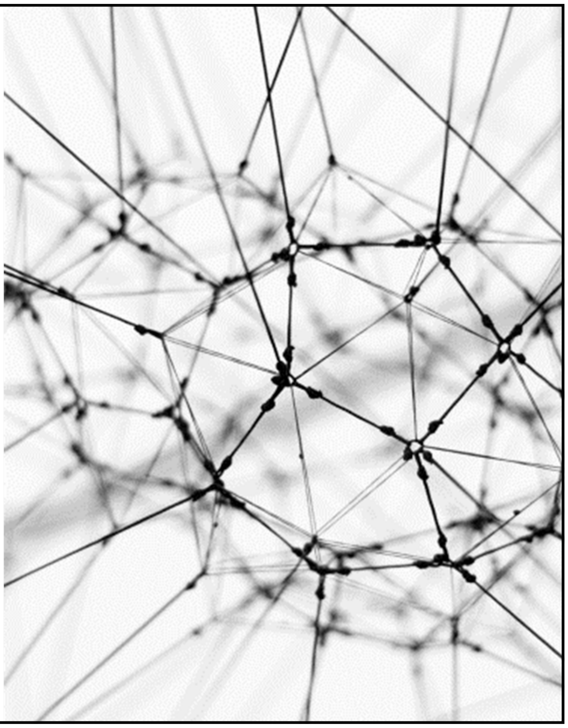
Which of the following is minimized when acceptable risk is achieved?

A. Transferred risk

B. Control risk

C. Residual risk

D. Inherent risk



DISCUSSION QUESTION

Which of the following should management use to allocate resources for risk response?

A. Audit report findings

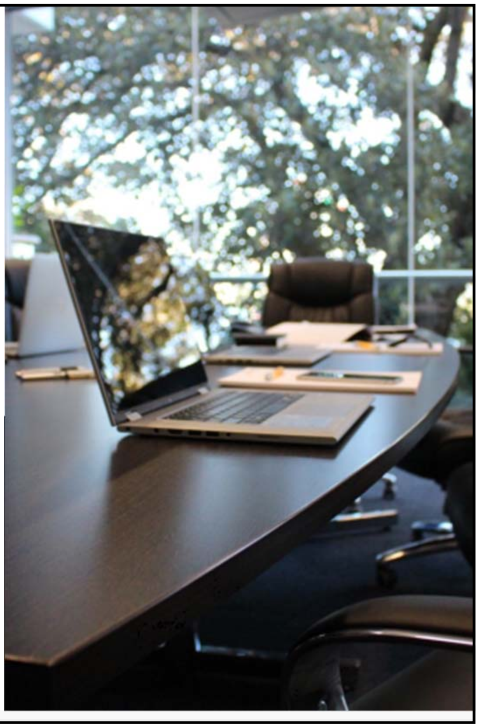
B. Penetration test results

C. Risk analysis results

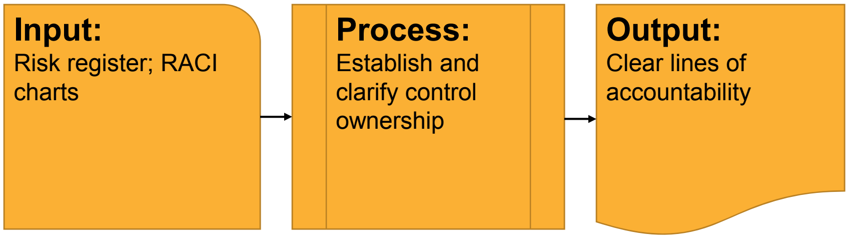
D. Vulnerability test results

TASK 3.4

Ensure that control ownership is assigned in order to establish clear lines of accountability.



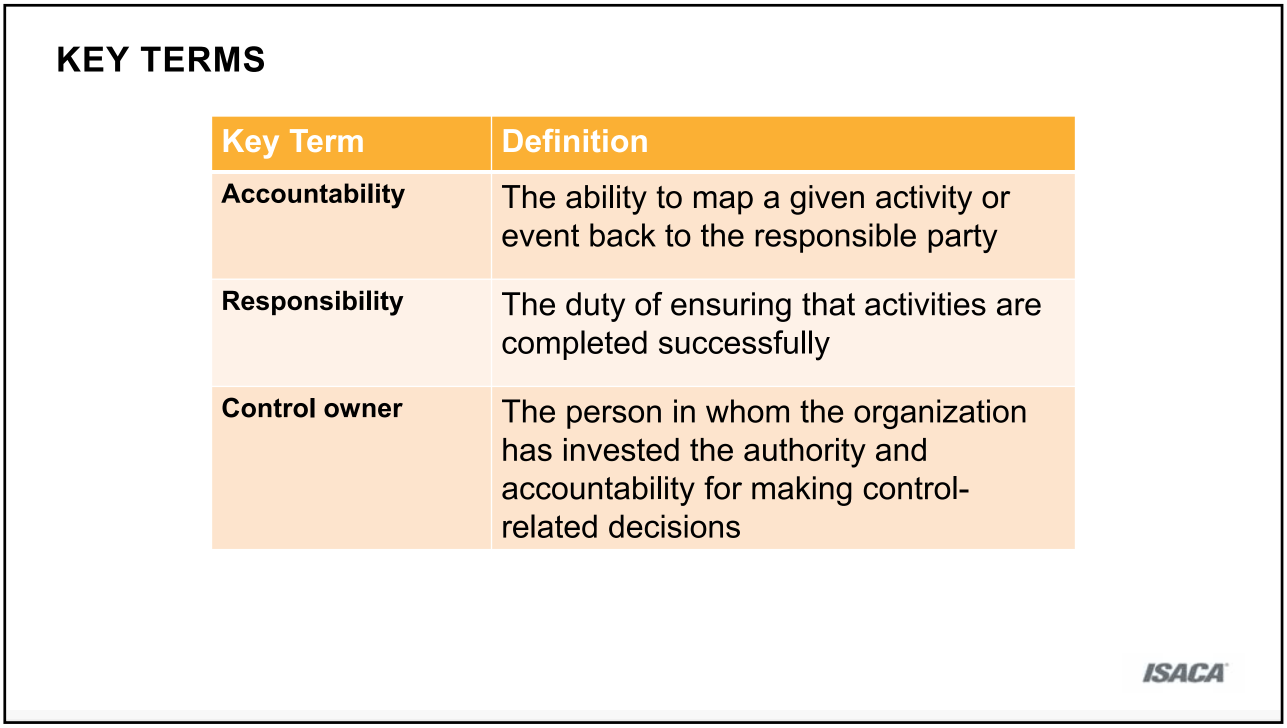
FOCUS ON TASK 3.4



Input:
Risk register; RACI charts

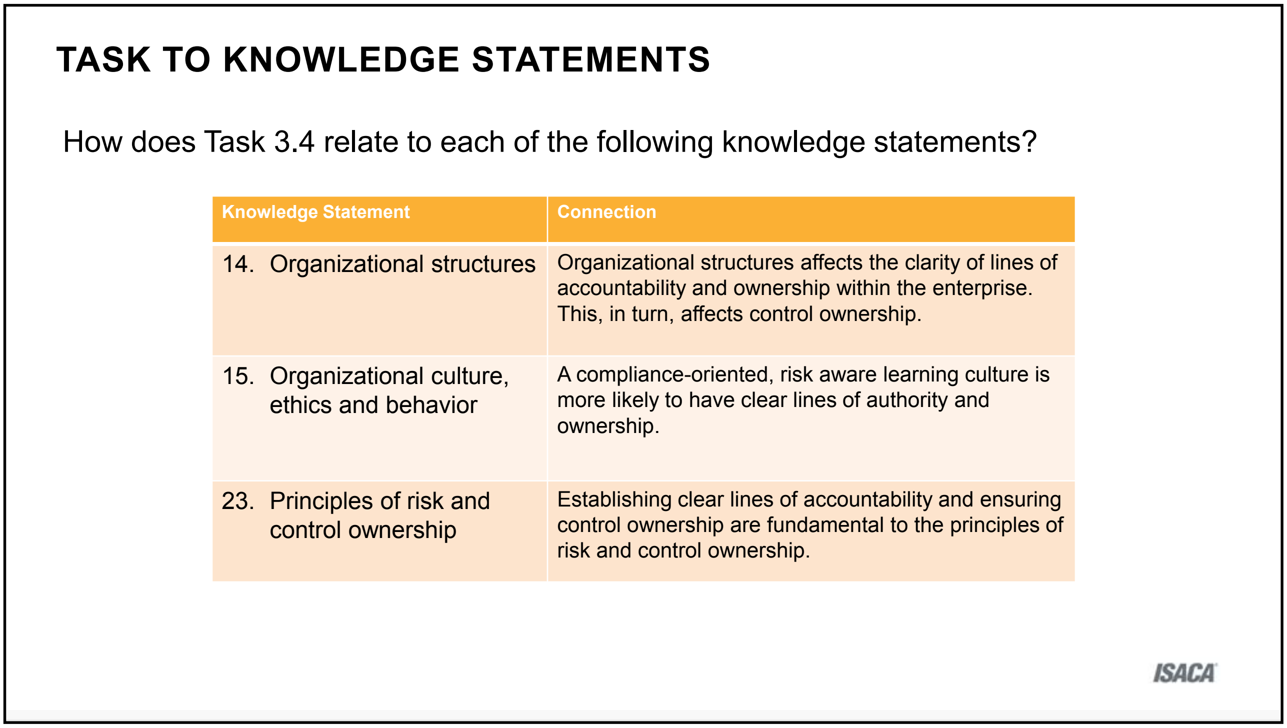
Process:
Establish and clarify control ownership

Output:
Clear lines of accountability



KEY TERMS

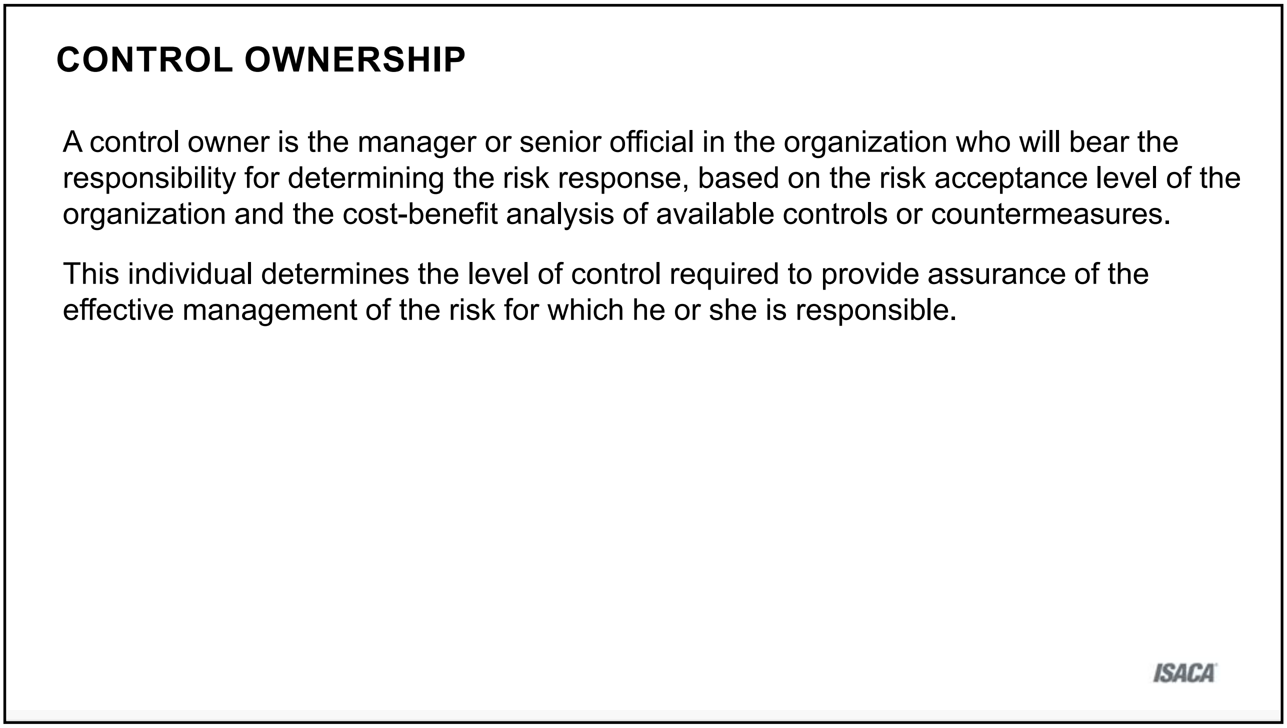
Key Term	Definition
Accountability	The ability to map a given activity or event back to the responsible party
Responsibility	The duty of ensuring that activities are completed successfully
Control owner	The person in whom the organization has invested the authority and accountability for making control-related decisions



TASK TO KNOWLEDGE STATEMENTS

How does Task 3.4 relate to each of the following knowledge statements?

Knowledge Statement	Connection
14. Organizational structures	Organizational structures affects the clarity of lines of accountability and ownership within the enterprise. This, in turn, affects control ownership.
15. Organizational culture, ethics and behavior	A compliance-oriented, risk aware learning culture is more likely to have clear lines of authority and ownership.
23. Principles of risk and control ownership	Establishing clear lines of accountability and ensuring control ownership are fundamental to the principles of risk and control ownership.



CONTROL OWNERSHIP

A control owner is the manager or senior official in the organization who will bear the responsibility for determining the risk response, based on the risk acceptance level of the organization and the cost-benefit analysis of available controls or countermeasures.

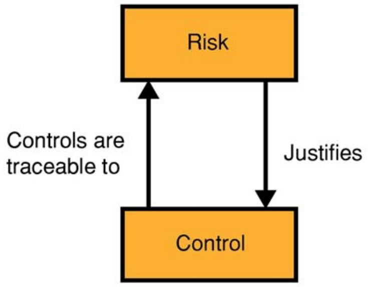
This individual determines the level of control required to provide assurance of the effective management of the risk for which he or she is responsible.

CONTROL OWNERSHIP (CONT’D)

The concept of a direct link between risk and control is important.

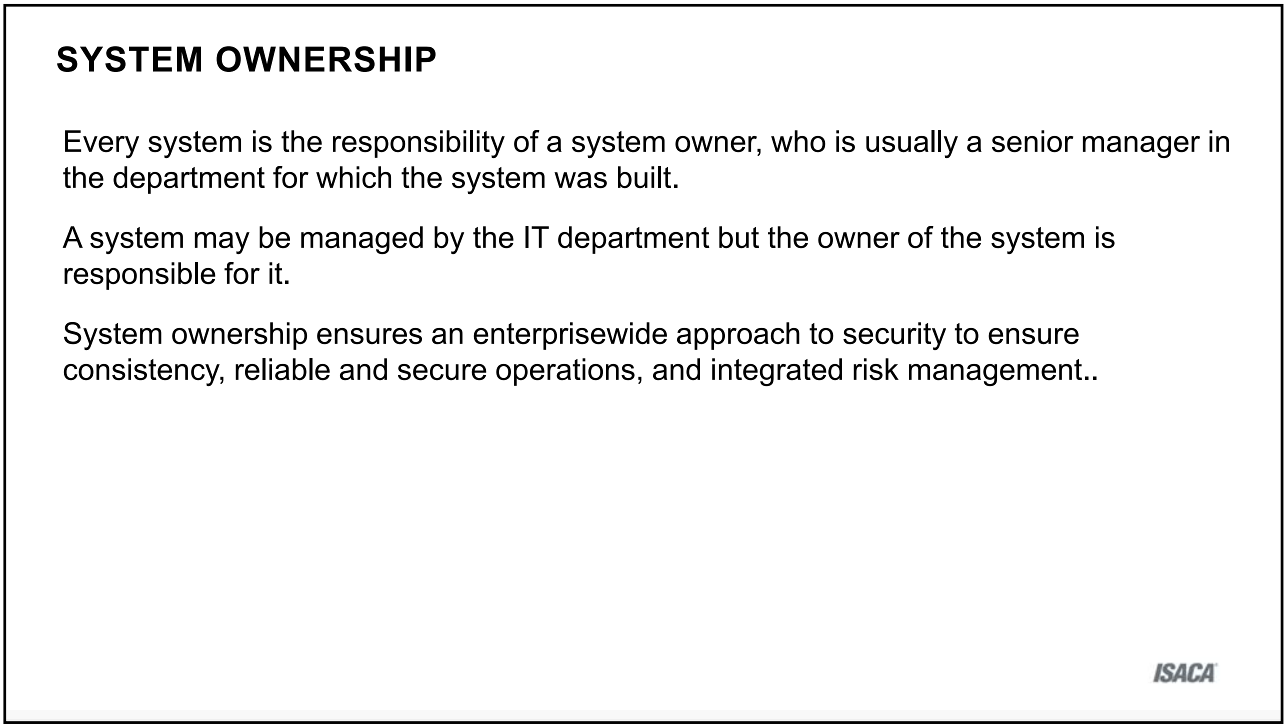
This concept ensures that each of the following is true:

- All risk has been addressed through appropriate controls.
- All controls are justified by the risk that mandates the requirement for that control.



Source: ISACA, *CRISC Review Manual 6th Edition*, figure 1.30

ISACA

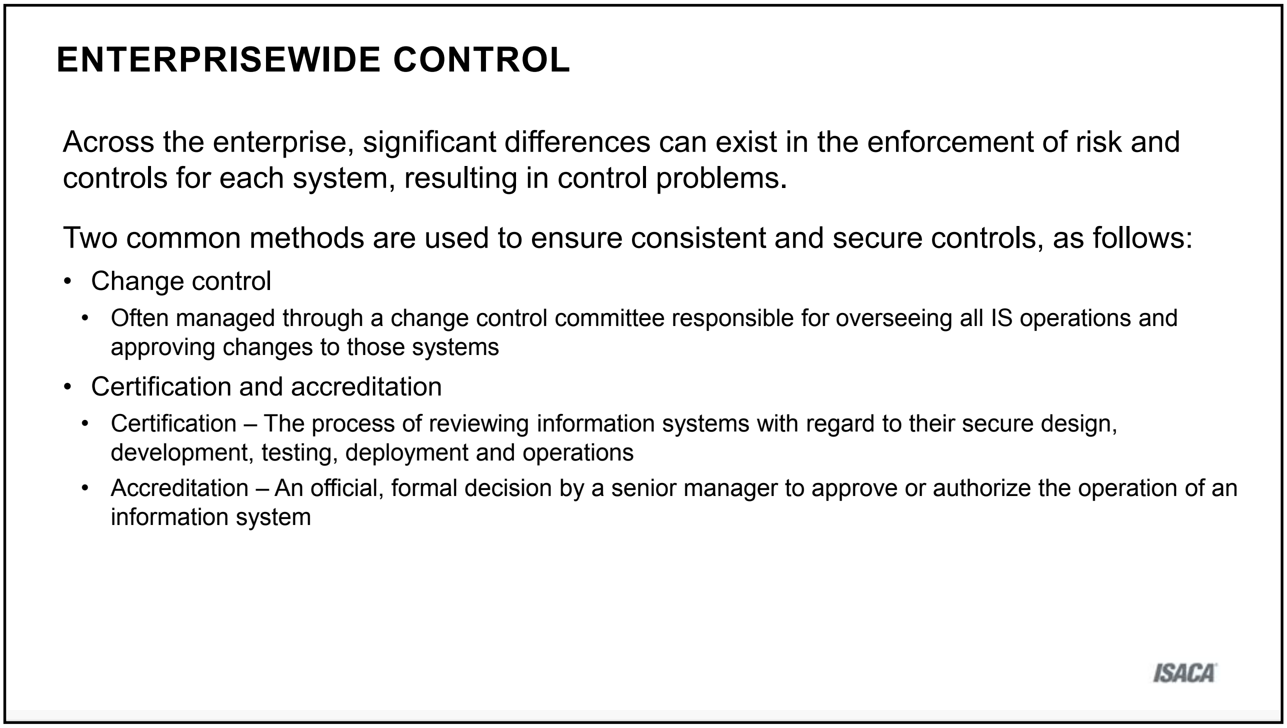


SYSTEM OWNERSHIP

Every system is the responsibility of a system owner, who is usually a senior manager in the department for which the system was built.

A system may be managed by the IT department but the owner of the system is responsible for it.

System ownership ensures an enterprisewide approach to security to ensure consistency, reliable and secure operations, and integrated risk management..

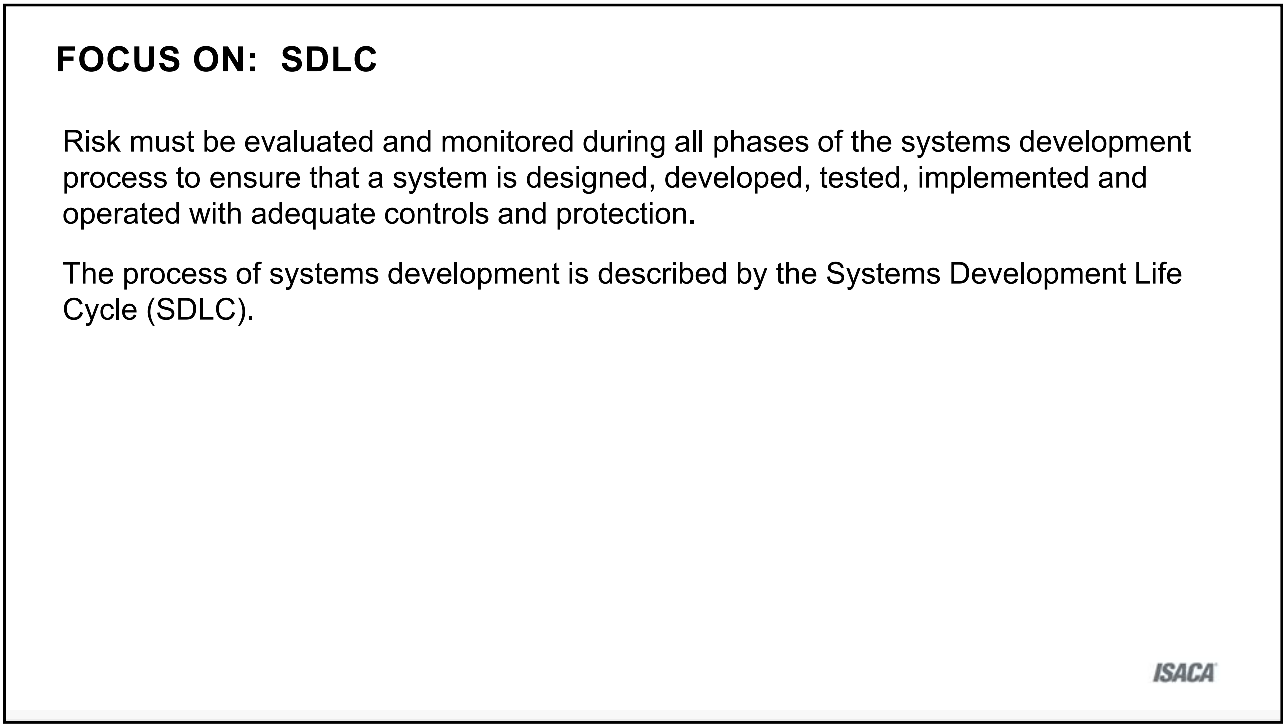


ENTERPRISEWIDE CONTROL

Across the enterprise, significant differences can exist in the enforcement of risk and controls for each system, resulting in control problems.

Two common methods are used to ensure consistent and secure controls, as follows:

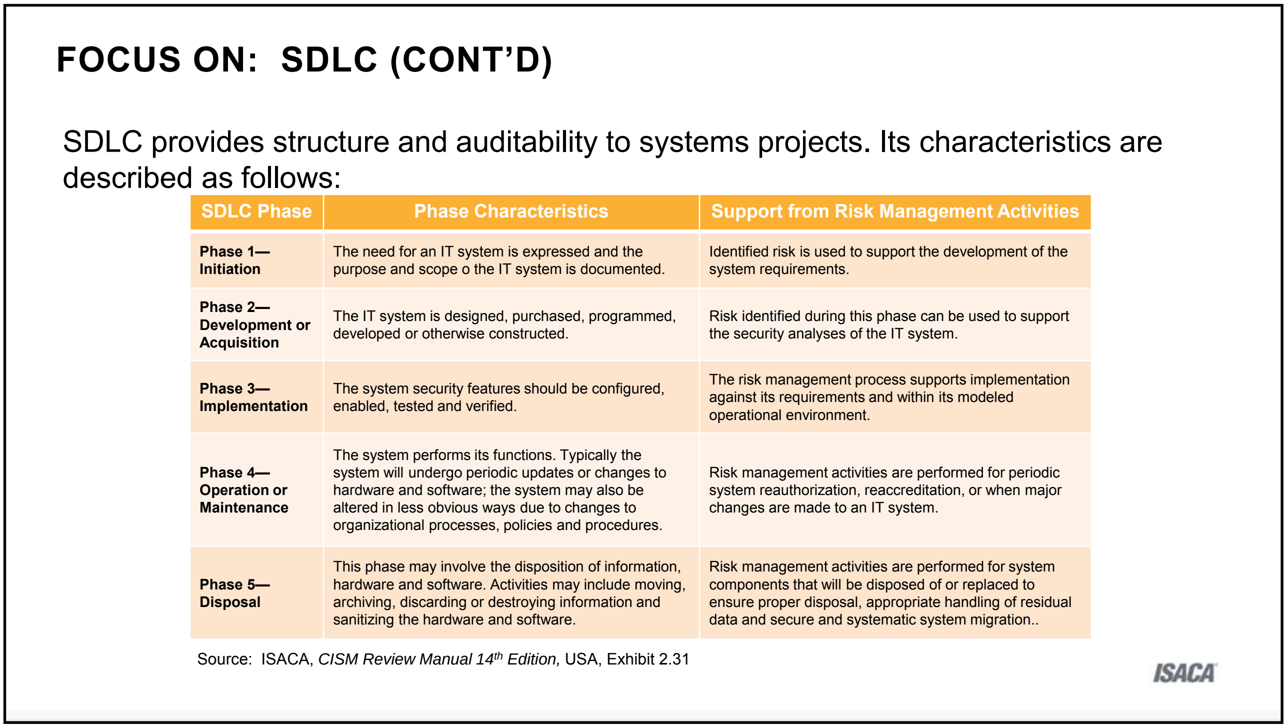
- Change control
  - Often managed through a change control committee responsible for overseeing all IS operations and approving changes to those systems
- Certification and accreditation
  - Certification – The process of reviewing information systems with regard to their secure design, development, testing, deployment and operations
  - Accreditation – An official, formal decision by a senior manager to approve or authorize the operation of an information system



FOCUS ON: SDLC

Risk must be evaluated and monitored during all phases of the systems development process to ensure that a system is designed, developed, tested, implemented and operated with adequate controls and protection.

The process of systems development is described by the Systems Development Life Cycle (SDLC).

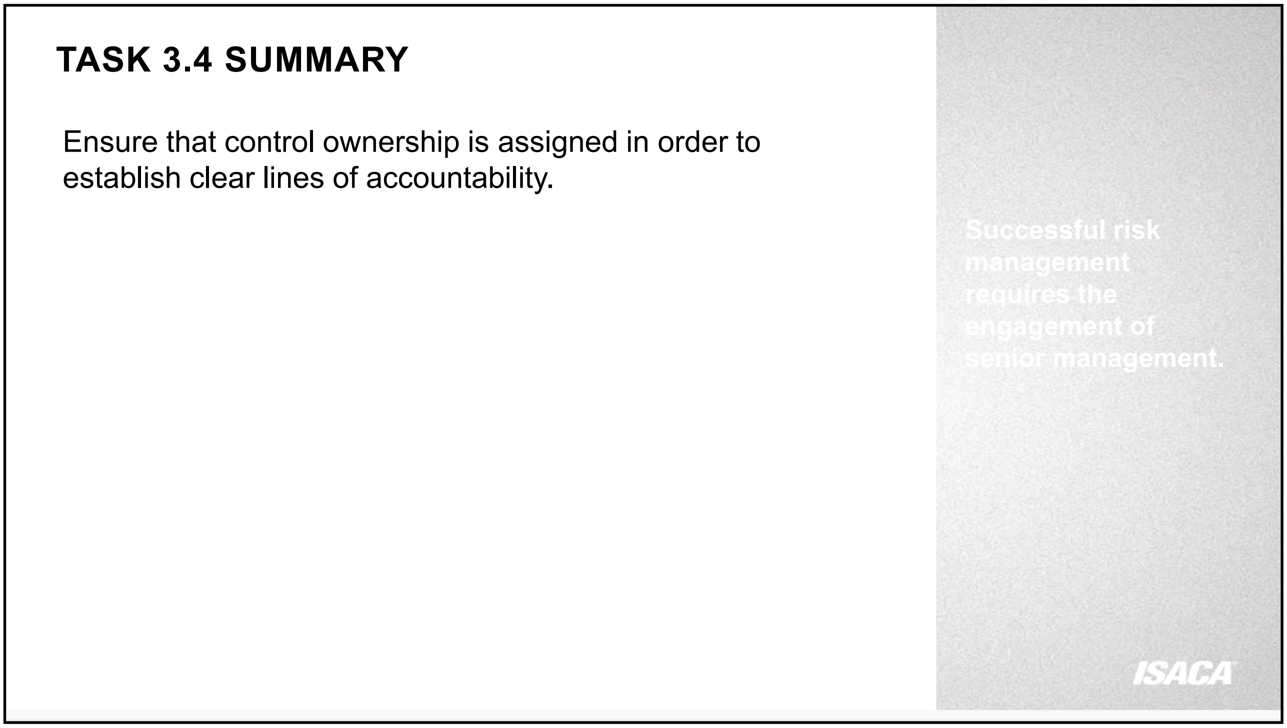


FOCUS ON: SDLC (CONT'D)

SDLC provides structure and auditability to systems projects. Its characteristics are described as follows:

SDLC Phase	Phase Characteristics	Support from Risk Management Activities
Phase 1—Initiation	The need for an IT system is expressed and the purpose and scope o the IT system is documented.	Identified risk is used to support the development of the system requirements.
Phase 2—Development or Acquisition	The IT system is designed, purchased, programmed, developed or otherwise constructed.	Risk identified during this phase can be used to support the security analyses of the IT system.
Phase 3—Implementation	The system security features should be configured, enabled, tested and verified.	The risk management process supports implementation against its requirements and within its modeled operational environment.
Phase 4—Operation or Maintenance	The system performs its functions. Typically the system will undergo periodic updates or changes to hardware and software; the system may also be altered in less obvious ways due to changes to organizational processes, policies and procedures.	Risk management activities are performed for periodic system reauthorization, reaccreditation, or when major changes are made to an IT system.
Phase 5—Disposal	This phase may involve the disposition of information, hardware and software. Activities may include moving, archiving, discarding or destroying information and sanitizing the hardware and software.	Risk management activities are performed for system components that will be disposed of or replaced to ensure proper disposal, appropriate handling of residual data and secure and systematic system migration..

Source: ISACA, *CISM Review Manual 14th Edition,* USA, Exhibit 2.31



TASK 3.4 SUMMARY

Ensure that control ownership is assigned in order to establish clear lines of accountability.

Successful risk management requires the engagement of senior management.

ISACA

TASK 3.4 DISCUSSION

Describe a scenario in which several different individuals could be named the owner of a risk and its control.

On what basis should the selection of the risk/control owner be made?

Which of the individuals in your scenario would you choose as risk/control owner? Why?

DISCUSSION QUESTION

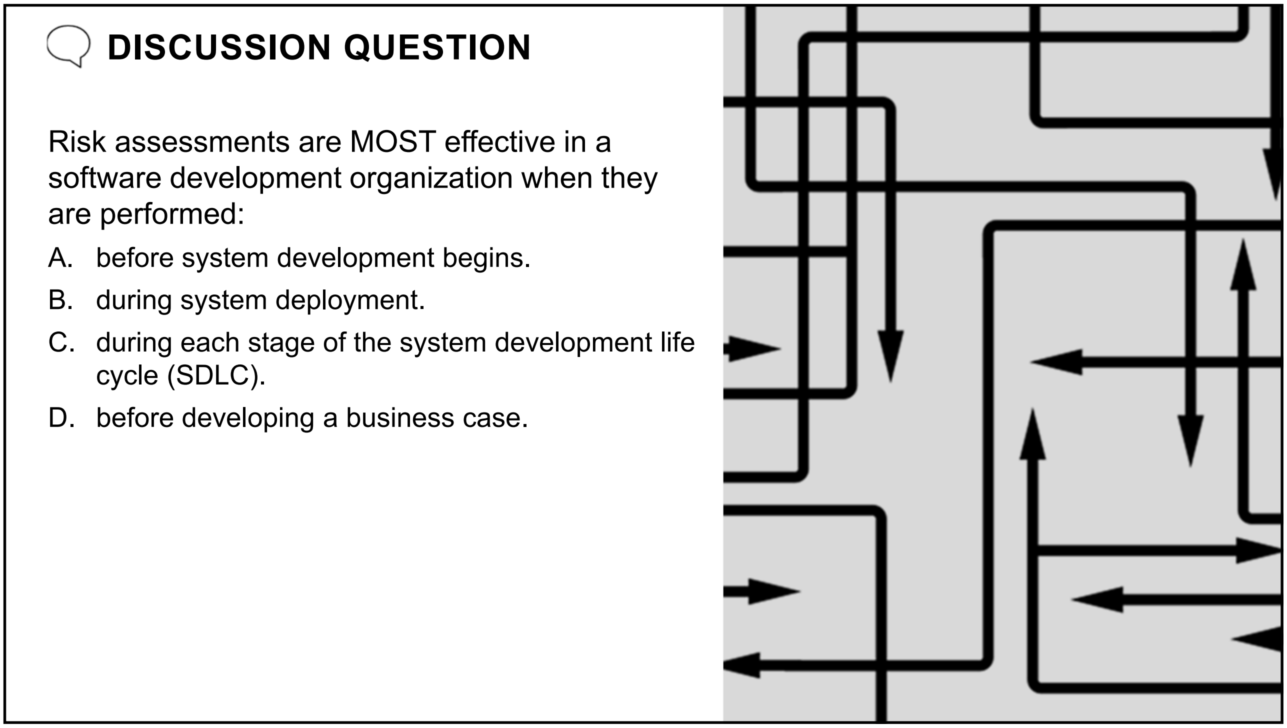
Who grants formal authorization for user access to a protected file?

A. The process owner

B. The system administrator

C. The data owner

D. The security manager



DISCUSSION QUESTION

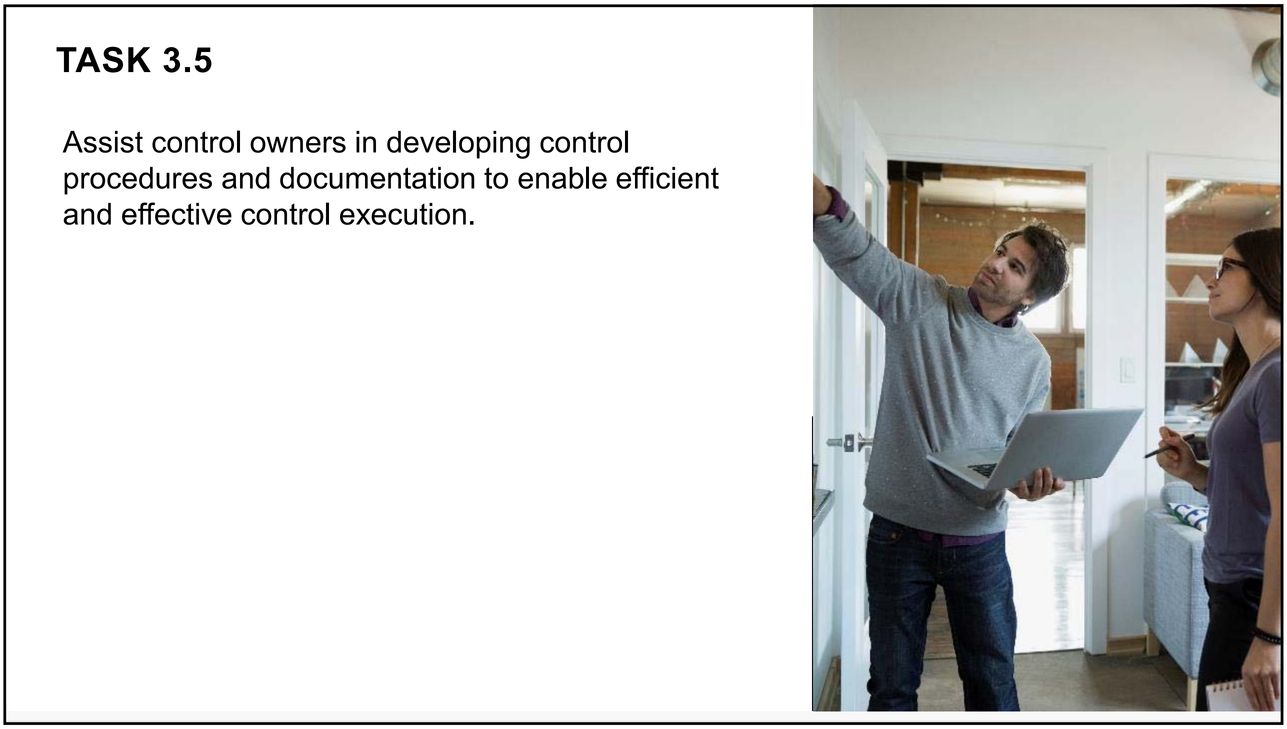
Risk assessments are MOST effective in a software development organization when they are performed:

A. before system development begins.

B. during system deployment.

C. during each stage of the system development life cycle (SDLC).

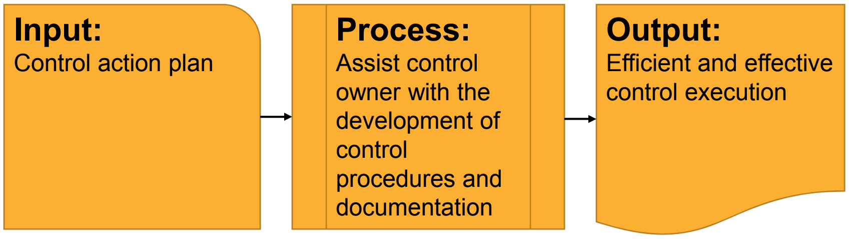
D. before developing a business case.



TASK 3.5

Assist control owners in developing control procedures and documentation to enable efficient and effective control execution.

FOCUS ON TASK 3.5

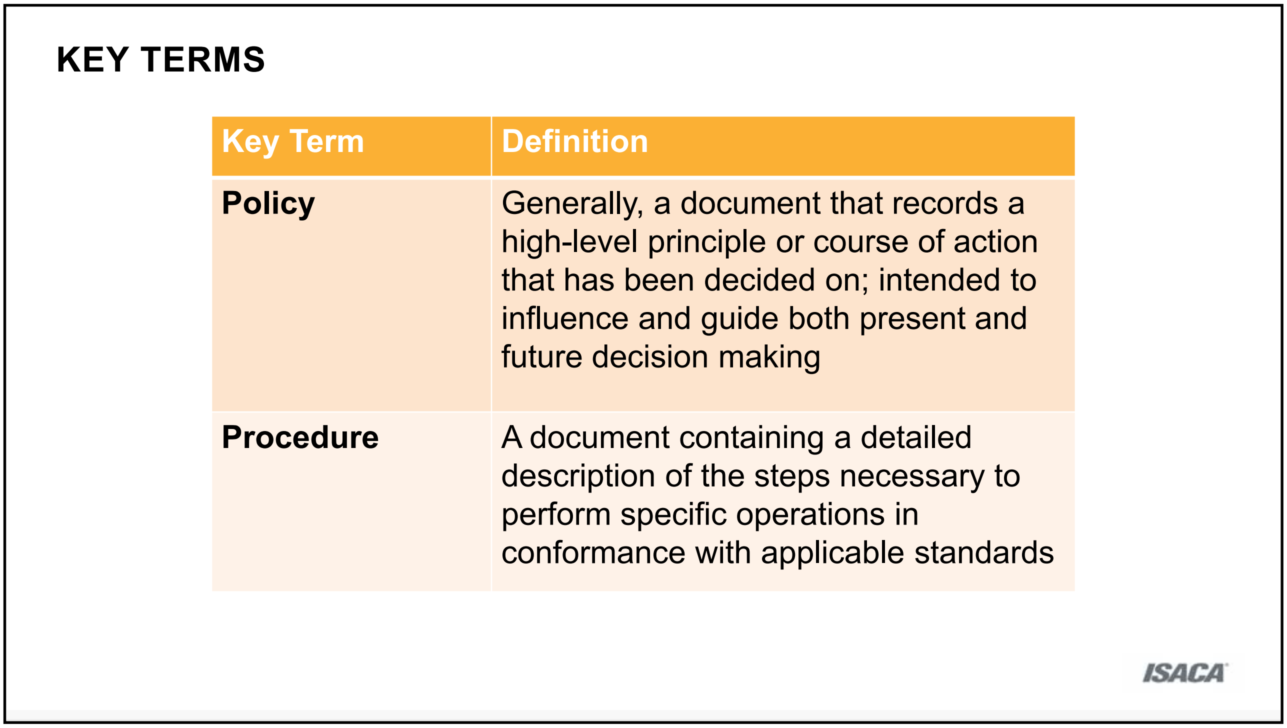


Input:
Control action plan

Process:
Assist control owner with the development of control procedures and documentation

Output:
Efficient and effective control execution

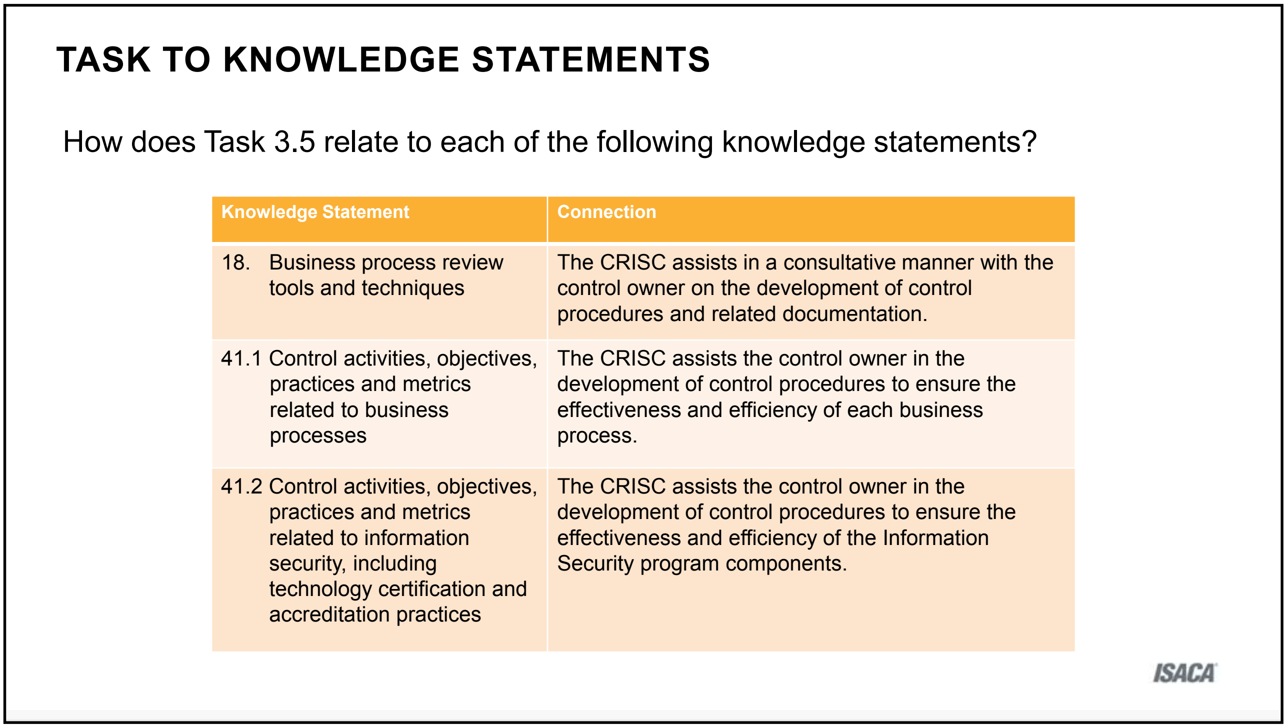
ISACA



KEY TERMS

Key Term	Definition
Policy	Generally, a document that records a high-level principle or course of action that has been decided on; intended to influence and guide both present and future decision making
Procedure	A document containing a detailed description of the steps necessary to perform specific operations in conformance with applicable standards

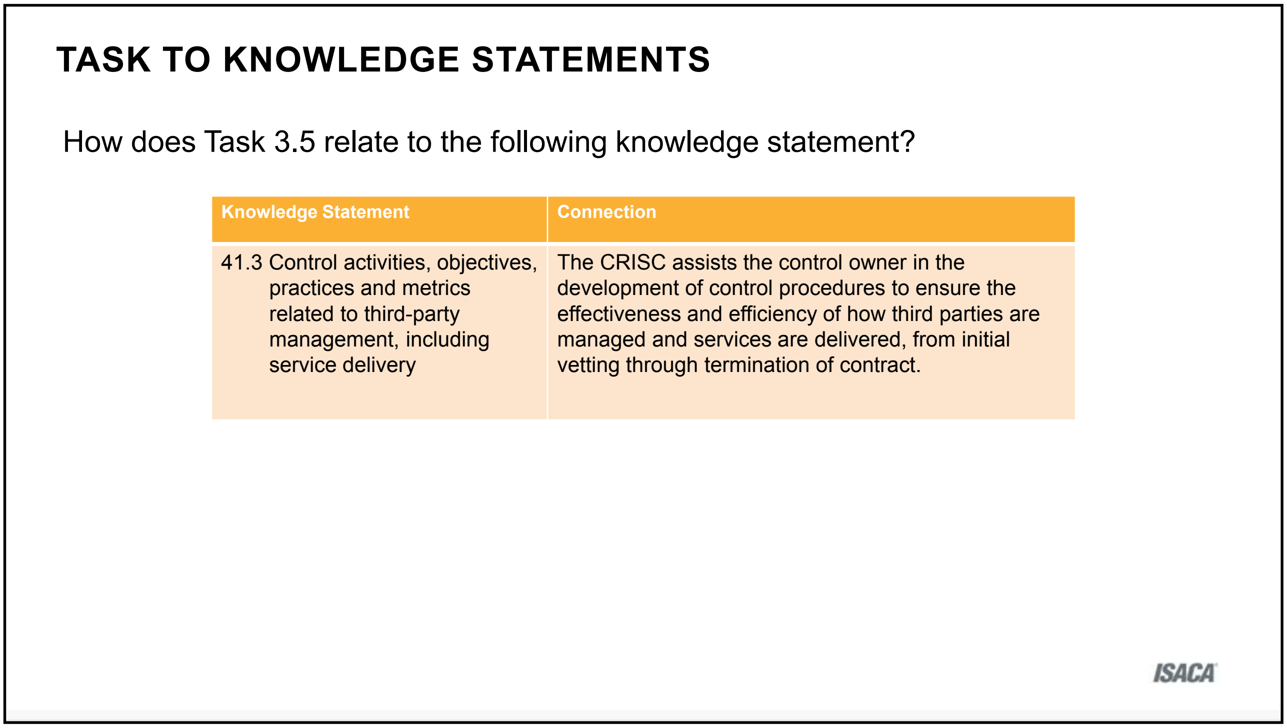
ISACA



TASK TO KNOWLEDGE STATEMENTS

How does Task 3.5 relate to each of the following knowledge statements?

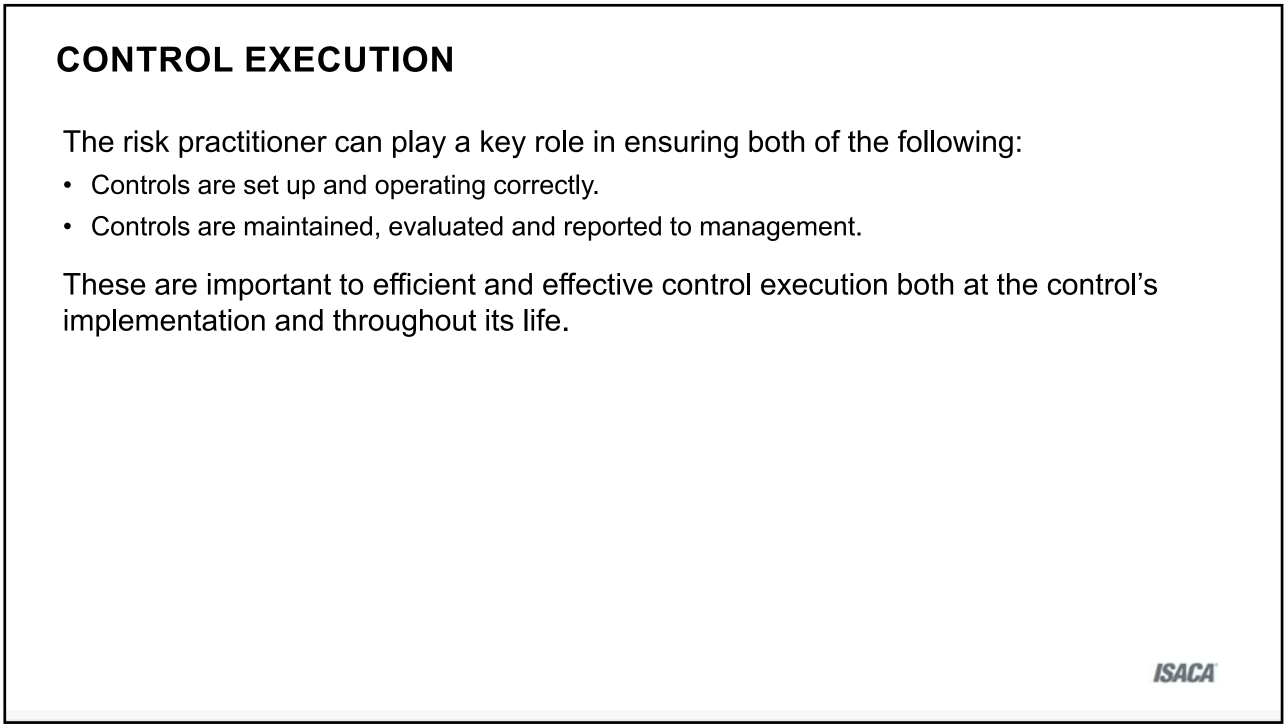
Knowledge Statement	Connection
18. Business process review tools and techniques	The CRISC assists in a consultative manner with the control owner on the development of control procedures and related documentation.
41.1 Control activities, objectives, practices and metrics related to business processes	The CRISC assists the control owner in the development of control procedures to ensure the effectiveness and efficiency of each business process.
41.2 Control activities, objectives, practices and metrics related to information security, including technology certification and accreditation practices	The CRISC assists the control owner in the development of control procedures to ensure the effectiveness and efficiency of the Information Security program components.



TASK TO KNOWLEDGE STATEMENTS

How does Task 3.5 relate to the following knowledge statement?

Knowledge Statement	Connection
41.3 Control activities, objectives, practices and metrics related to third-party management, including service delivery	The CRISC assists the control owner in the development of control procedures to ensure the effectiveness and efficiency of how third parties are managed and services are delivered, from initial vetting through termination of contract.

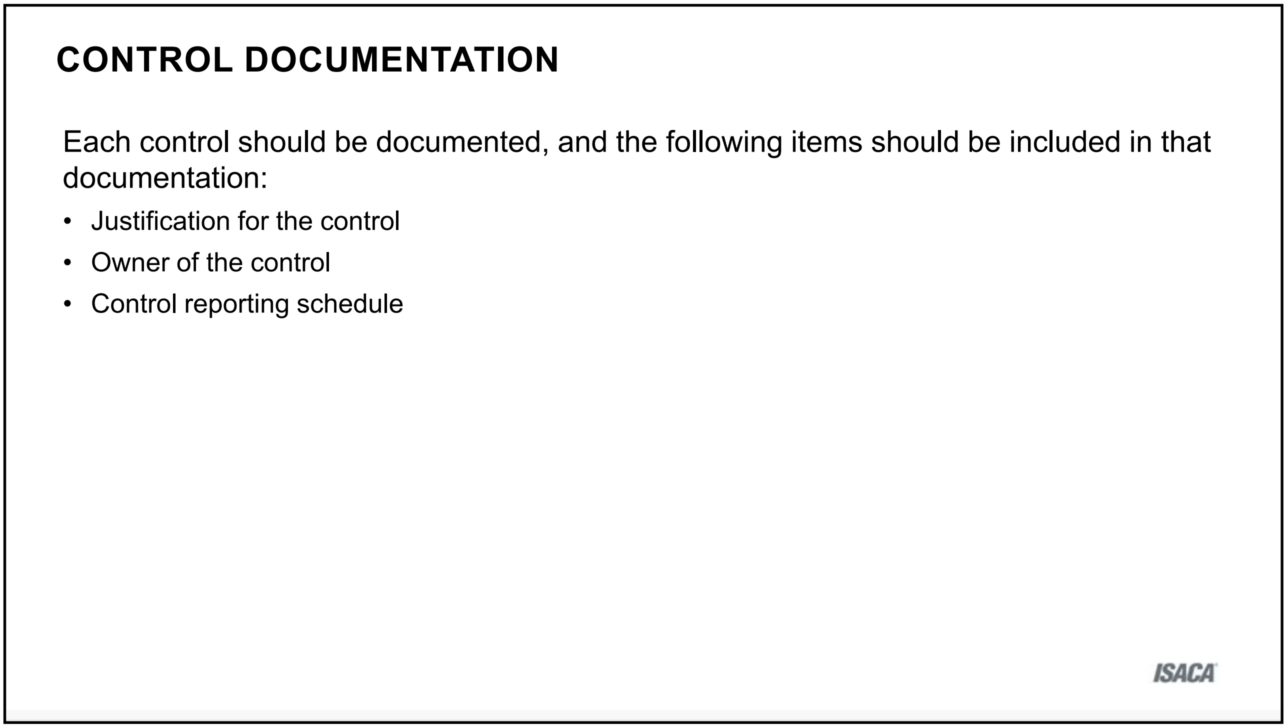


CONTROL EXECUTION

The risk practitioner can play a key role in ensuring both of the following:

- Controls are set up and operating correctly.
- Controls are maintained, evaluated and reported to management.

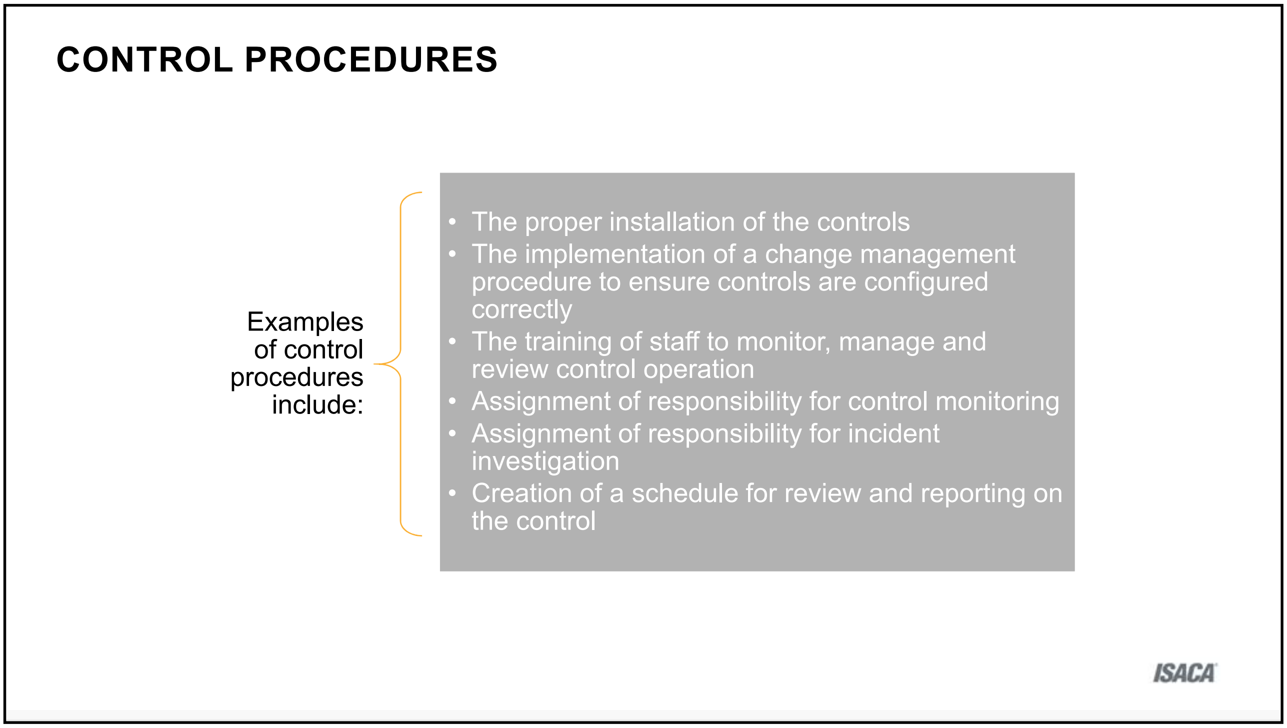
These are important to efficient and effective control execution both at the control’s implementation and throughout its life.



CONTROL DOCUMENTATION

Each control should be documented, and the following items should be included in that documentation:

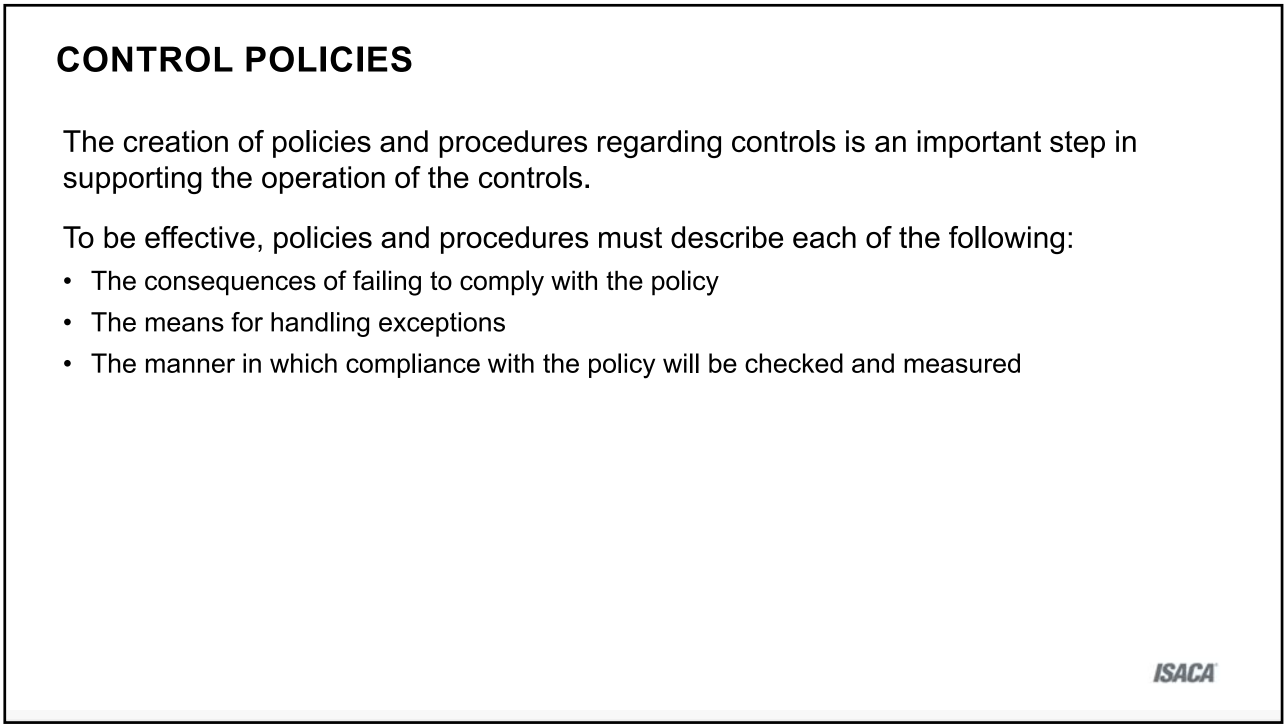
- Justification for the control
- Owner of the control
- Control reporting schedule



CONTROL PROCEDURES

Examples of control procedures include:

- The proper installation of the controls
- The implementation of a change management procedure to ensure controls are configured correctly
- The training of staff to monitor, manage and review control operation
- Assignment of responsibility for control monitoring
- Assignment of responsibility for incident investigation
- Creation of a schedule for review and reporting on the control

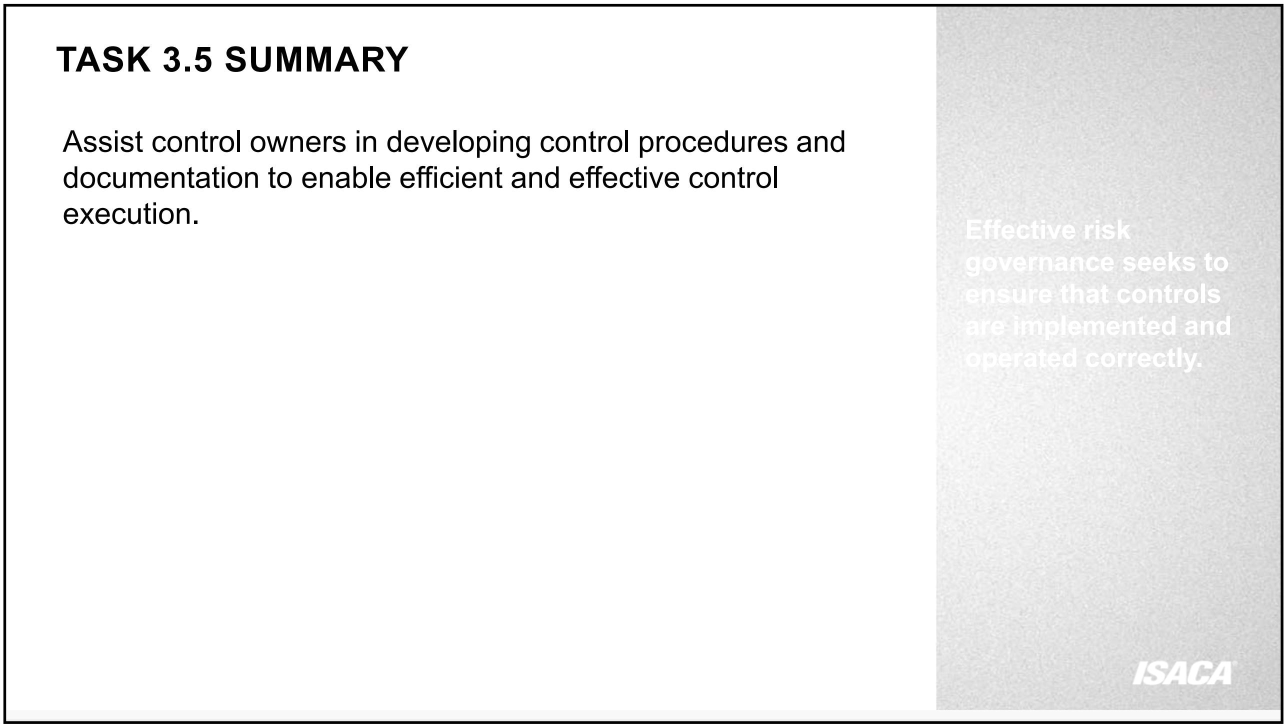


CONTROL POLICIES

The creation of policies and procedures regarding controls is an important step in supporting the operation of the controls.

To be effective, policies and procedures must describe each of the following:

- The consequences of failing to comply with the policy
- The means for handling exceptions
- The manner in which compliance with the policy will be checked and measured



TASK 3.5 SUMMARY

Assist control owners in developing control procedures and documentation to enable efficient and effective control execution.

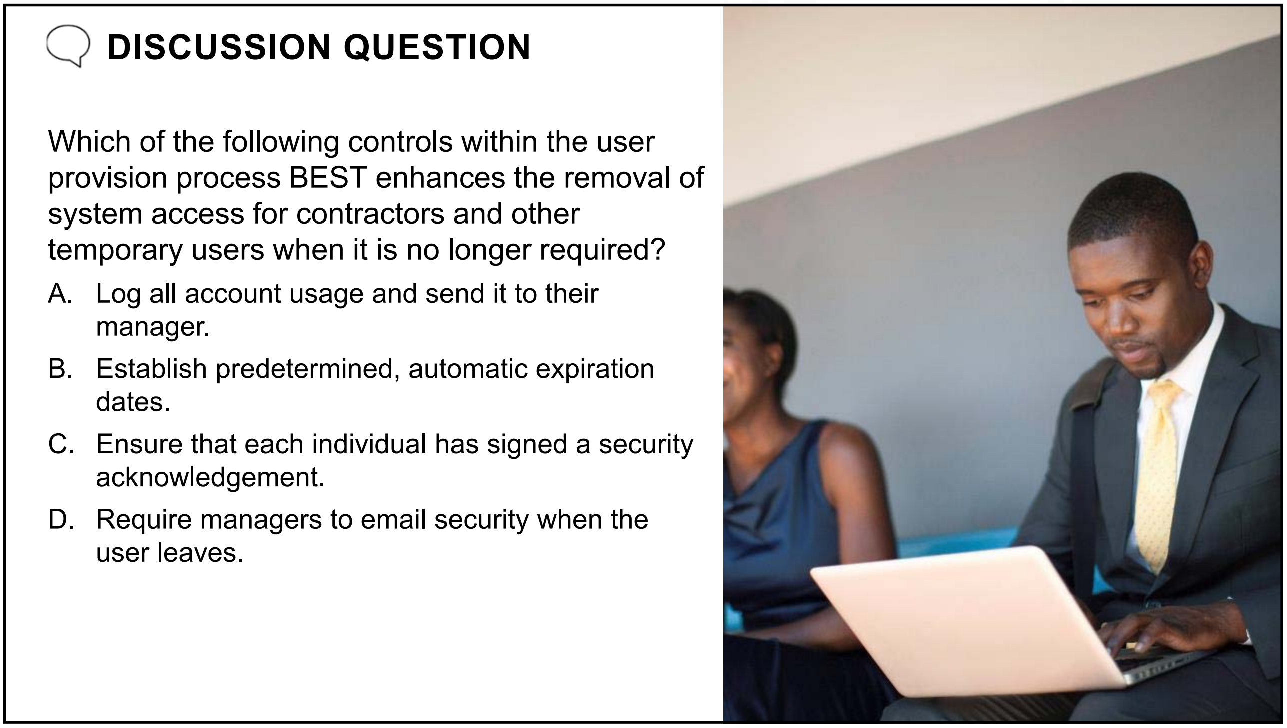
Effective risk governance seeks to ensure that controls are implemented and operated correctly.

TASK 3.5 DISCUSSION

In considering documentation of controls, what elements do you believe are most important?

Which elements are least important?

Provide the reasons for your responses.



DISCUSSION QUESTION

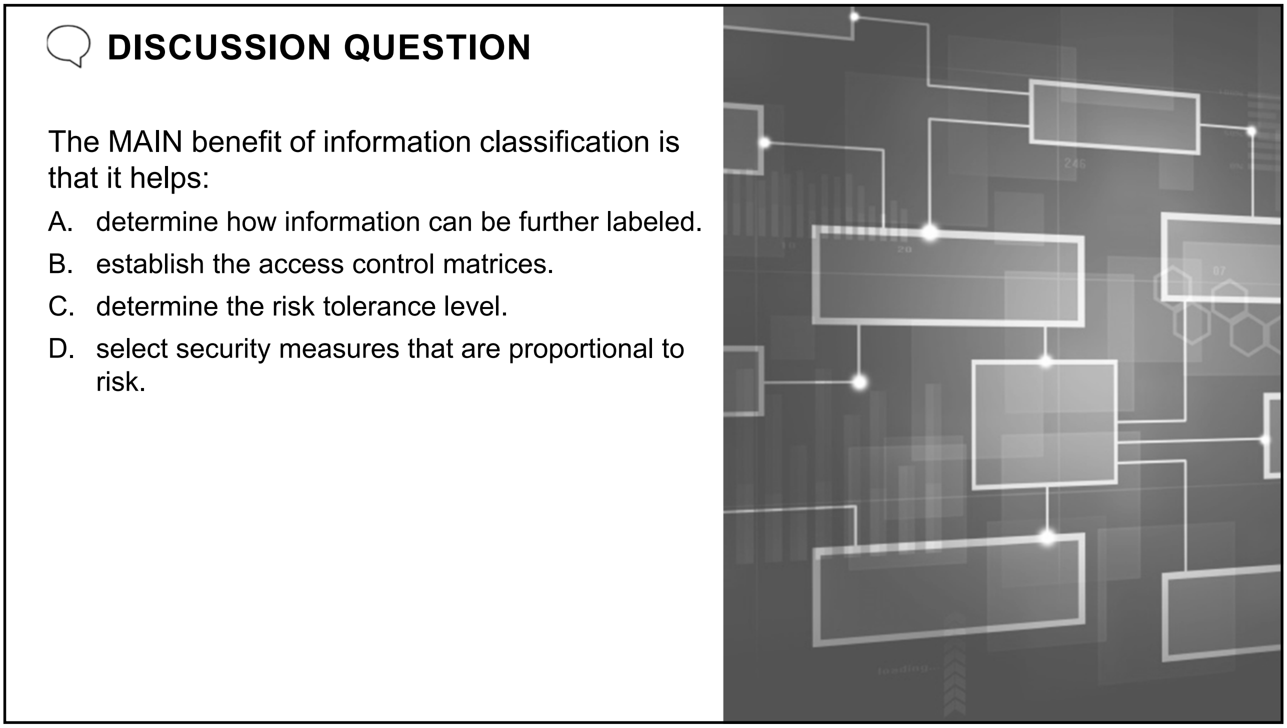
Which of the following controls within the user provision process BEST enhances the removal of system access for contractors and other temporary users when it is no longer required?

A. Log all account usage and send it to their manager.

B. Establish predetermined, automatic expiration dates.

C. Ensure that each individual has signed a security acknowledgement.

D. Require managers to email security when the user leaves.



DISCUSSION QUESTION

The MAIN benefit of information classification is that it helps:

A. determine how information can be further labeled.

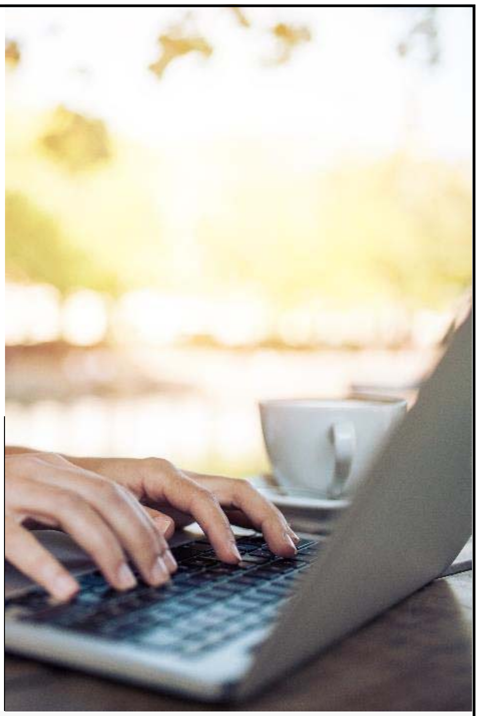
B. establish the access control matrices.

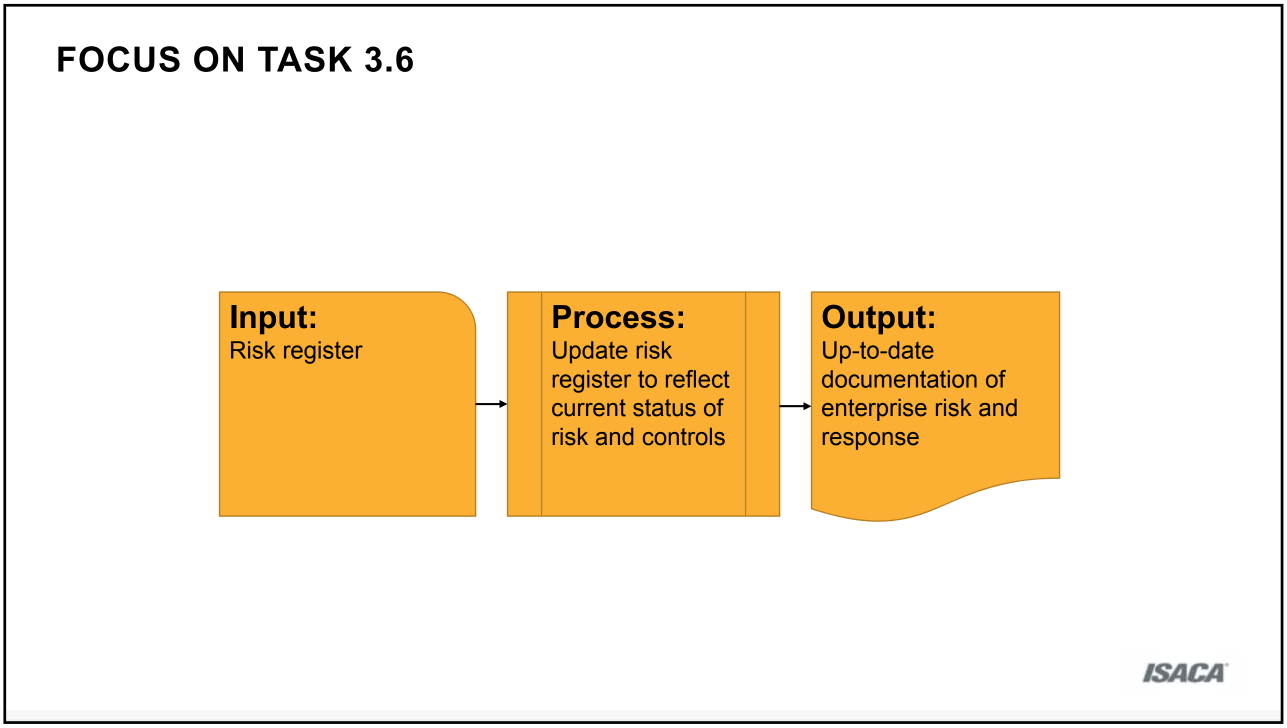
C. determine the risk tolerance level.

D. select security measures that are proportional to risk.

TASK 3.6

Update the risk register to reflect changes in risk and management's risk response.



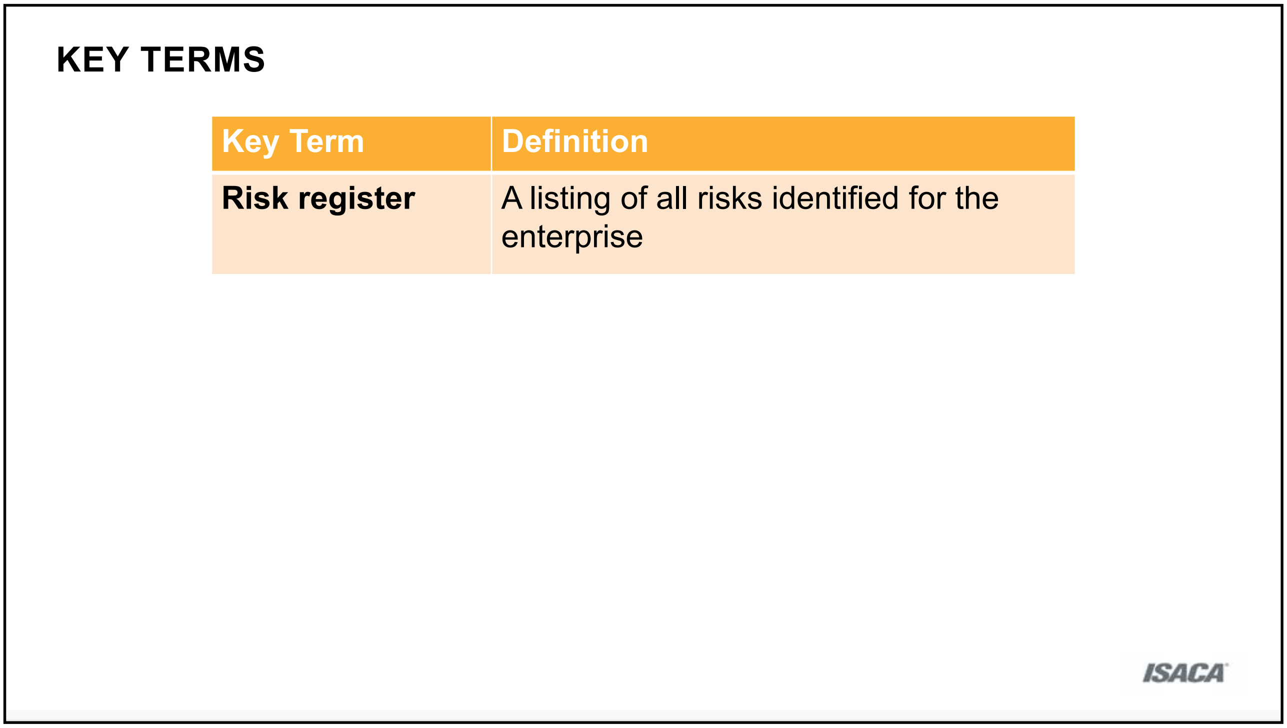


FOCUS ON TASK 3.6

Input:
Risk register

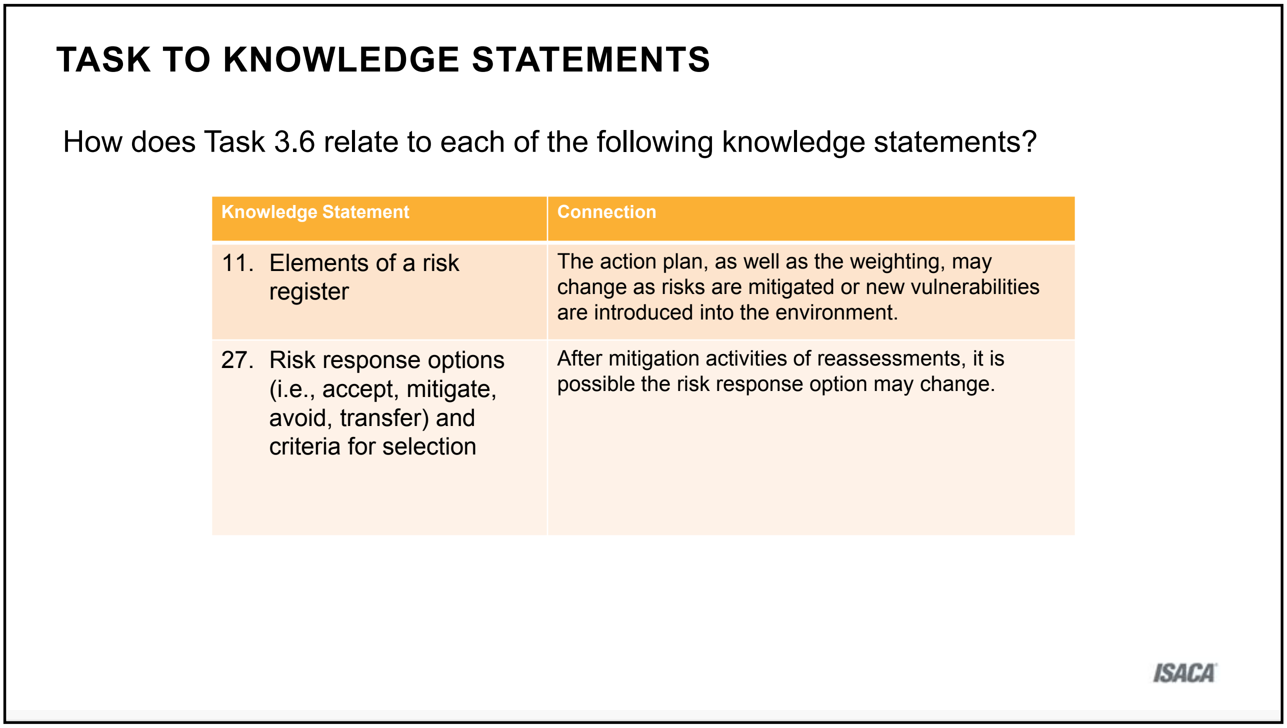
Process:
Update risk register to reflect current status of risk and controls

Output:
Up-to-date documentation of enterprise risk and response



KEY TERMS

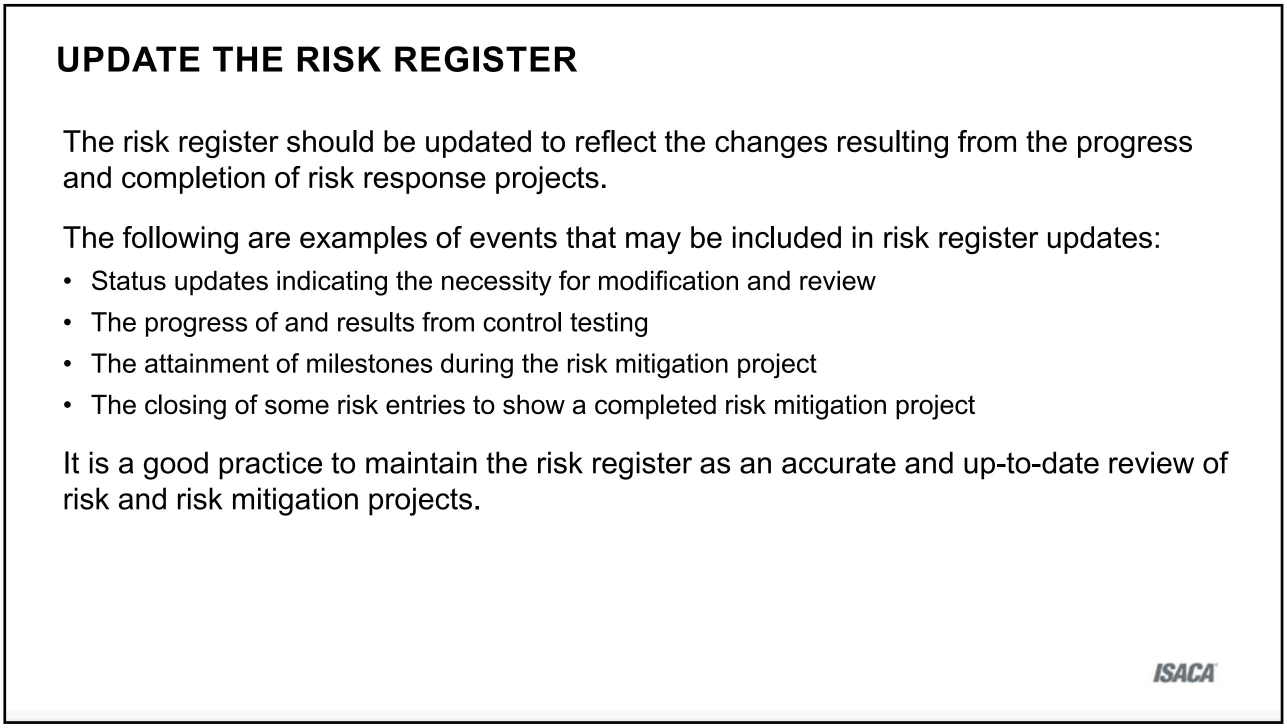
Key Term	Definition
Risk register	A listing of all risks identified for the enterprise



TASK TO KNOWLEDGE STATEMENTS

How does Task 3.6 relate to each of the following knowledge statements?

Knowledge Statement	Connection
11. Elements of a risk register	The action plan, as well as the weighting, may change as risks are mitigated or new vulnerabilities are introduced into the environment.
27. Risk response options (i.e., accept, mitigate, avoid, transfer) and criteria for selection	After mitigation activities of reassessments, it is possible the risk response option may change.



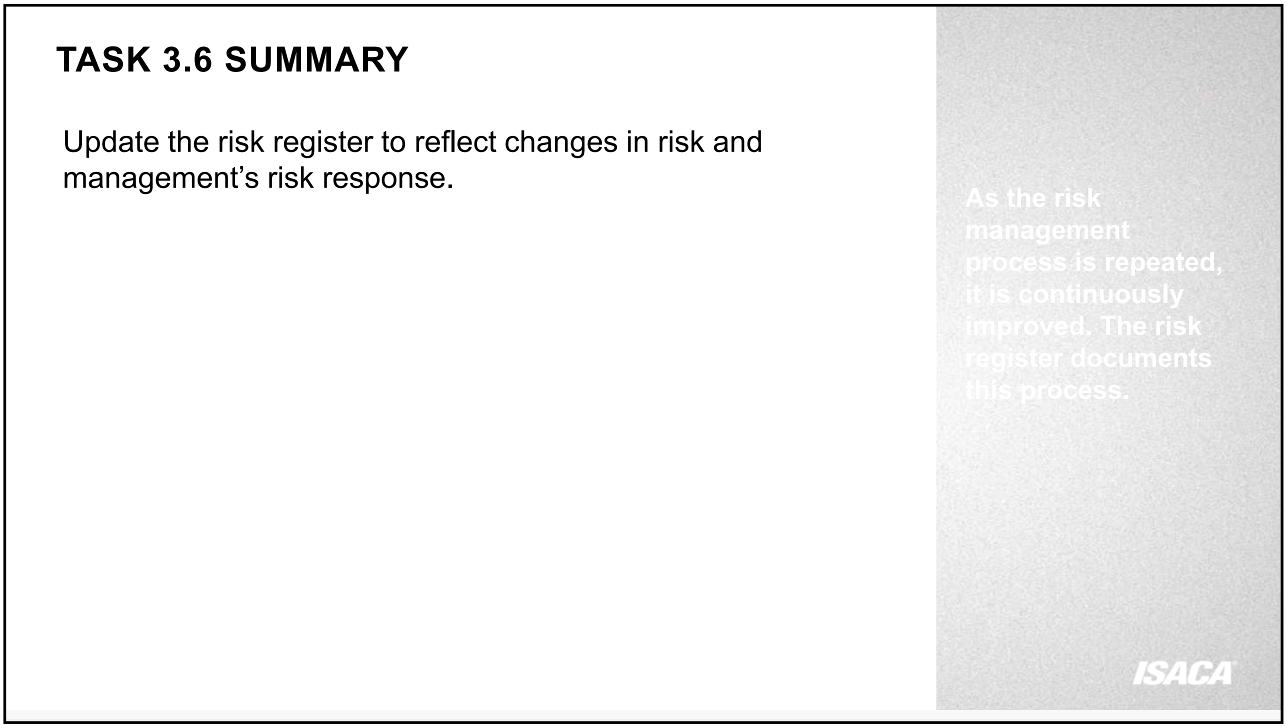
UPDATE THE RISK REGISTER

The risk register should be updated to reflect the changes resulting from the progress and completion of risk response projects.

The following are examples of events that may be included in risk register updates:

- Status updates indicating the necessity for modification and review
- The progress of and results from control testing
- The attainment of milestones during the risk mitigation project
- The closing of some risk entries to show a completed risk mitigation project

It is a good practice to maintain the risk register as an accurate and up-to-date review of risk and risk mitigation projects.



TASK 3.6 SUMMARY

Update the risk register to reflect changes in risk and management’s risk response.

As the risk management process is repeated, it is continuously improved. The risk register documents this process.

TASK 3.6 ACTIVITY

Using your risk register, update Parts I and IV with risk control information.

DISCUSSION QUESTION

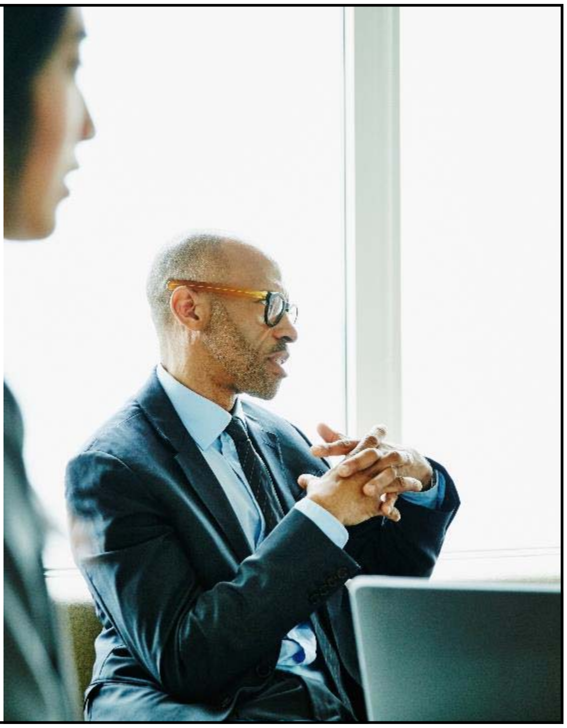
A business case developed to support risk mitigation efforts for a complex application development project should be retained until:

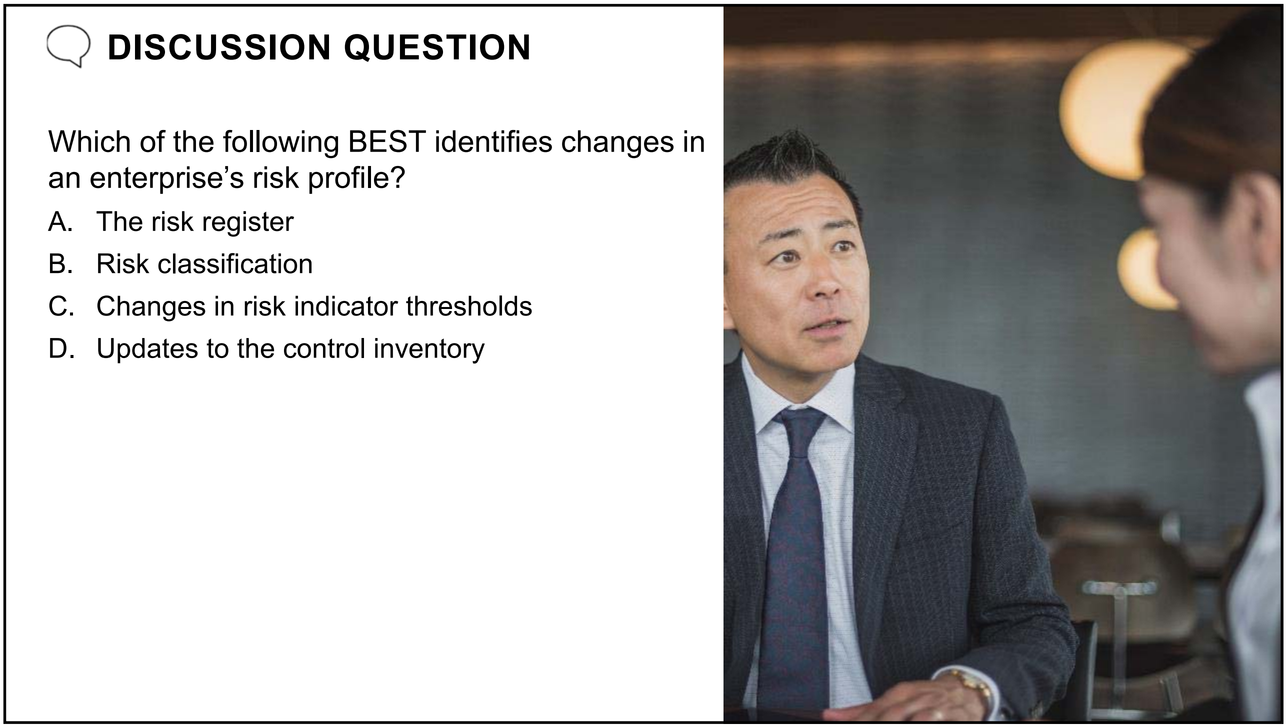
A. the project is approved.

B. user acceptance of the application.

C. the application is deployed.

D. the application’s end of life.





DISCUSSION QUESTION

Which of the following BEST identifies changes in an enterprise’s risk profile?

A. The risk register

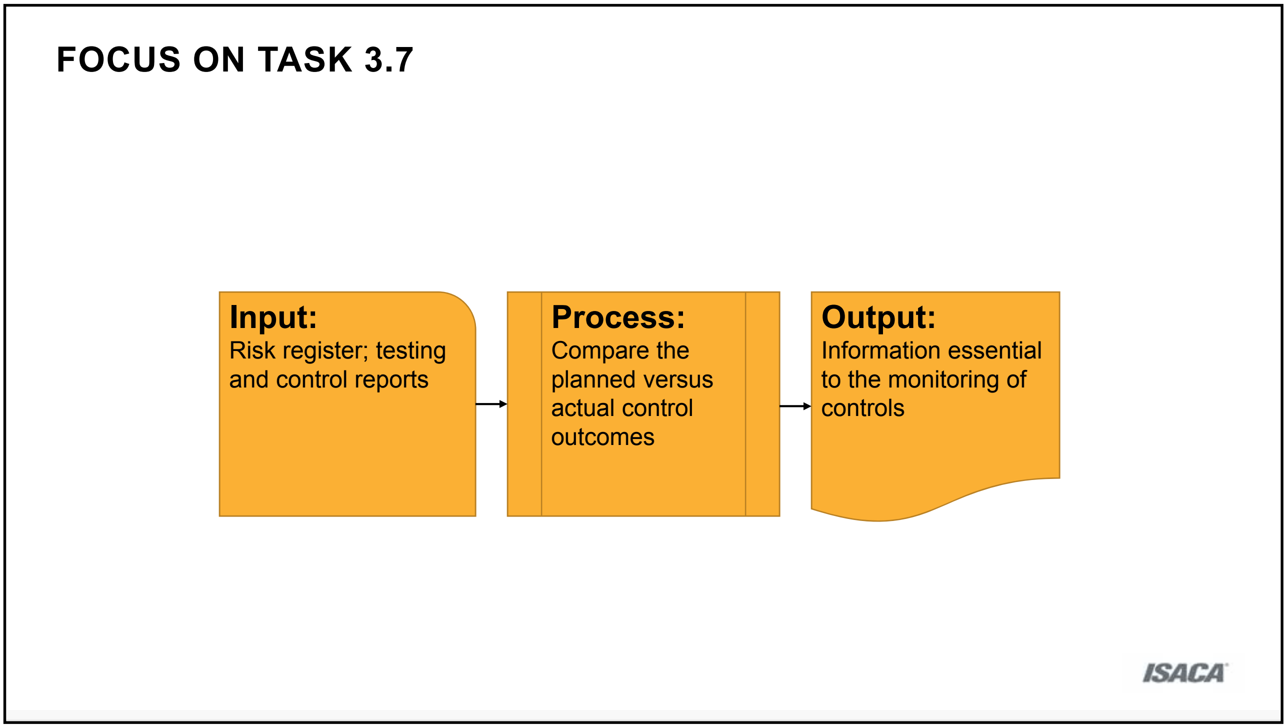
B. Risk classification

C. Changes in risk indicator thresholds

D. Updates to the control inventory

TASK 3.7

Validate that risk responses have been executed according to the risk action plans.

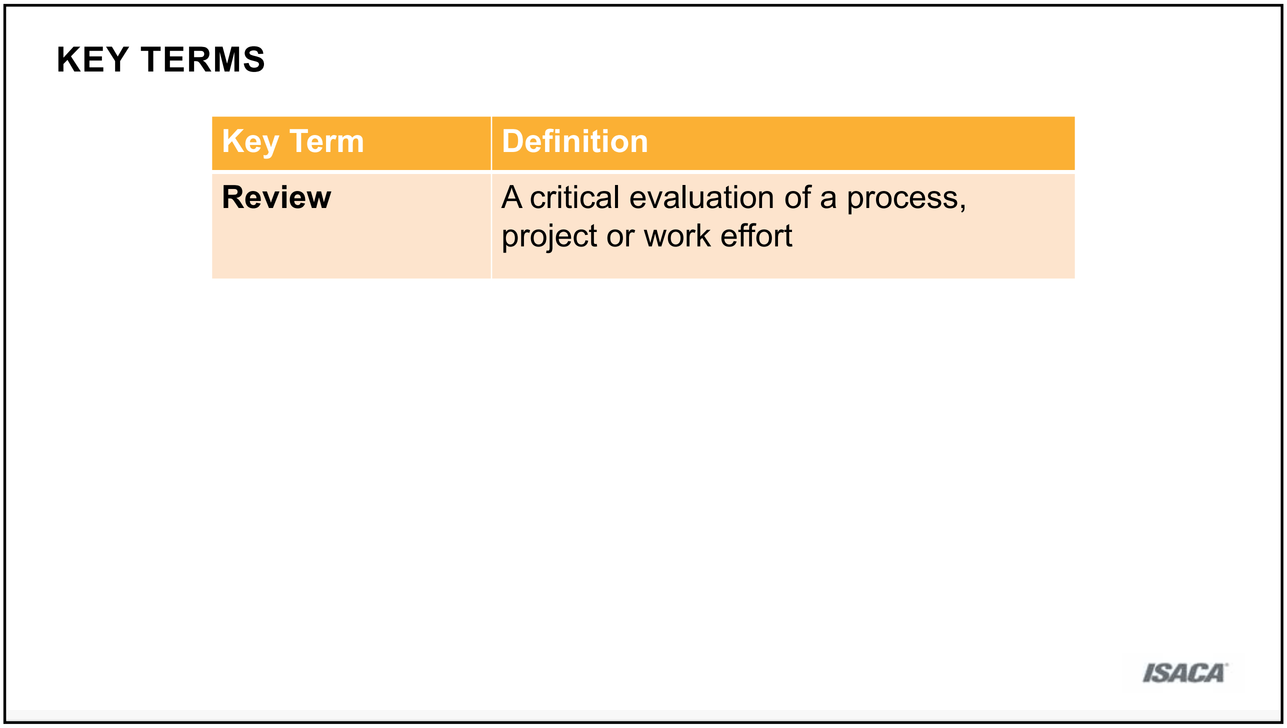


FOCUS ON TASK 3.7

Input:
Risk register; testing and control reports

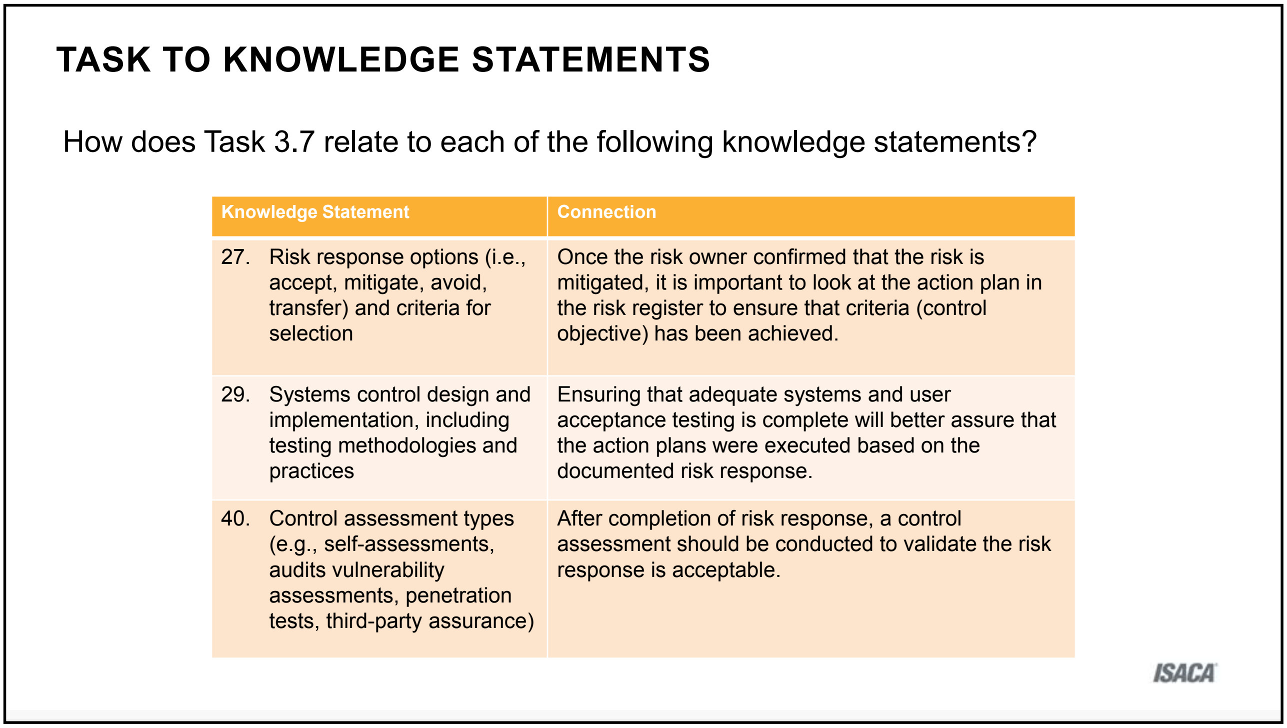
Process:
Compare the planned versus actual control outcomes

Output:
Information essential to the monitoring of controls



KEY TERMS

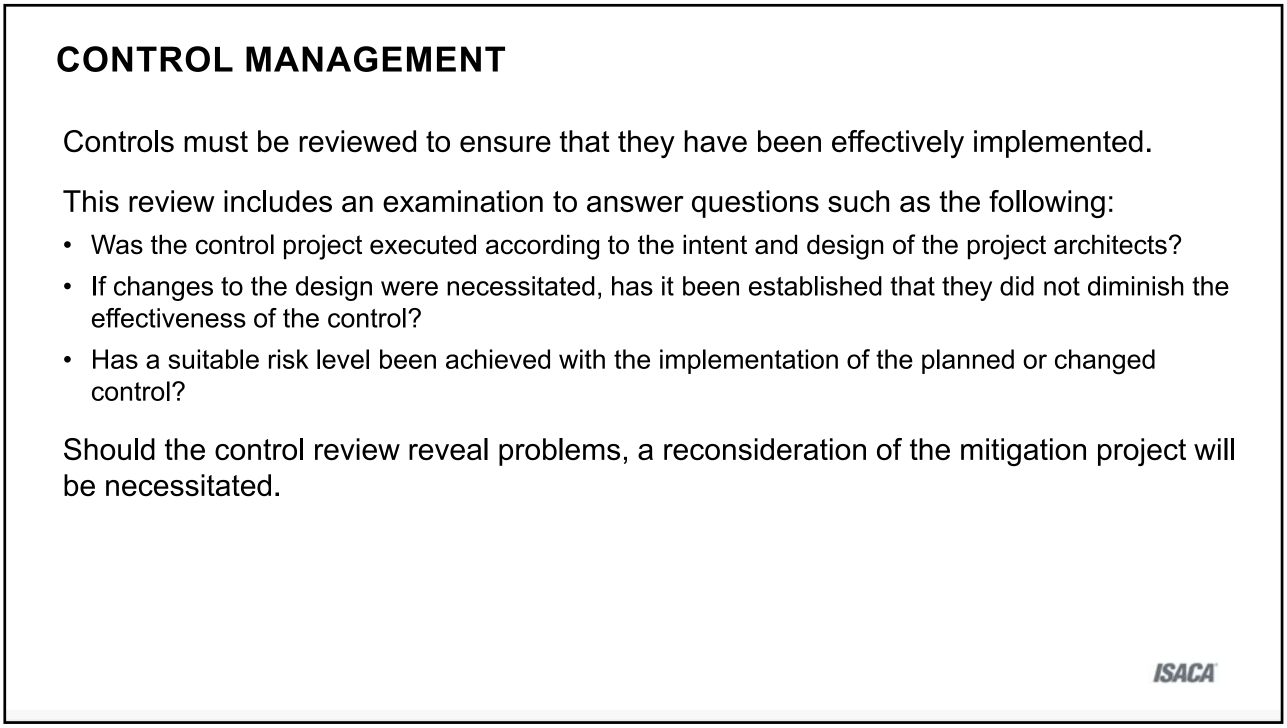
Key Term	Definition
Review	A critical evaluation of a process, project or work effort



TASK TO KNOWLEDGE STATEMENTS

How does Task 3.7 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	Once the risk owner confirmed that the risk is mitigated, it is important to look at the action plan in the risk register to ensure that criteria (control objective) has been achieved.
29. Systems control design and implementation, including testing methodologies and practices	Ensuring that adequate systems and user acceptance testing is complete will better assure that the action plans were executed based on the documented risk response.
40. Control assessment types (e.g., self-assessments, audits vulnerability assessments, penetration tests, third-party assurance)	After completion of risk response, a control assessment should be conducted to validate the risk response is acceptable.



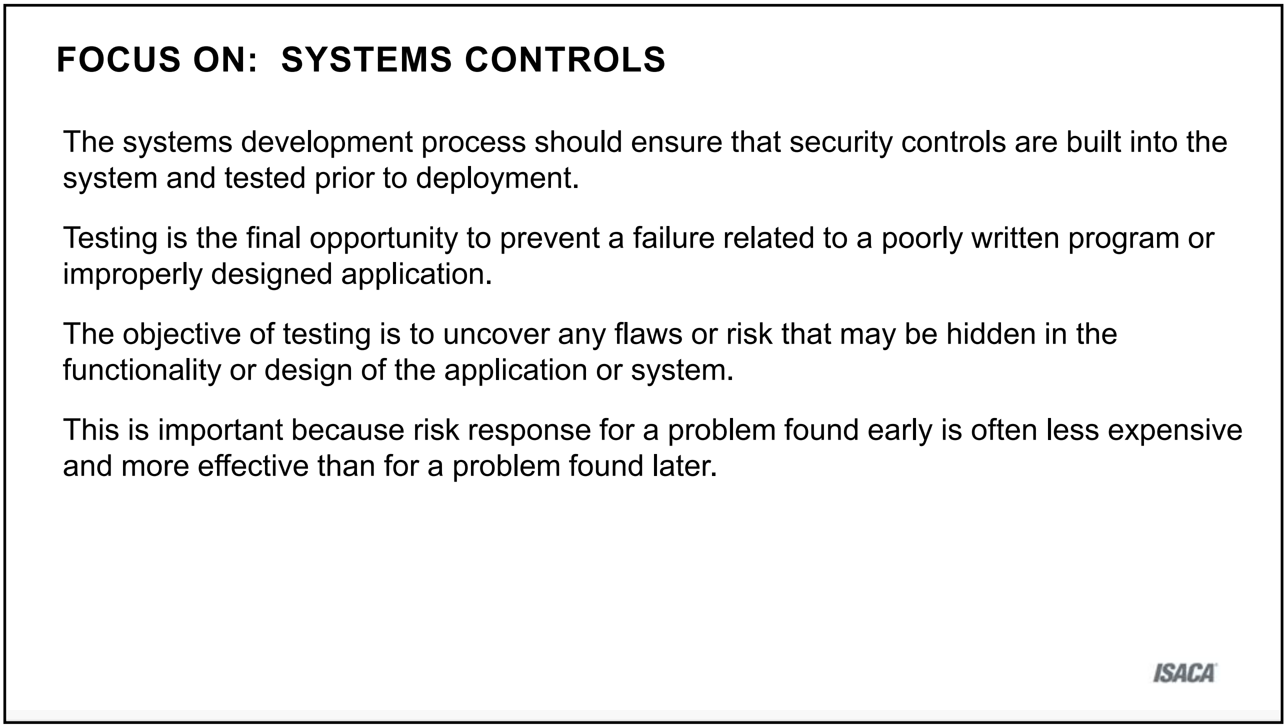
CONTROL MANAGEMENT

Controls must be reviewed to ensure that they have been effectively implemented.

This review includes an examination to answer questions such as the following:

- Was the control project executed according to the intent and design of the project architects?
- If changes to the design were necessitated, has it been established that they did not diminish the effectiveness of the control?
- Has a suitable risk level been achieved with the implementation of the planned or changed control?

Should the control review reveal problems, a reconsideration of the mitigation project will be necessitated.



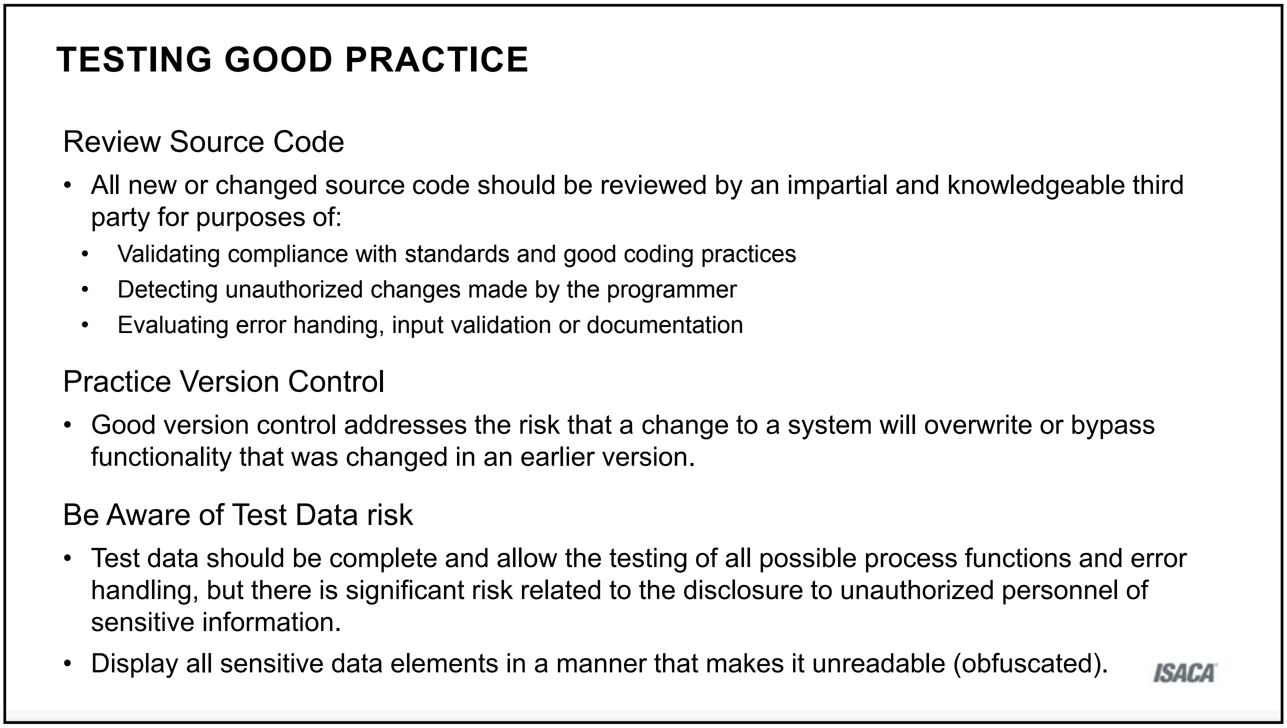
FOCUS ON: SYSTEMS CONTROLS

The systems development process should ensure that security controls are built into the system and tested prior to deployment.

Testing is the final opportunity to prevent a failure related to a poorly written program or improperly designed application.

The objective of testing is to uncover any flaws or risk that may be hidden in the functionality or design of the application or system.

This is important because risk response for a problem found early is often less expensive and more effective than for a problem found later.



TESTING GOOD PRACTICE

Review Source Code

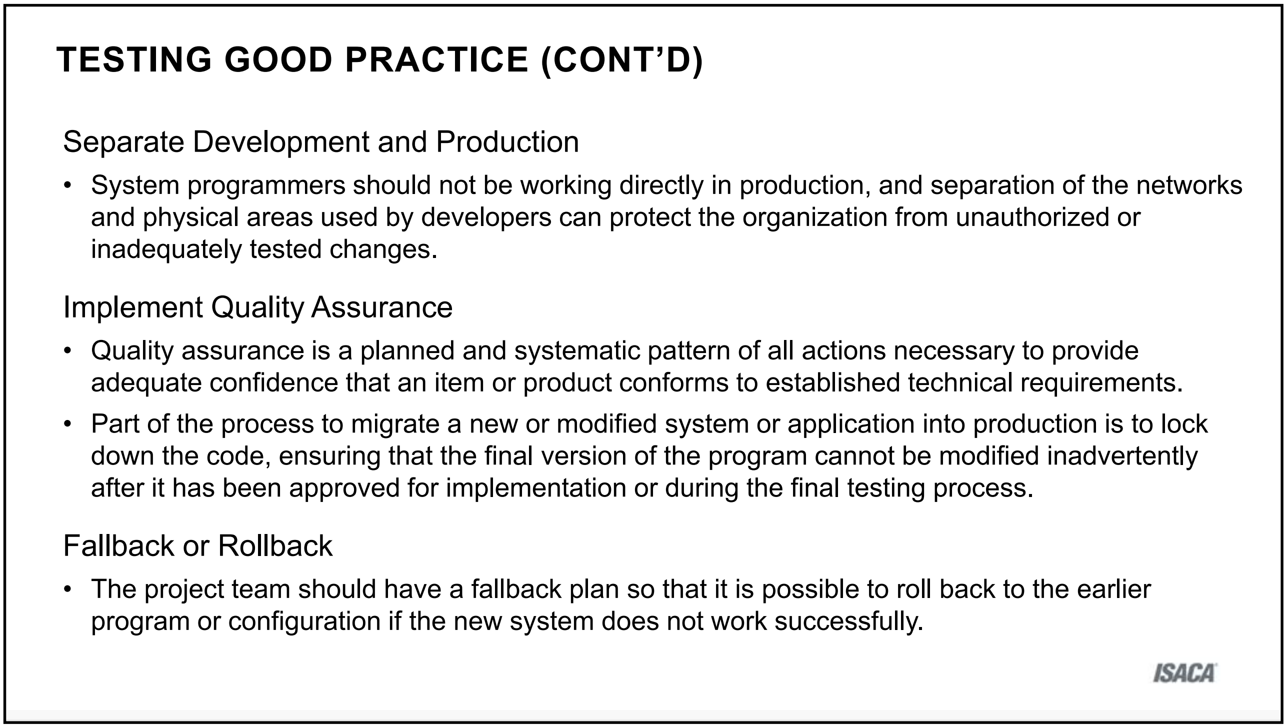
- All new or changed source code should be reviewed by an impartial and knowledgeable third party for purposes of:
  - Validating compliance with standards and good coding practices
  - Detecting unauthorized changes made by the programmer
  - Evaluating error handing, input validation or documentation

Practice Version Control

- Good version control addresses the risk that a change to a system will overwrite or bypass functionality that was changed in an earlier version.

Be Aware of Test Data risk

- Test data should be complete and allow the testing of all possible process functions and error handling, but there is significant risk related to the disclosure to unauthorized personnel of sensitive information.
- Display all sensitive data elements in a manner that makes it unreadable (obfuscated).



TESTING GOOD PRACTICE (CONT'D)

Separate Development and Production

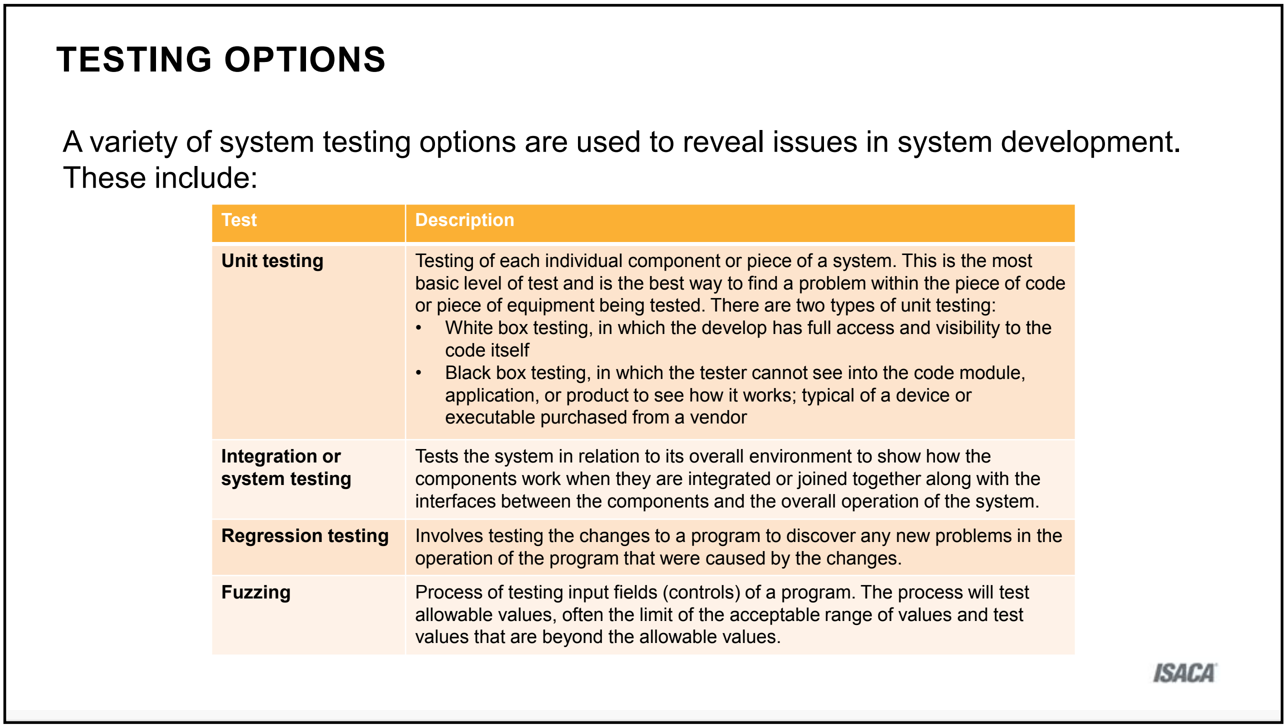
- System programmers should not be working directly in production, and separation of the networks and physical areas used by developers can protect the organization from unauthorized or inadequately tested changes.

Implement Quality Assurance

- Quality assurance is a planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements.
- Part of the process to migrate a new or modified system or application into production is to lock down the code, ensuring that the final version of the program cannot be modified inadvertently after it has been approved for implementation or during the final testing process.

Fallback or Rollback

- The project team should have a fallback plan so that it is possible to roll back to the earlier program or configuration if the new system does not work successfully.

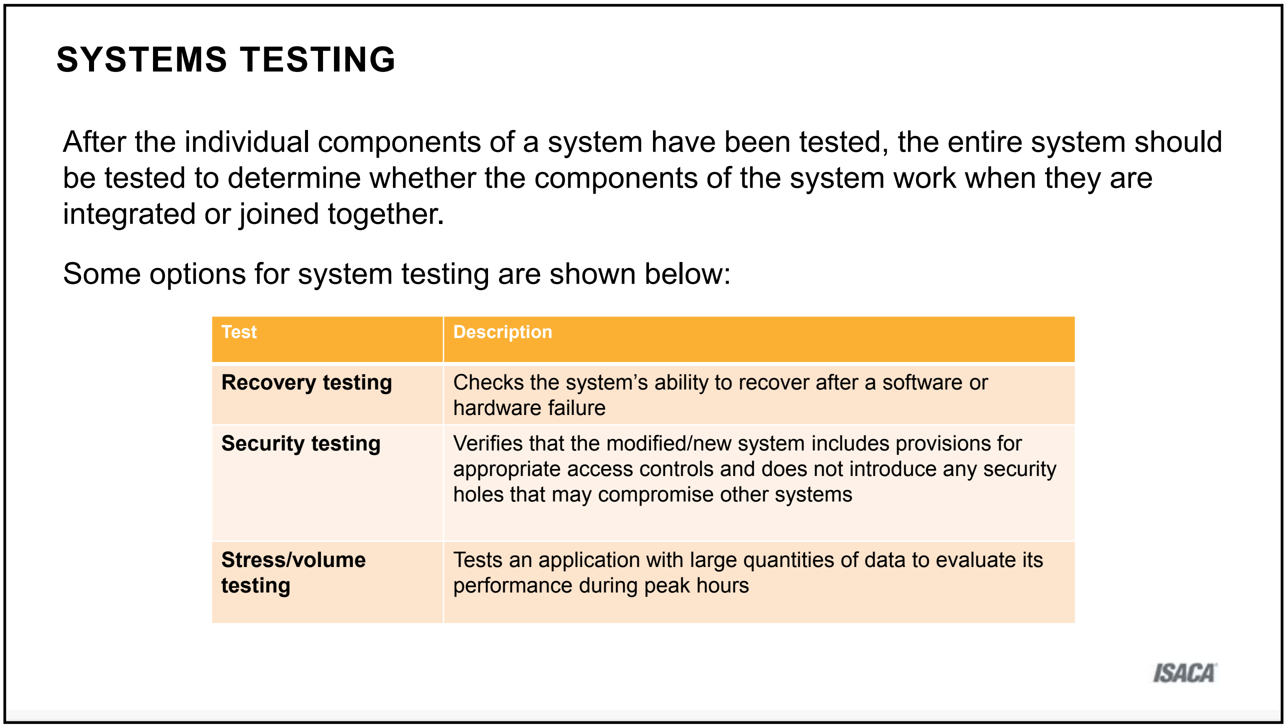


TESTING OPTIONS

A variety of system testing options are used to reveal issues in system development. These include:

Test	Description
Unit testing	Testing of each individual component or piece of a system. This is the most basic level of test and is the best way to find a problem within the piece of code or piece of equipment being tested. There are two types of unit testing: • White box testing, in which the develop has full access and visibility to the code itself • Black box testing, in which the tester cannot see into the code module, application, or product to see how it works; typical of a device or executable purchased from a vendor
Integration or system testing	Tests the system in relation to its overall environment to show how the components work when they are integrated or joined together along with the interfaces between the components and the overall operation of the system.
Regression testing	Involves testing the changes to a program to discover any new problems in the operation of the program that were caused by the changes.
Fuzzing	Process of testing input fields (controls) of a program. The process will test allowable values, often the limit of the acceptable range of values and test values that are beyond the allowable values.

ISACA

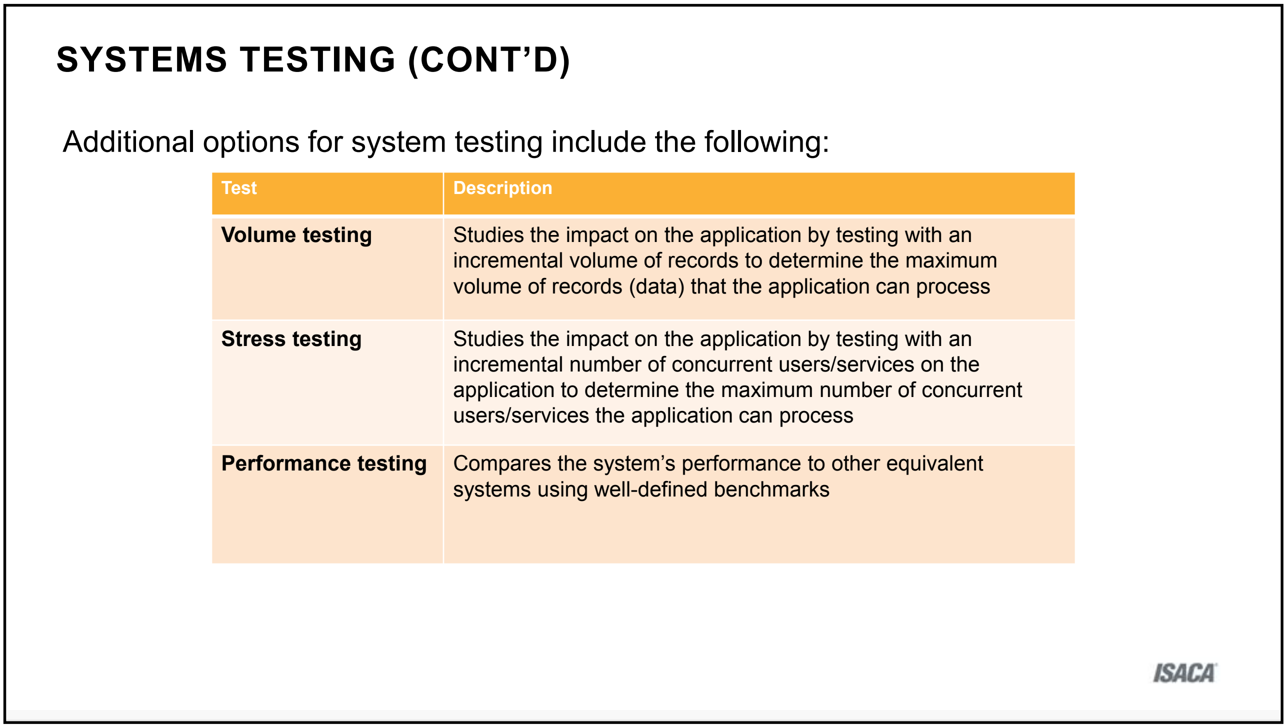


SYSTEMS TESTING

After the individual components of a system have been tested, the entire system should be tested to determine whether the components of the system work when they are integrated or joined together.

Some options for system testing are shown below:

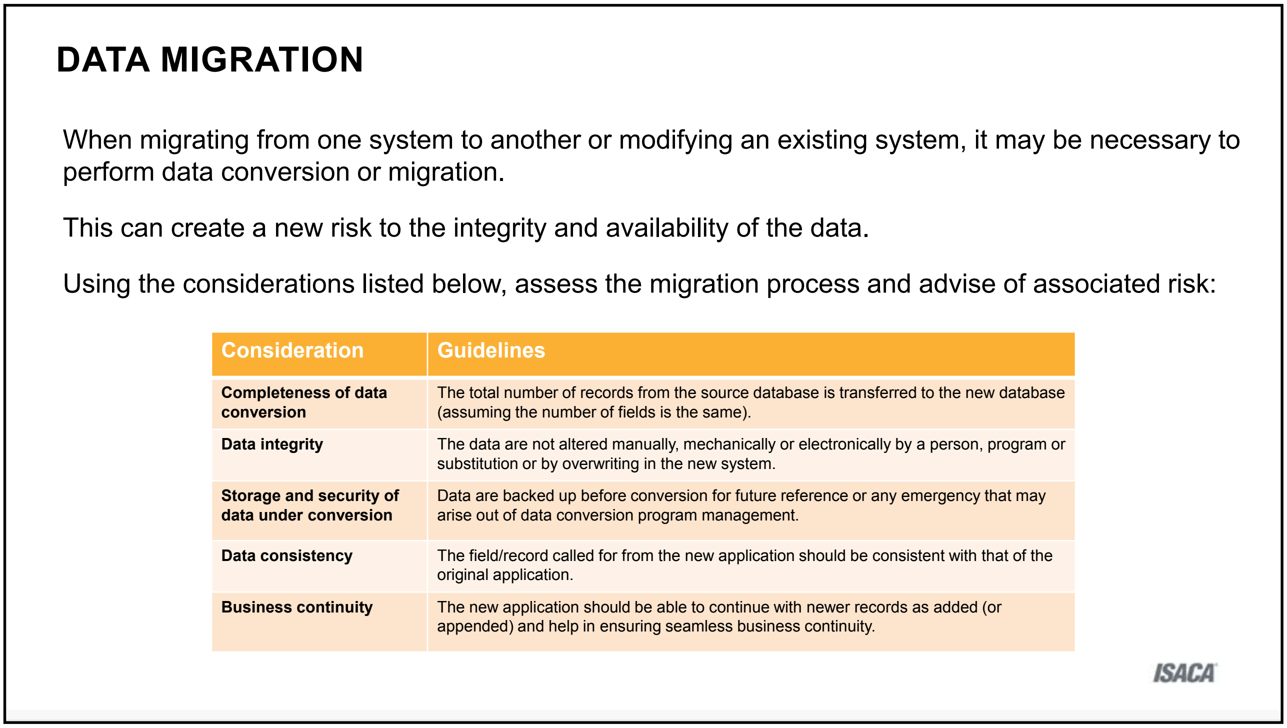
Test	Description
Recovery testing	Checks the system's ability to recover after a software or hardware failure
Security testing	Verifies that the modified/new system includes provisions for appropriate access controls and does not introduce any security holes that may compromise other systems
Stress/volume testing	Tests an application with large quantities of data to evaluate its performance during peak hours



SYSTEMS TESTING (CONT'D)

Additional options for system testing include the following:

Test	Description
Volume testing	Studies the impact on the application by testing with an incremental volume of records to determine the maximum volume of records (data) that the application can process
Stress testing	Studies the impact on the application by testing with an incremental number of concurrent users/services on the application to determine the maximum number of concurrent users/services the application can process
Performance testing	Compares the system's performance to other equivalent systems using well-defined benchmarks



DATA MIGRATION

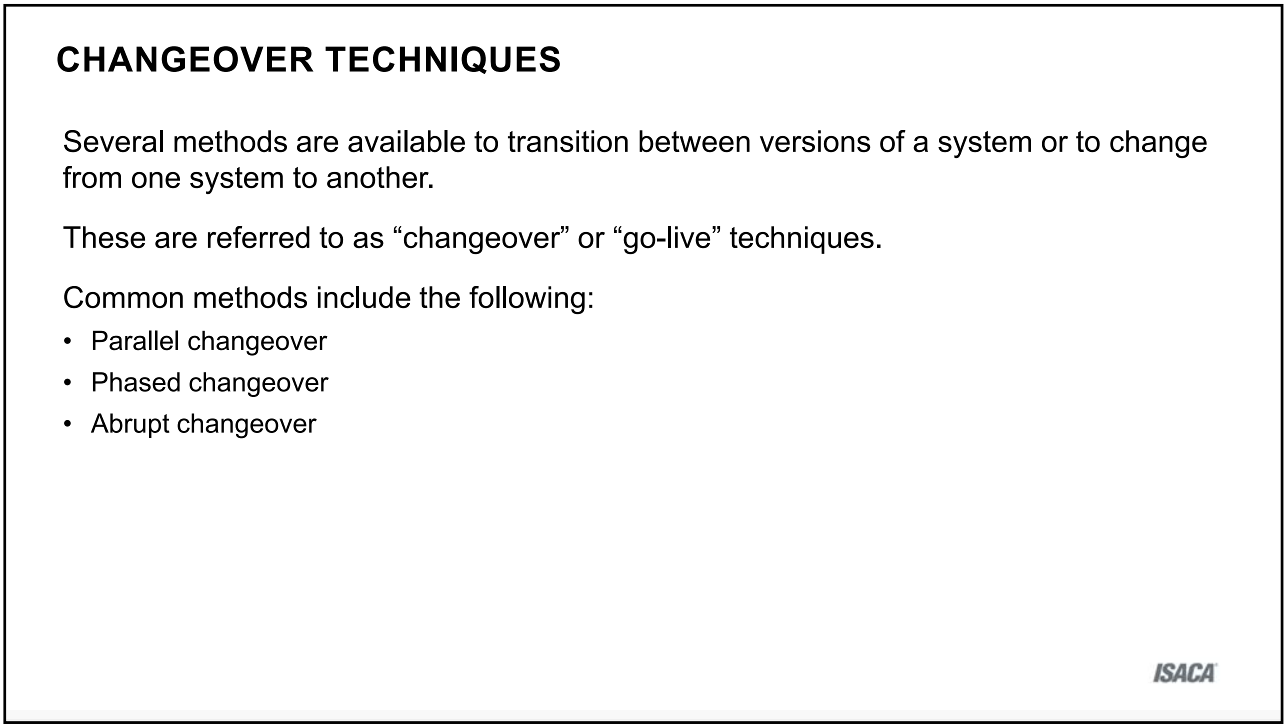
When migrating from one system to another or modifying an existing system, it may be necessary to perform data conversion or migration.

This can create a new risk to the integrity and availability of the data.

Using the considerations listed below, assess the migration process and advise of associated risk:

Consideration	Guidelines
Completeness of data conversion	The total number of records from the source database is transferred to the new database (assuming the number of fields is the same).
Data integrity	The data are not altered manually, mechanically or electronically by a person, program or substitution or by overwriting in the new system.
Storage and security of data under conversion	Data are backed up before conversion for future reference or any emergency that may arise out of data conversion program management.
Data consistency	The field/record called for from the new application should be consistent with that of the original application.
Business continuity	The new application should be able to continue with newer records as added (or appended) and help in ensuring seamless business continuity.

ISACA



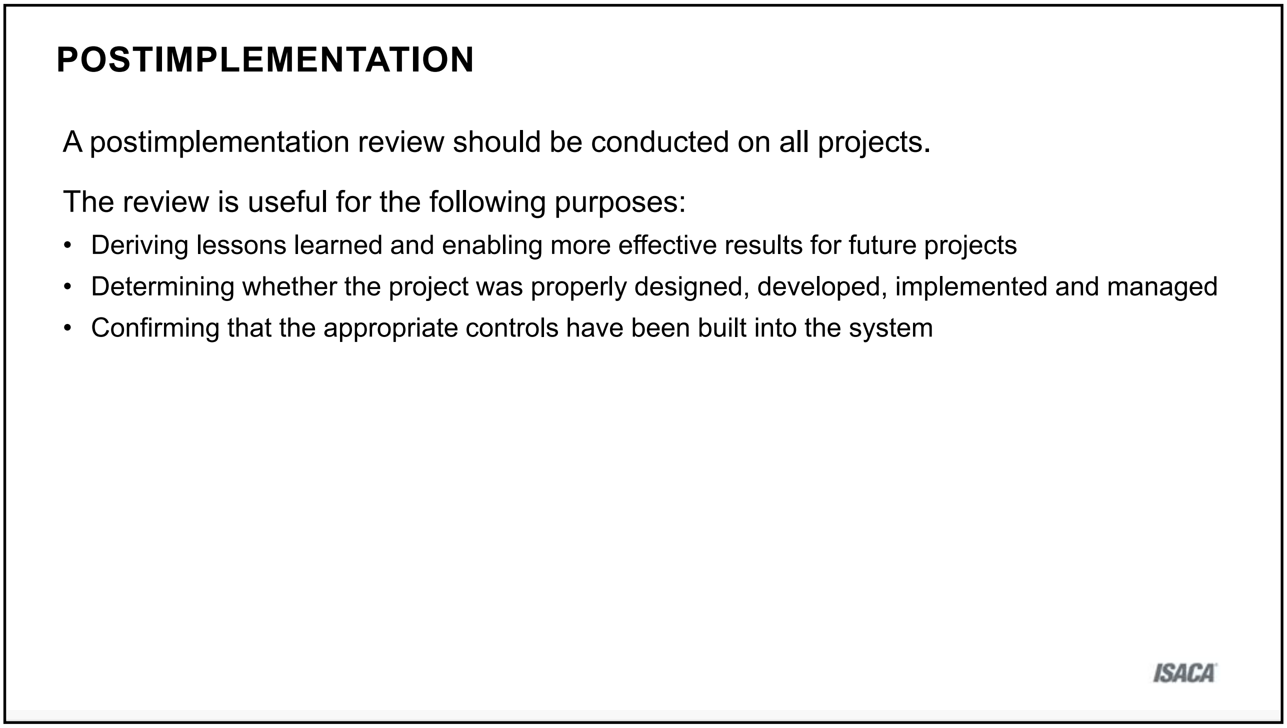
CHANGEOVER TECHNIQUES

Several methods are available to transition between versions of a system or to change from one system to another.

These are referred to as “changeover” or “go-live” techniques.

Common methods include the following:

- Parallel changeover
- Phased changeover
- Abrupt changeover

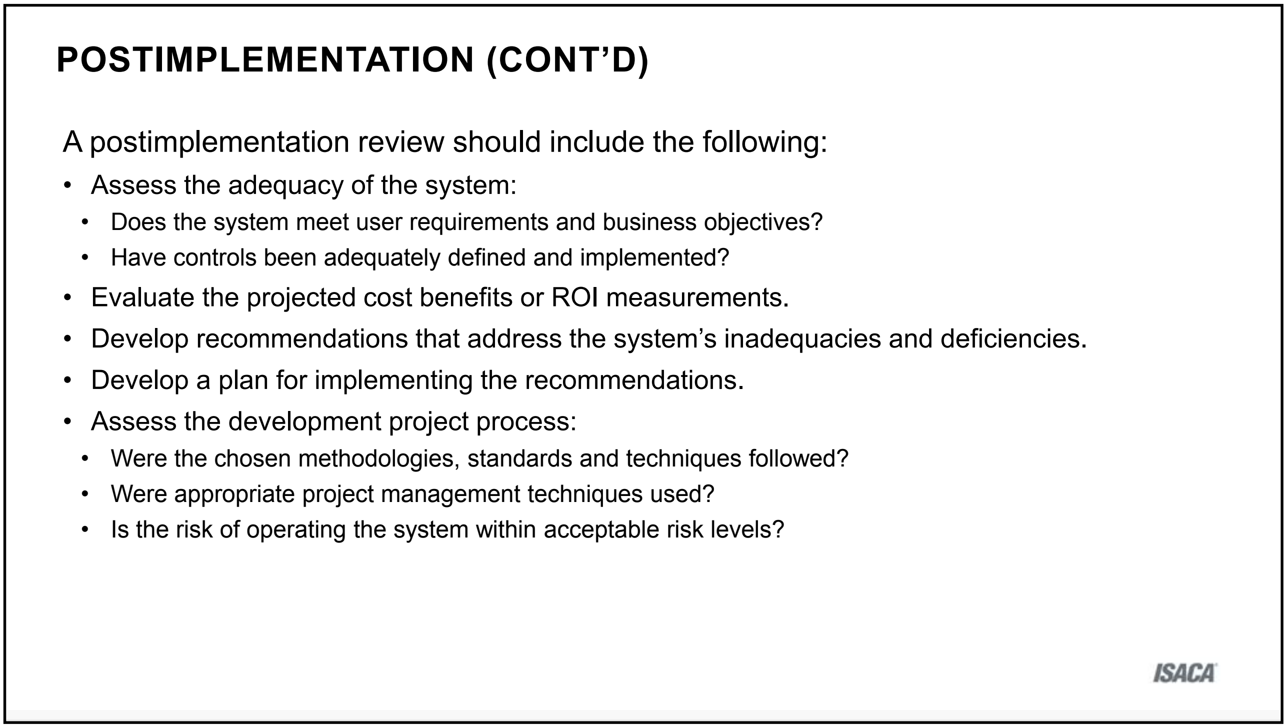


POSTIMPLEMENTATION

A postimplementation review should be conducted on all projects.

The review is useful for the following purposes:

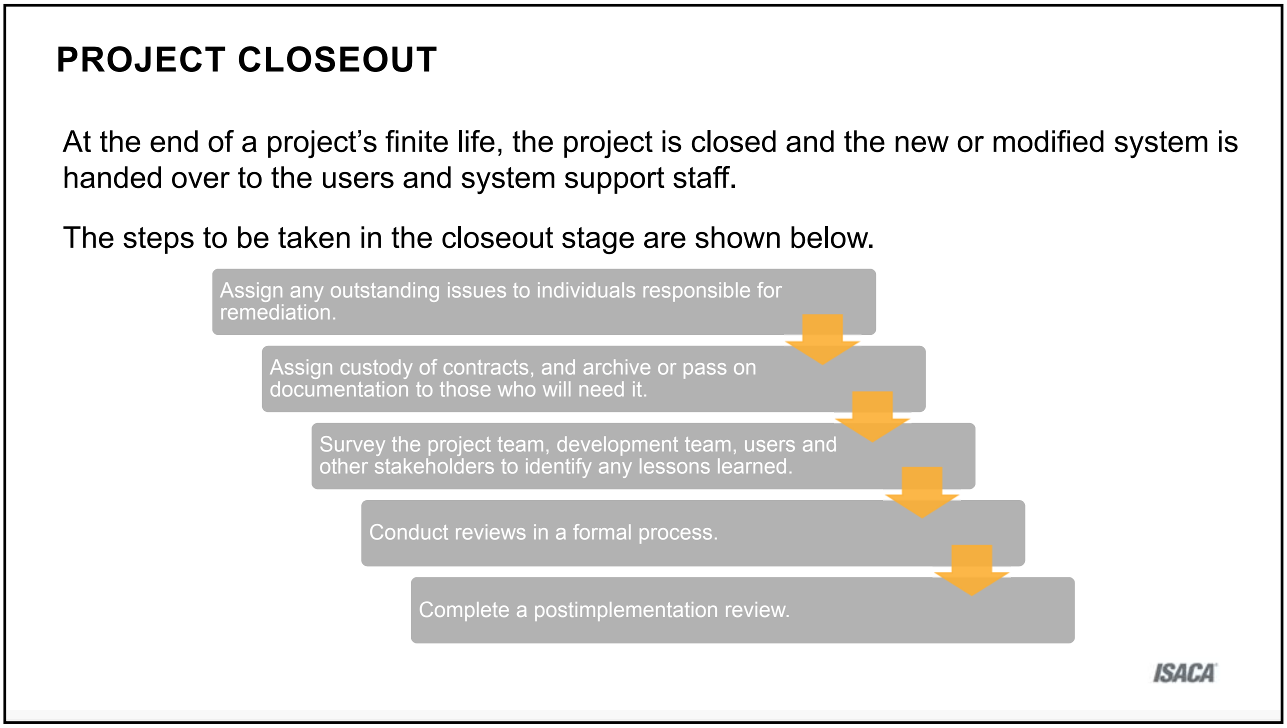
- Deriving lessons learned and enabling more effective results for future projects
- Determining whether the project was properly designed, developed, implemented and managed
- Confirming that the appropriate controls have been built into the system



POSTIMPLEMENTATION (CONT'D)

A postimplementation review should include the following:

- Assess the adequacy of the system:
  - Does the system meet user requirements and business objectives?
  - Have controls been adequately defined and implemented?
- Evaluate the projected cost benefits or ROI measurements.
- Develop recommendations that address the system's inadequacies and deficiencies.
- Develop a plan for implementing the recommendations.
- Assess the development project process:
  - Were the chosen methodologies, standards and techniques followed?
  - Were appropriate project management techniques used?
  - Is the risk of operating the system within acceptable risk levels?



PROJECT CLOSEOUT

At the end of a project's finite life, the project is closed and the new or modified system is handed over to the users and system support staff.

The steps to be taken in the closeout stage are shown below.

Assign any outstanding issues to individuals responsible for remediation.

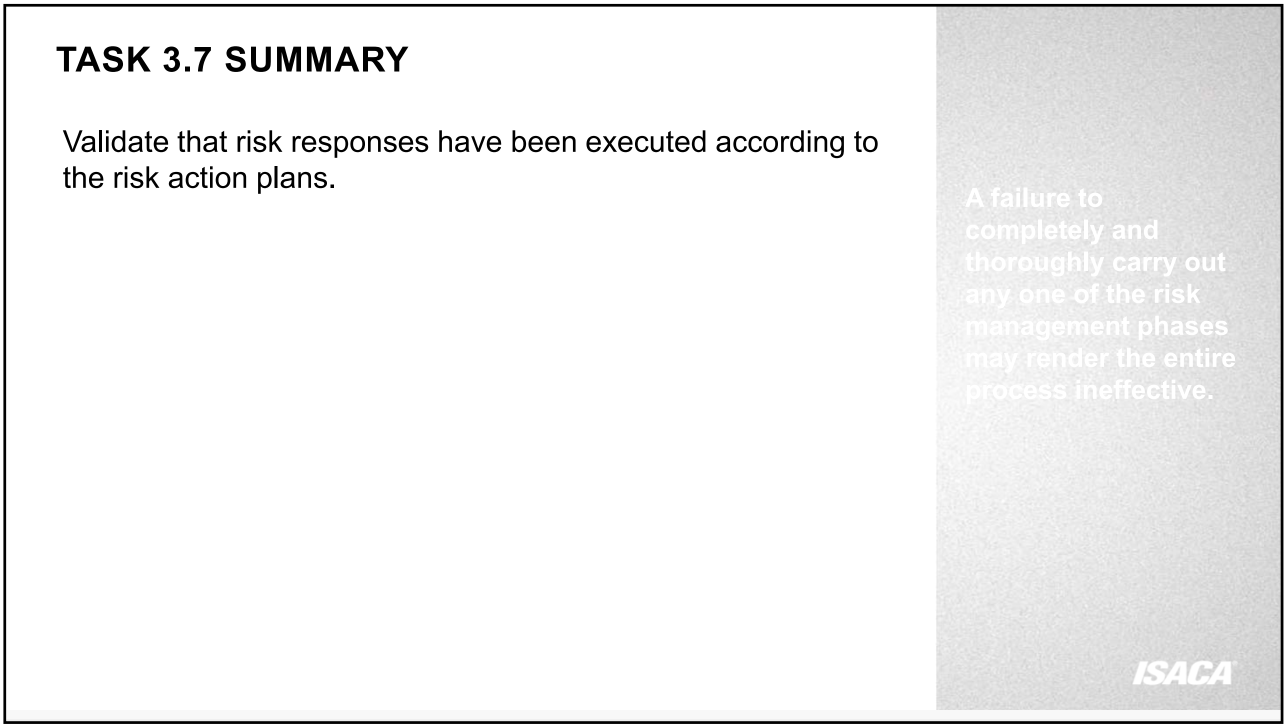
Assign custody of contracts, and archive or pass on documentation to those who will need it.

Survey the project team, development team, users and other stakeholders to identify any lessons learned.

Conduct reviews in a formal process.

Complete a postimplementation review.

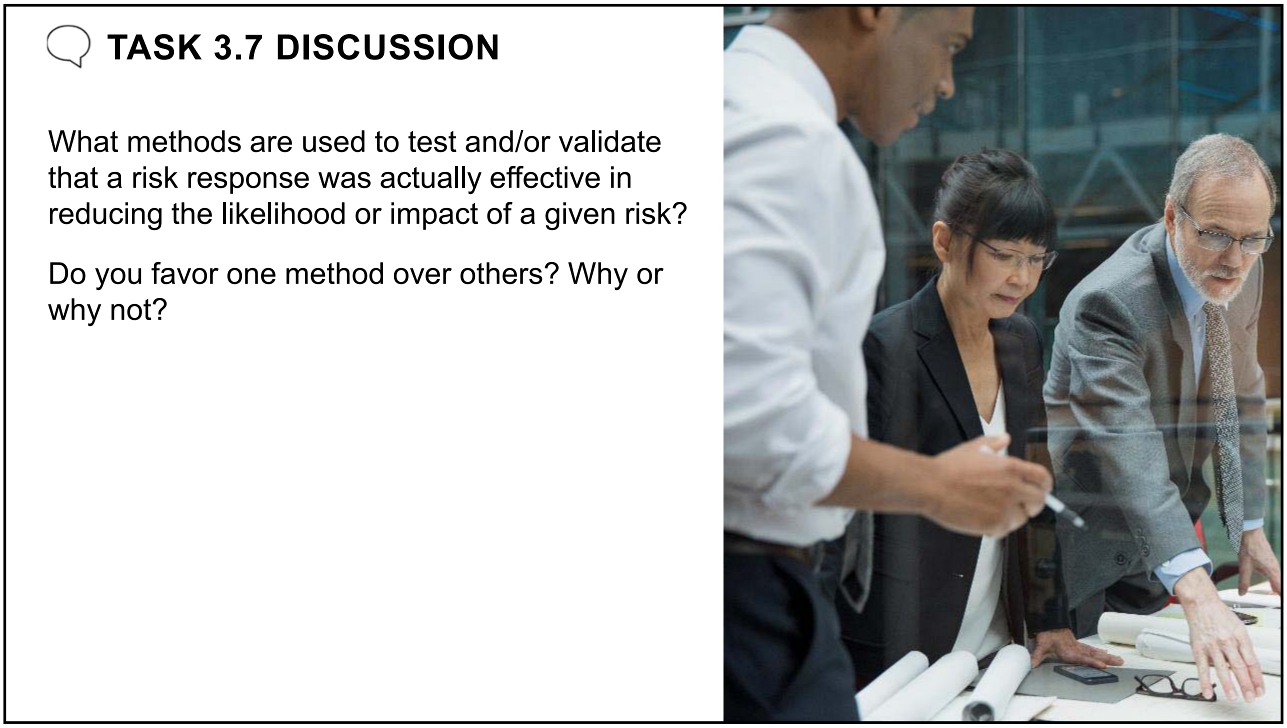
ISACA



TASK 3.7 SUMMARY

Validate that risk responses have been executed according to the risk action plans.

A failure to completely and thoroughly carry out any one of the risk management phases may render the entire process ineffective.



TASK 3.7 DISCUSSION

What methods are used to test and/or validate that a risk response was actually effective in reducing the likelihood or impact of a given risk?

Do you favor one method over others? Why or why not?

DISCUSSION QUESTION

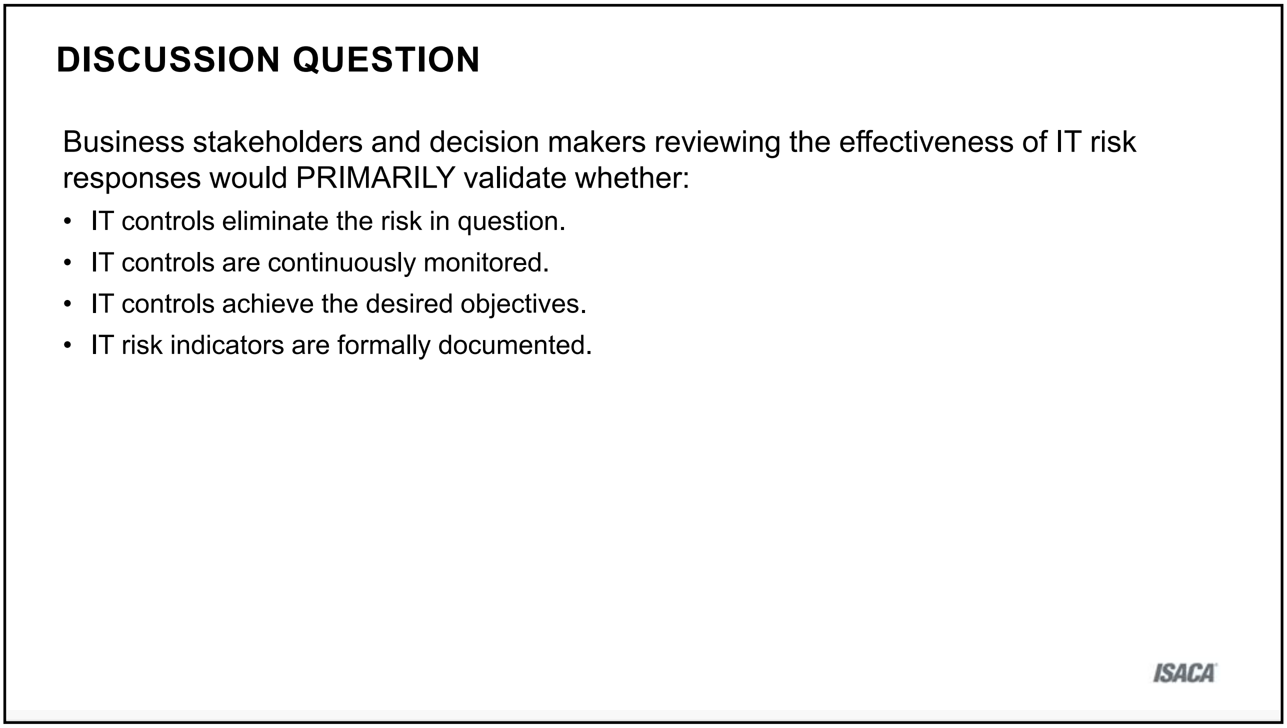
Prior to releasing an operating system security patch into production, a leading practice is to have the patch:

A. applied simultaneously to all systems.

B. procured from an approved vendor.

C. tested in a preproduction test environment.

D. approved by business stakeholders.



DISCUSSION QUESTION

Business stakeholders and decision makers reviewing the effectiveness of IT risk responses would PRIMARILY validate whether:

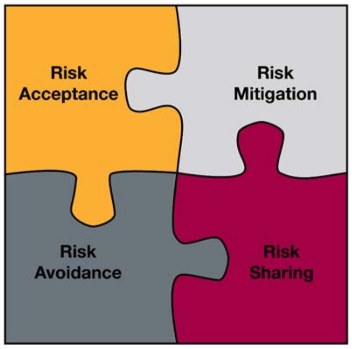
- IT controls eliminate the risk in question.
- IT controls are continuously monitored.
- IT controls achieve the desired objectives.
- IT risk indicators are formally documented.

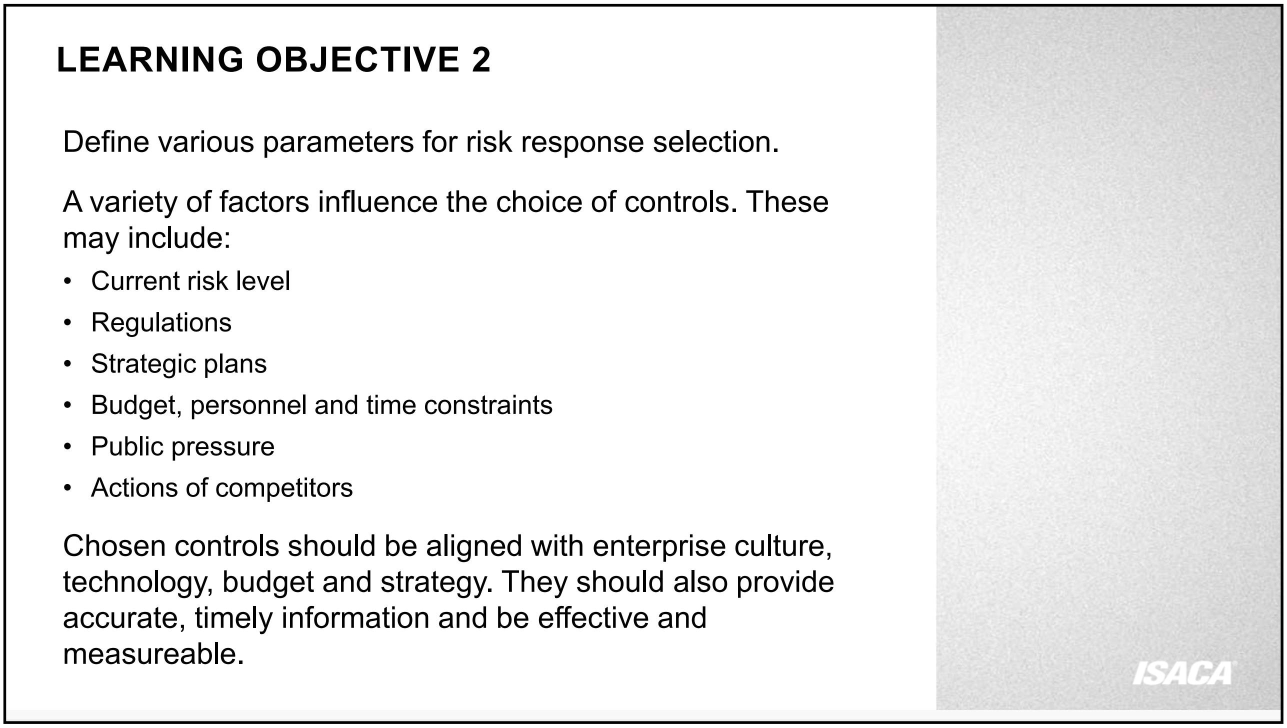
LEARNING OBJECTIVE 1

List the different risk response options.

Risk response options include the following:

- Acceptance
- Mitigation
- Avoidance
- Sharing





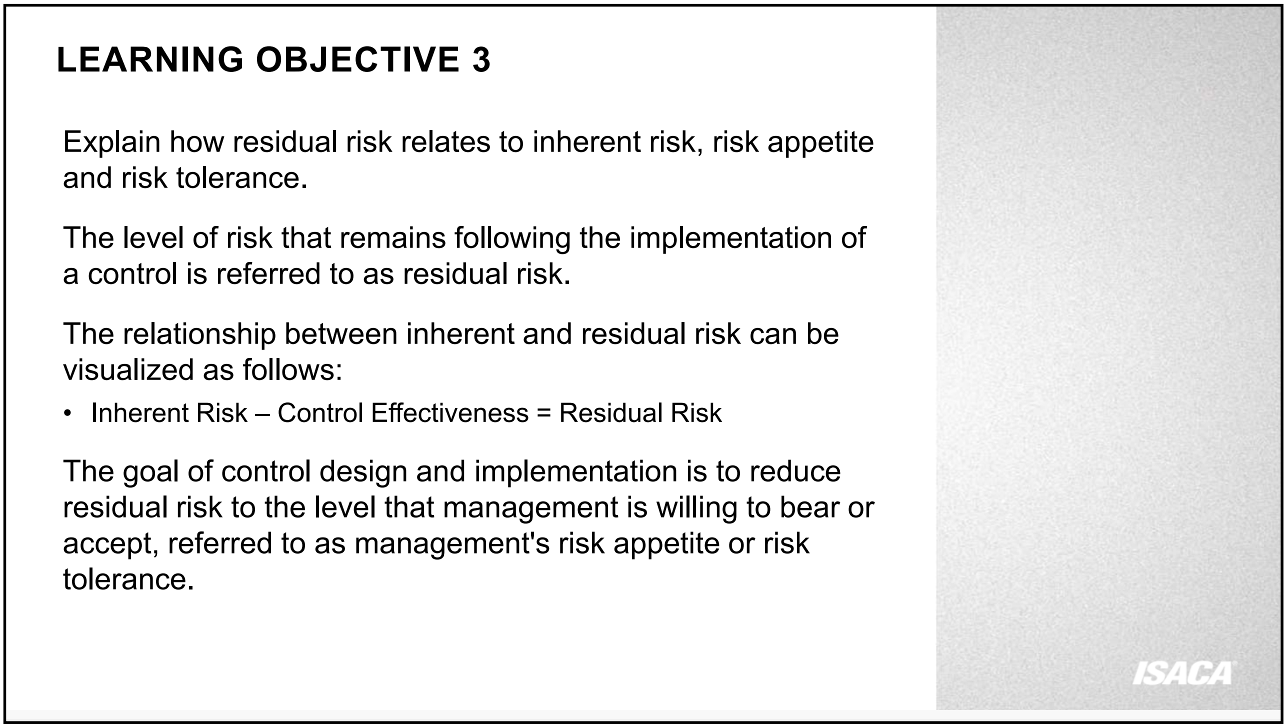
LEARNING OBJECTIVE 2

Define various parameters for risk response selection.

A variety of factors influence the choice of controls. These may include:

- Current risk level
- Regulations
- Strategic plans
- Budget, personnel and time constraints
- Public pressure
- Actions of competitors

Chosen controls should be aligned with enterprise culture, technology, budget and strategy. They should also provide accurate, timely information and be effective and measureable.



LEARNING OBJECTIVE 3

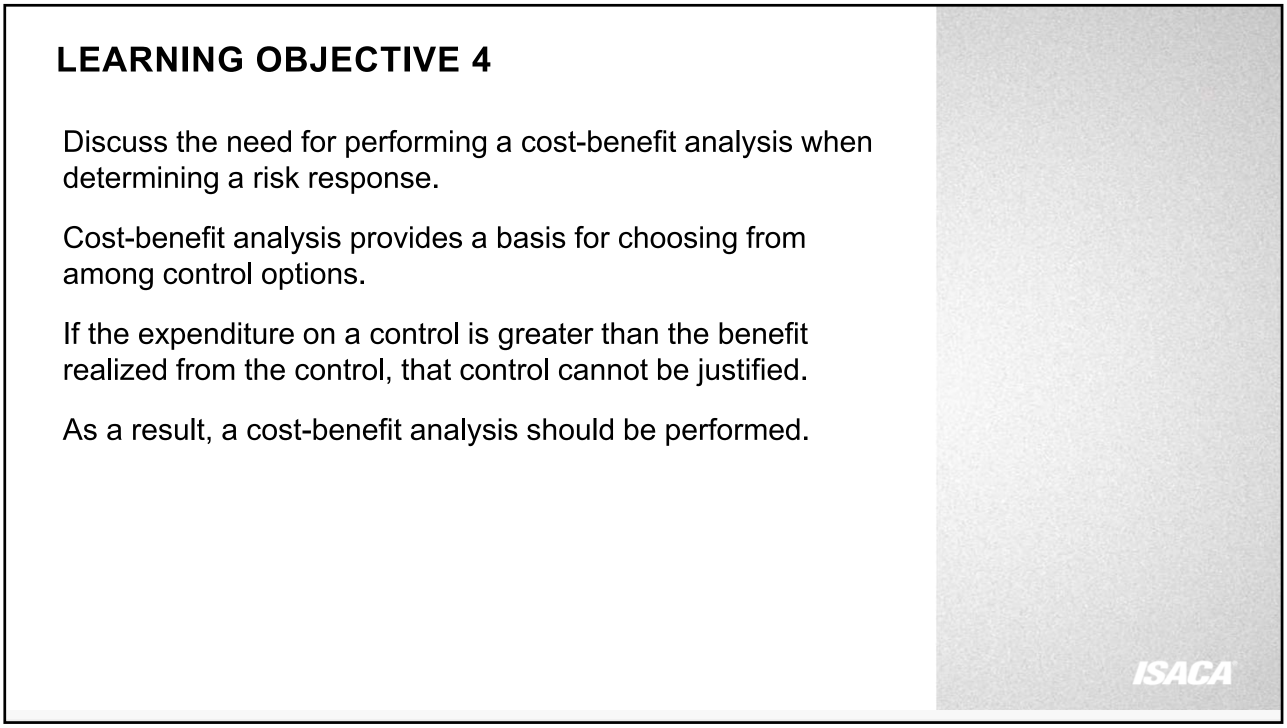
Explain how residual risk relates to inherent risk, risk appetite and risk tolerance.

The level of risk that remains following the implementation of a control is referred to as residual risk.

The relationship between inherent and residual risk can be visualized as follows:

- Inherent Risk – Control Effectiveness = Residual Risk

The goal of control design and implementation is to reduce residual risk to the level that management is willing to bear or accept, referred to as management's risk appetite or risk tolerance.



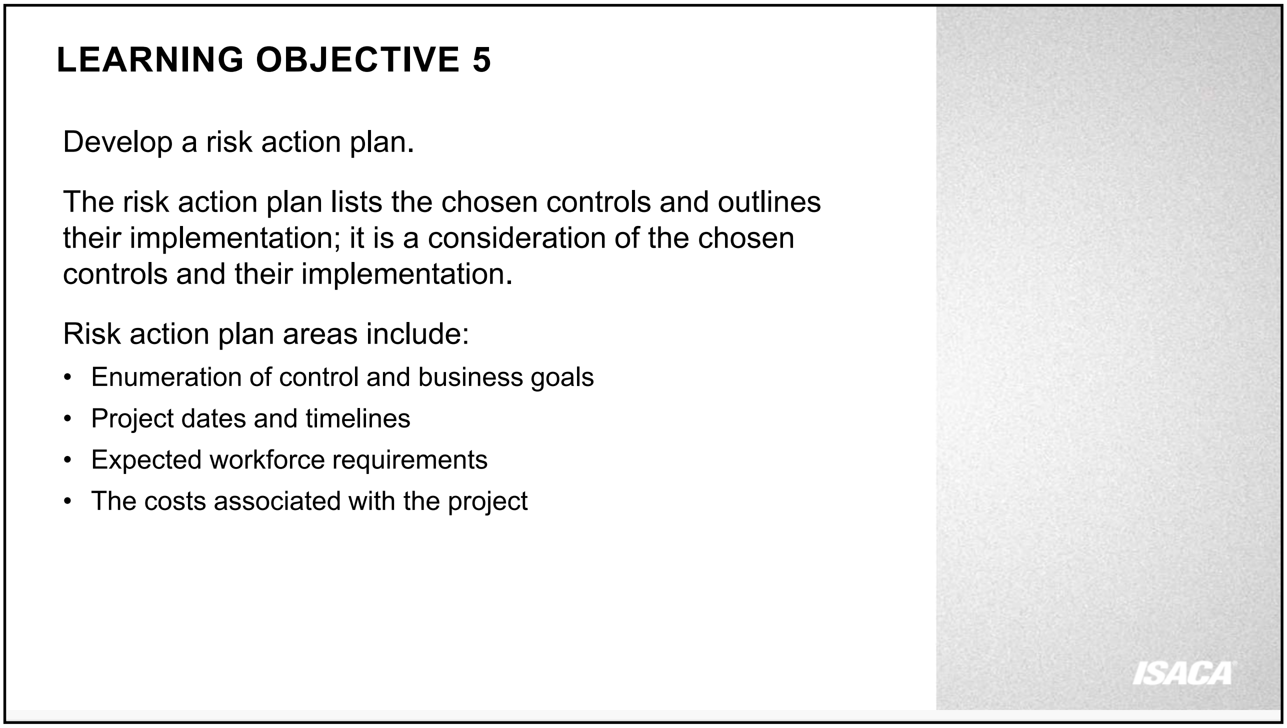
LEARNING OBJECTIVE 4

Discuss the need for performing a cost-benefit analysis when determining a risk response.

Cost-benefit analysis provides a basis for choosing from among control options.

If the expenditure on a control is greater than the benefit realized from the control, that control cannot be justified.

As a result, a cost-benefit analysis should be performed.



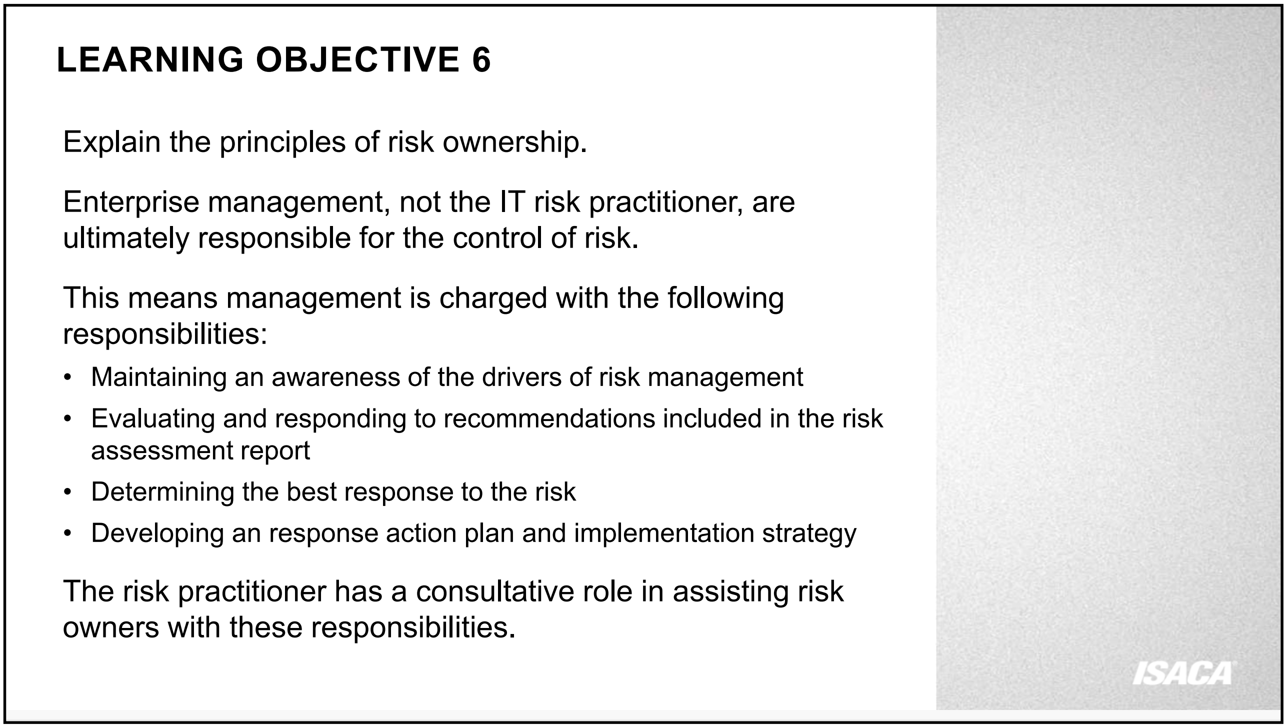
LEARNING OBJECTIVE 5

Develop a risk action plan.

The risk action plan lists the chosen controls and outlines their implementation; it is a consideration of the chosen controls and their implementation.

Risk action plan areas include:

- Enumeration of control and business goals
- Project dates and timelines
- Expected workforce requirements
- The costs associated with the project



LEARNING OBJECTIVE 6

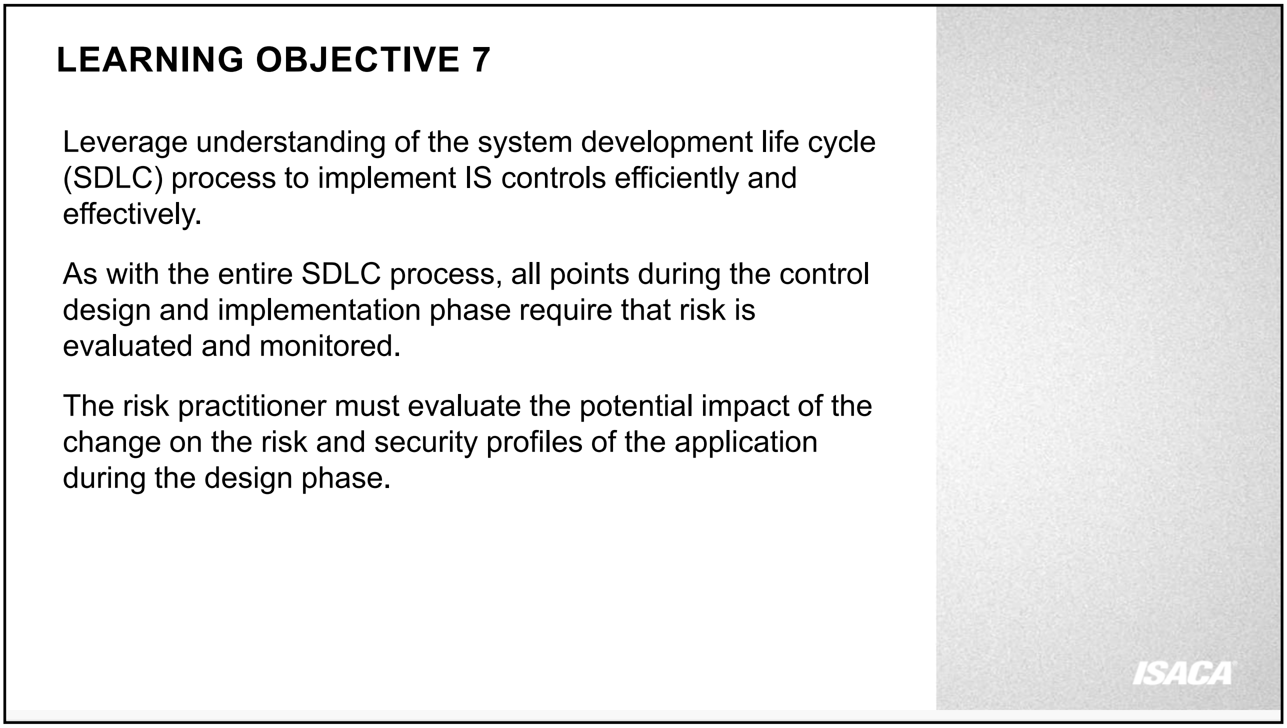
Explain the principles of risk ownership.

Enterprise management, not the IT risk practitioner, are ultimately responsible for the control of risk.

This means management is charged with the following responsibilities:

- Maintaining an awareness of the drivers of risk management
- Evaluating and responding to recommendations included in the risk assessment report
- Determining the best response to the risk
- Developing an response action plan and implementation strategy

The risk practitioner has a consultative role in assisting risk owners with these responsibilities.

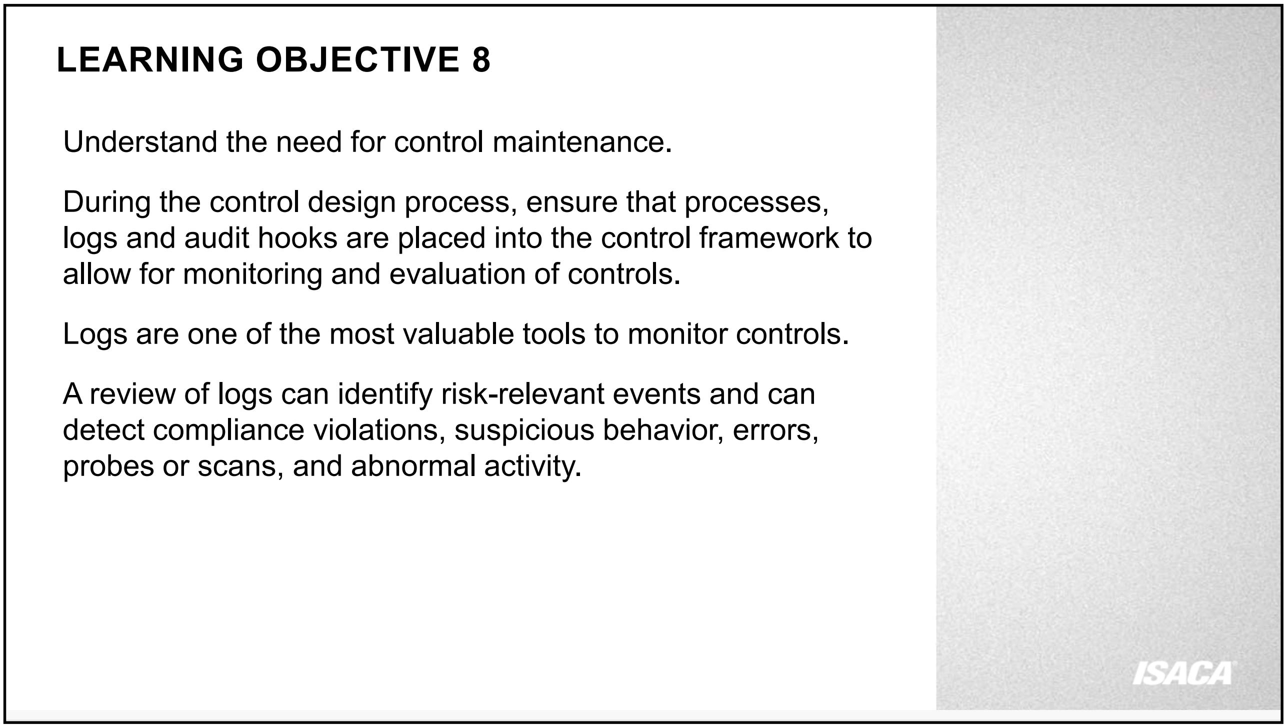


LEARNING OBJECTIVE 7

Leverage understanding of the system development life cycle (SDLC) process to implement IS controls efficiently and effectively.

As with the entire SDLC process, all points during the control design and implementation phase require that risk is evaluated and monitored.

The risk practitioner must evaluate the potential impact of the change on the risk and security profiles of the application during the design phase.



LEARNING OBJECTIVE 8

Understand the need for control maintenance.

During the control design process, ensure that processes, logs and audit hooks are placed into the control framework to allow for monitoring and evaluation of controls.

Logs are one of the most valuable tools to monitor controls.

A review of logs can identify risk-relevant events and can detect compliance violations, suspicious behavior, errors, probes or scans, and abnormal activity.

DISCUSSION QUESTION

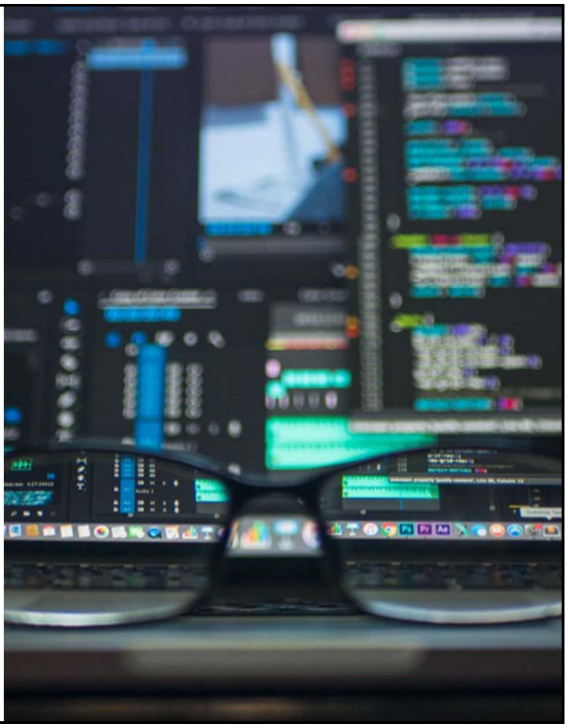
Which of the following provides the formal authorization on user access?

A. Database administrator

B. Data owner

C. Process owner

D. Data custodian



DISCUSSION QUESTION

In the risk management process, a cost-benefit analysis is MAINLY performed:

A. as part of an initial risk assessment.

B. as part of risk response planning.

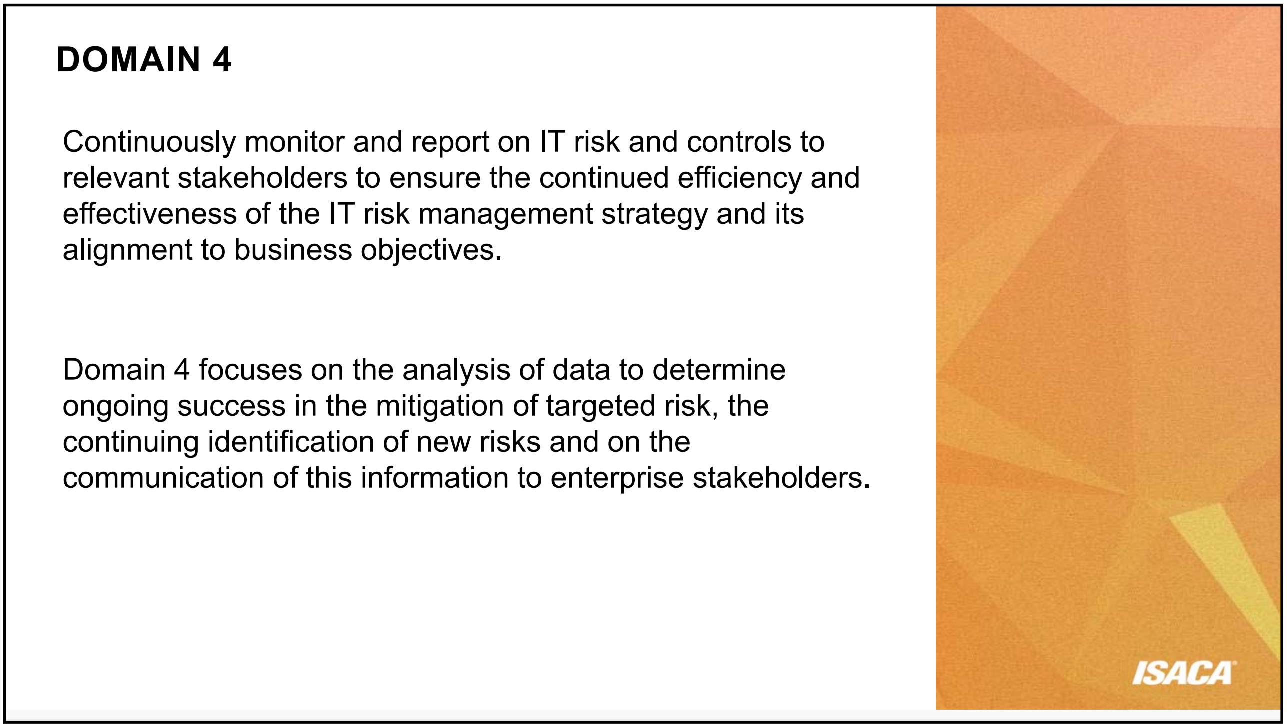
C. during an information asset valuation.

D. when insurance is calculated for risk transfer.

ISACA

DOMAIN 4

RISK AND CONTROL MONITORING AND REPORTING



DOMAIN 4

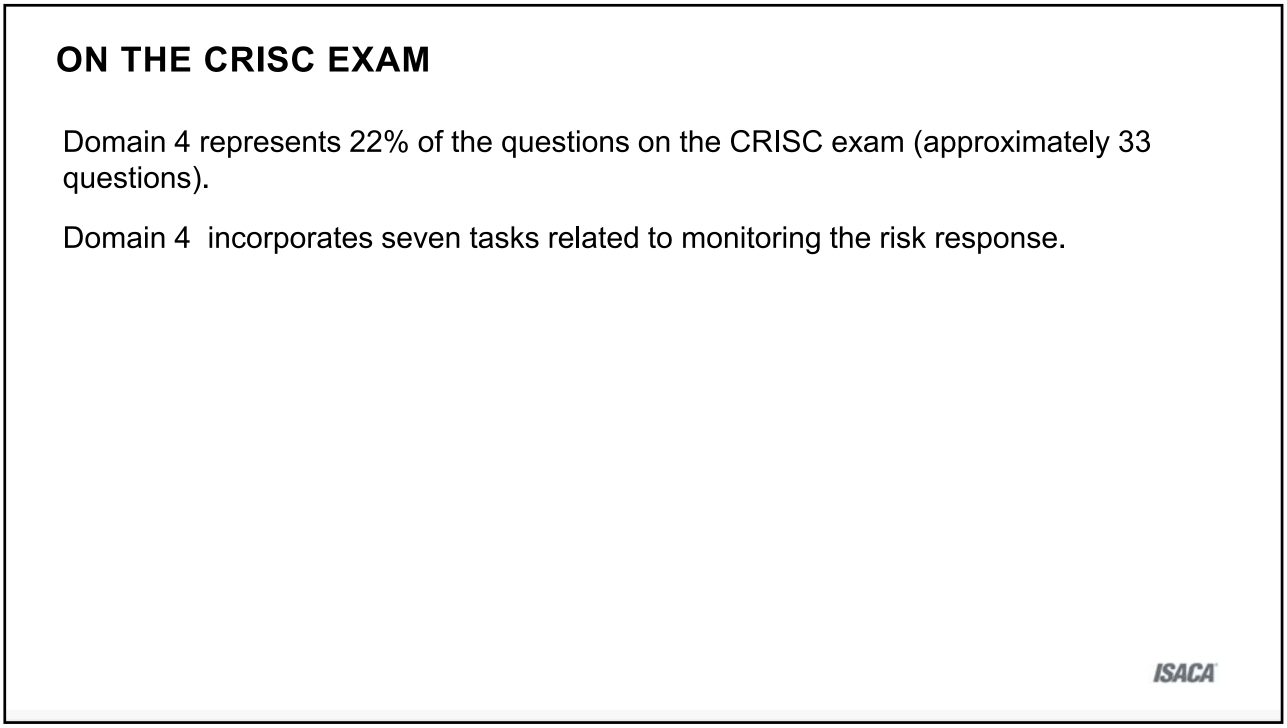
Continuously monitor and report on IT risk and controls to relevant stakeholders to ensure the continued efficiency and effectiveness of the IT risk management strategy and its alignment to business objectives.

Domain 4 focuses on the analysis of data to determine ongoing success in the mitigation of targeted risk, the continuing identification of new risks and on the communication of this information to enterprise stakeholders.

LEARNING OBJECTIVES

The objective of this domain is to ensure that the CRISC candidate has the knowledge necessary to:

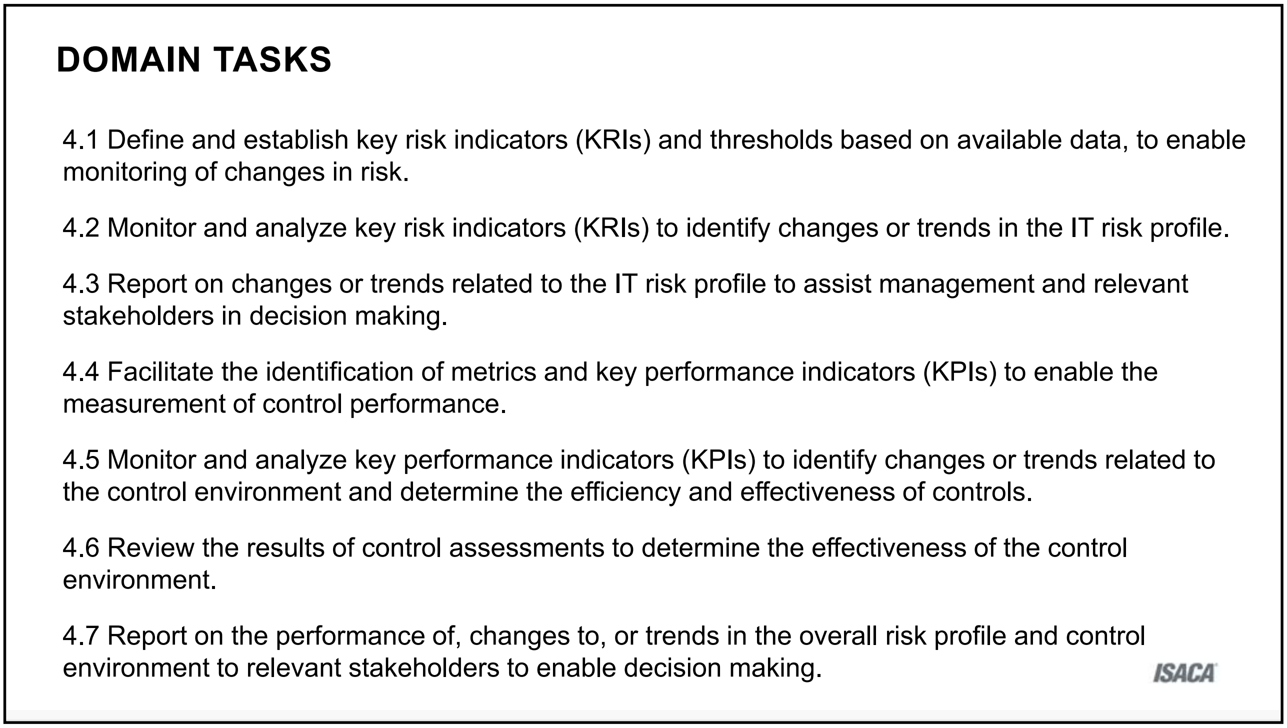
1. Differentiate between key risk indicators (KRIs) and key performance indicators (KPIs).
2. Describe data extraction, aggregation and analysis tools and techniques.
3. Compare different monitoring tools and techniques.
4. Describe various testing and assessment tools and techniques.



ON THE CRISC EXAM

Domain 4 represents 22% of the questions on the CRISC exam (approximately 33 questions).

Domain 4 incorporates seven tasks related to monitoring the risk response.



DOMAIN TASKS

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.

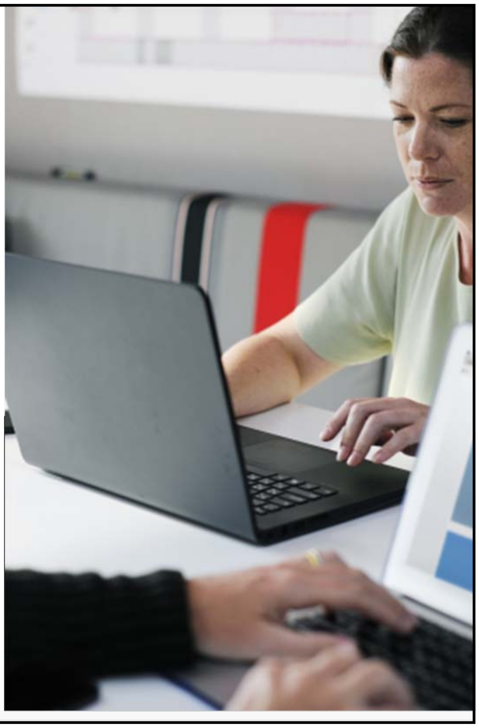
4.5 Monitor and analyze key performance indicators (KPIs) to identify changes or trends related to the control environment and determine the efficiency and effectiveness of controls.

4.6 Review the results of control assessments to determine the effectiveness of the control environment.

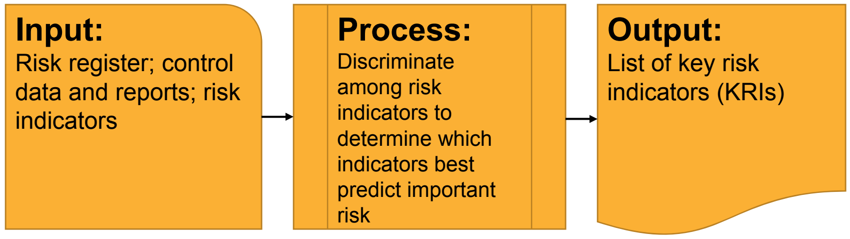
4.7 Report on the performance of, changes to, or trends in the overall risk profile and control environment to relevant stakeholders to enable decision making.

TASK 4.1

Define and establish key risk indicators (KRIs) and thresholds based on available data, to enable monitoring of changes in risk.



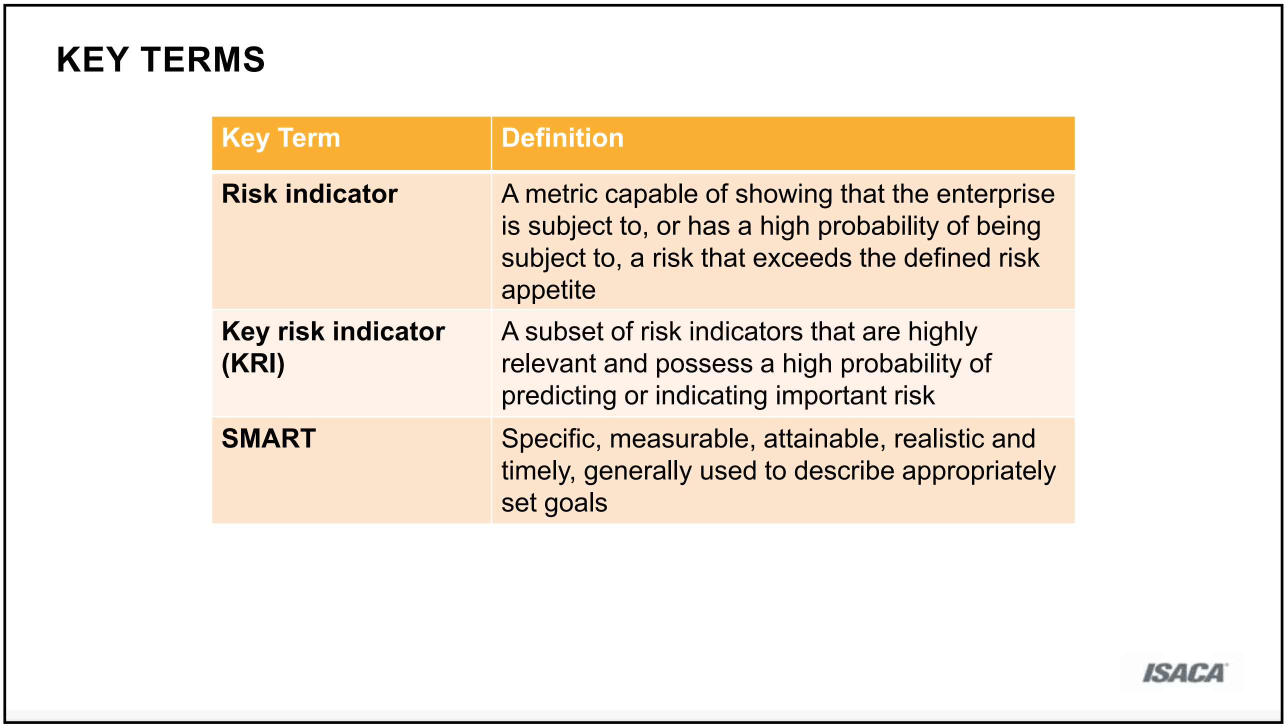
FOCUS ON TASK 4.1



Input:
Risk register; control data and reports; risk indicators

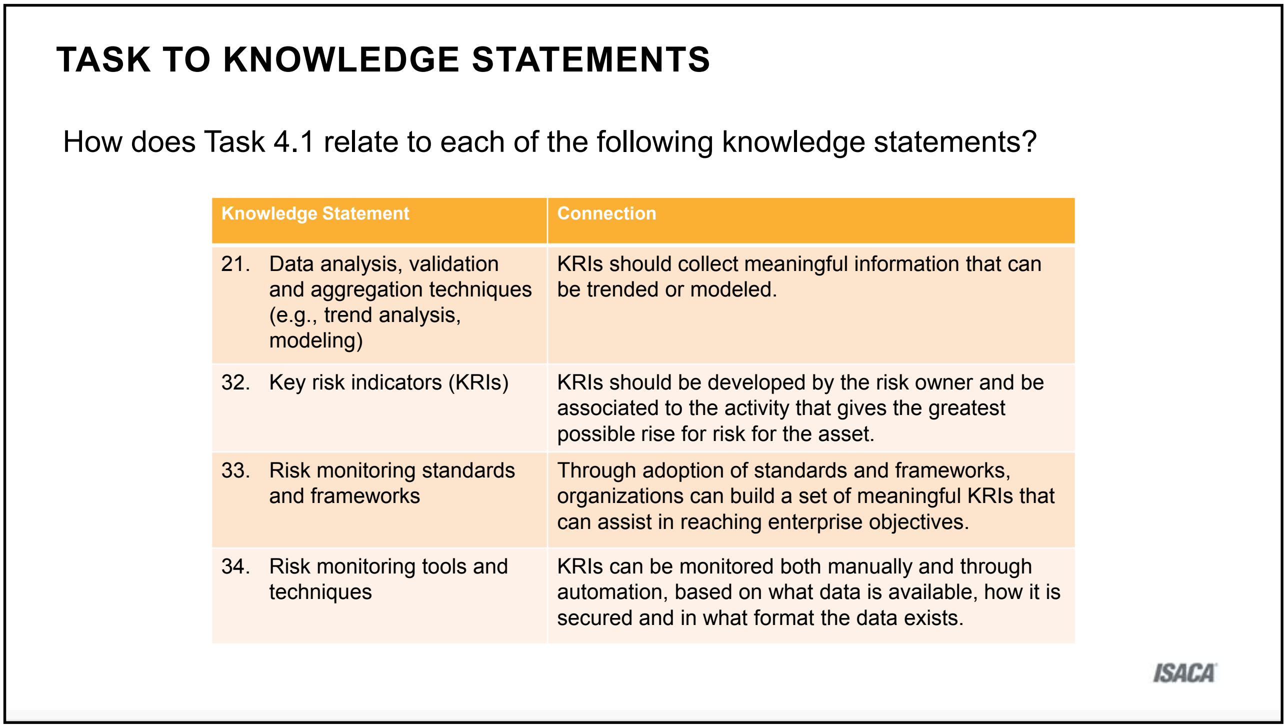
Process:
Discriminate among risk indicators to determine which indicators best predict important risk

Output:
List of key risk indicators (KRIs)



KEY TERMS

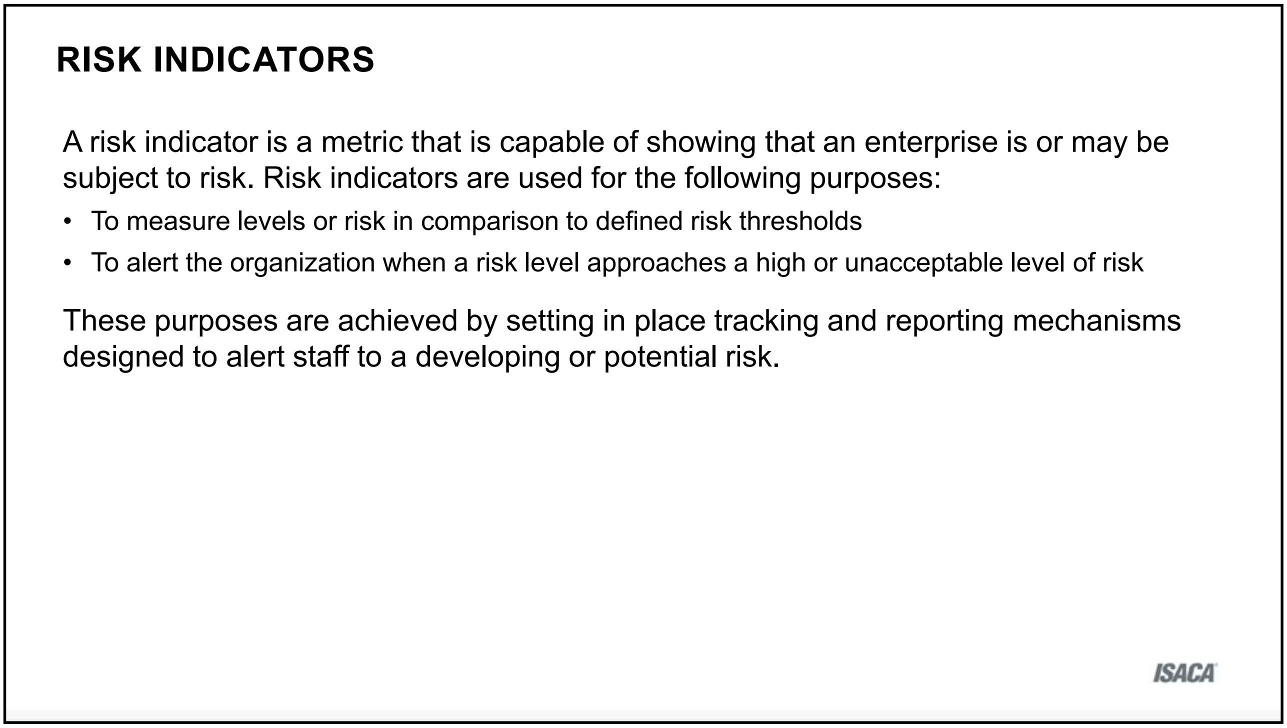
Key Term	Definition
Risk indicator	A metric capable of showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk appetite
Key risk indicator (KRI)	A subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk
SMART	Specific, measurable, attainable, realistic and timely, generally used to describe appropriately set goals



TASK TO KNOWLEDGE STATEMENTS

How does Task 4.1 relate to each of the following knowledge statements?

Knowledge Statement	Connection
21. Data analysis, validation and aggregation techniques (e.g., trend analysis, modeling)	KRIs should collect meaningful information that can be trended or modeled.
32. Key risk indicators (KRIs)	KRIs should be developed by the risk owner and be associated to the activity that gives the greatest possible rise for risk for the asset.
33. Risk monitoring standards and frameworks	Through adoption of standards and frameworks, organizations can build a set of meaningful KRIs that can assist in reaching enterprise objectives.
34. Risk monitoring tools and techniques	KRIs can be monitored both manually and through automation, based on what data is available, how it is secured and in what format the data exists.

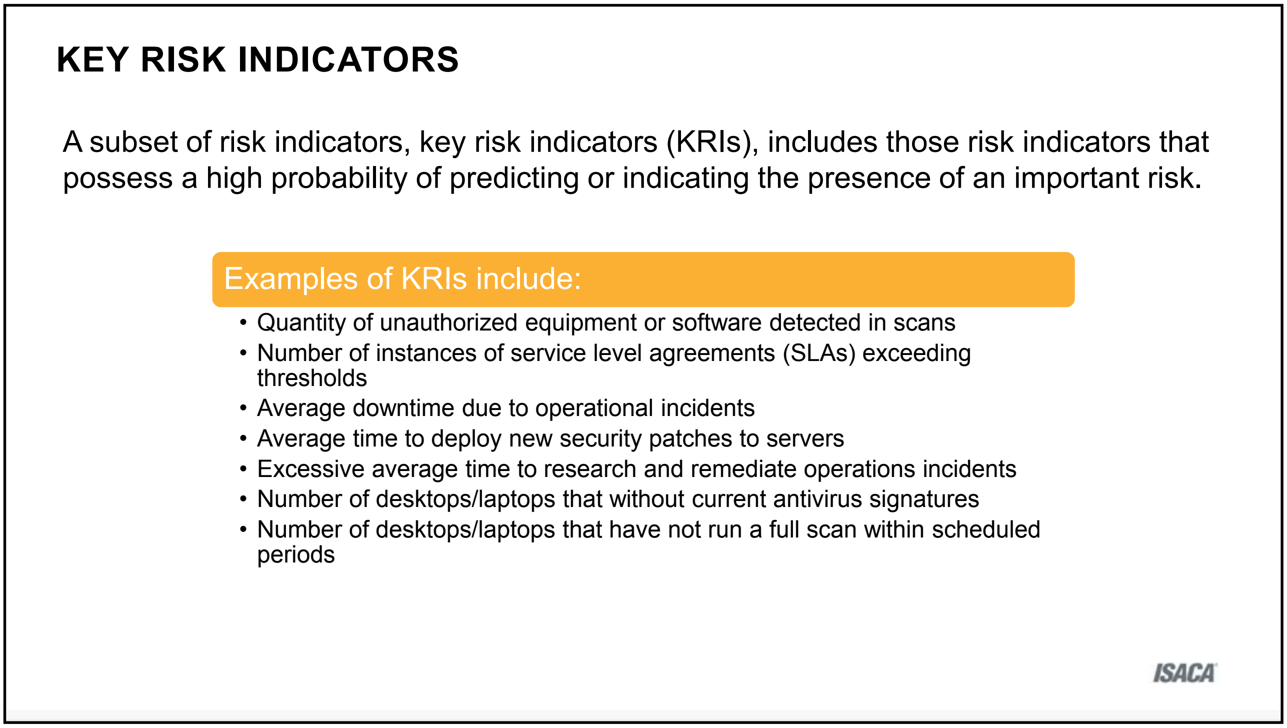


RISK INDICATORS

A risk indicator is a metric that is capable of showing that an enterprise is or may be subject to risk. Risk indicators are used for the following purposes:

- To measure levels or risk in comparison to defined risk thresholds
- To alert the organization when a risk level approaches a high or unacceptable level of risk

These purposes are achieved by setting in place tracking and reporting mechanisms designed to alert staff to a developing or potential risk.

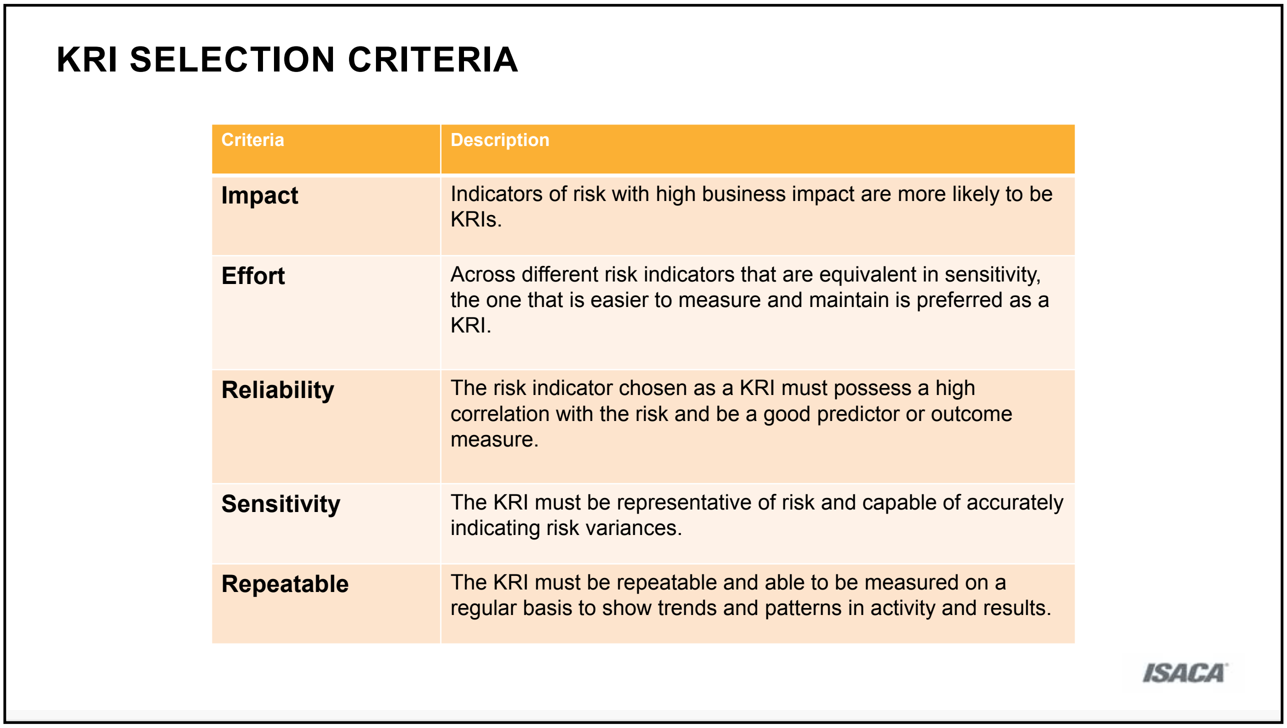


KEY RISK INDICATORS

A subset of risk indicators, key risk indicators (KRIs), includes those risk indicators that possess a high probability of predicting or indicating the presence of an important risk.

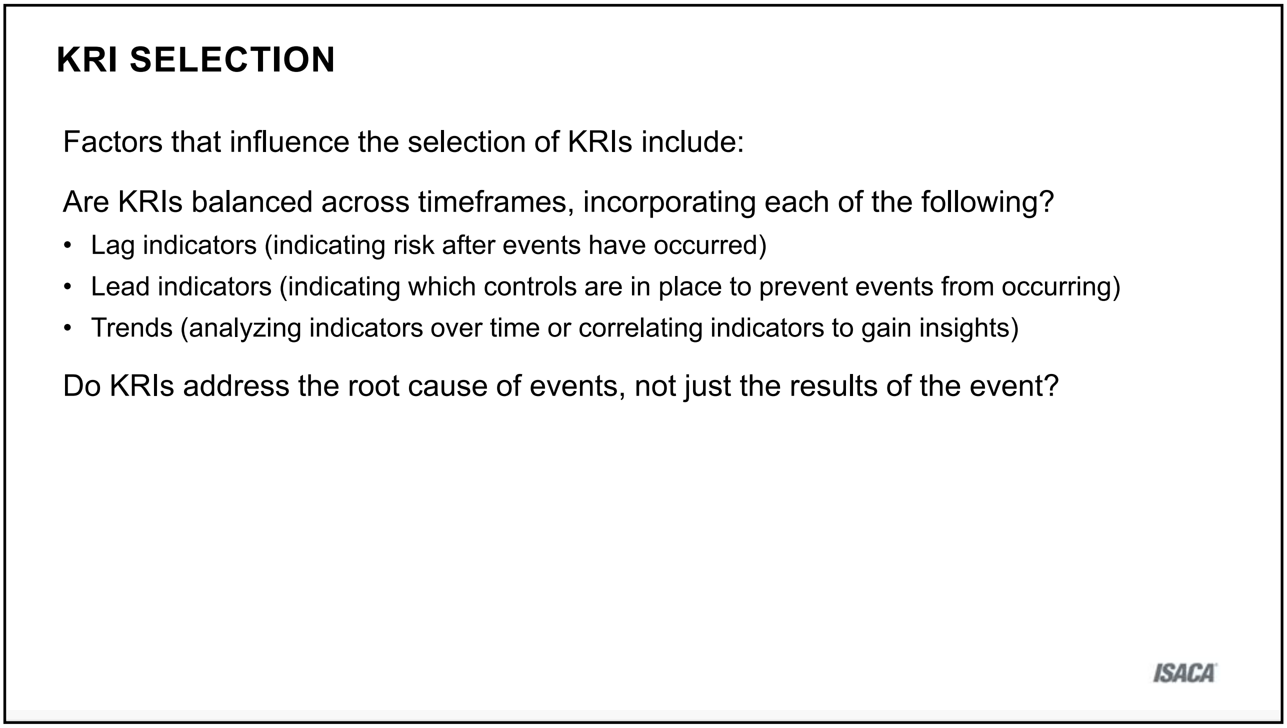
Examples of KRIs include:

- Quantity of unauthorized equipment or software detected in scans
- Number of instances of service level agreements (SLAs) exceeding thresholds
- 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 without current antivirus signatures
- Number of desktops/laptops that have not run a full scan within scheduled periods



KRI SELECTION CRITERIA

Criteria	Description
Impact	Indicators of risk with high business impact are more likely to be KRIs.
Effort	Across different risk indicators that are equivalent in sensitivity, the one that is easier to measure and maintain is preferred as a KRI.
Reliability	The risk indicator chosen as a KRI must possess a high correlation with the risk and be a good predictor or outcome measure.
Sensitivity	The KRI must be representative of risk and capable of accurately indicating risk variances.
Repeatable	The KRI must be repeatable and able to be measured on a regular basis to show trends and patterns in activity and results.



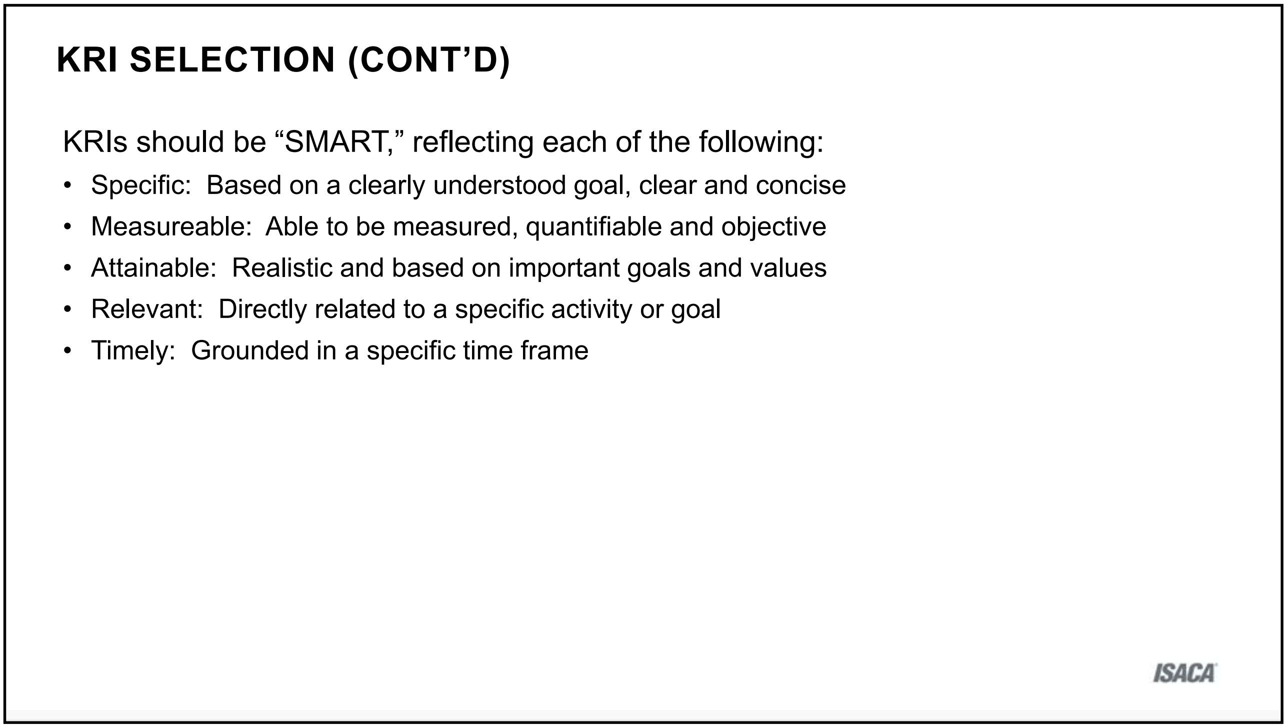
KRI SELECTION

Factors that influence the selection of KRIs include:

Are KRIs balanced across timeframes, incorporating each of the following?

- Lag indicators (indicating risk after events have occurred)
- Lead indicators (indicating which controls are in place to prevent events from occurring)
- Trends (analyzing indicators over time or correlating indicators to gain insights)

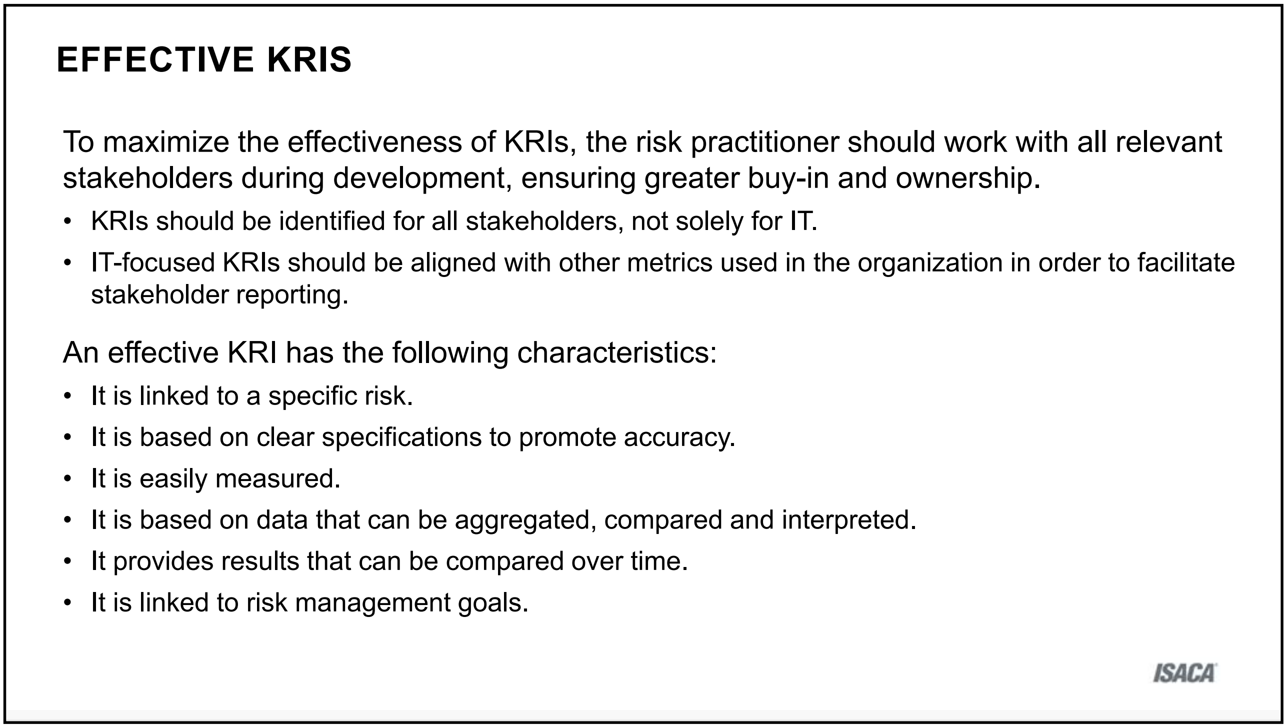
Do KRIs address the root cause of events, not just the results of the event?



KRI SELECTION (CONT'D)

KRIs should be "SMART," reflecting each of the following:

- Specific: Based on a clearly understood goal, clear and concise
- Measureable: Able to be measured, quantifiable and objective
- Attainable: Realistic and based on important goals and values
- Relevant: Directly related to a specific activity or goal
- Timely: Grounded in a specific time frame



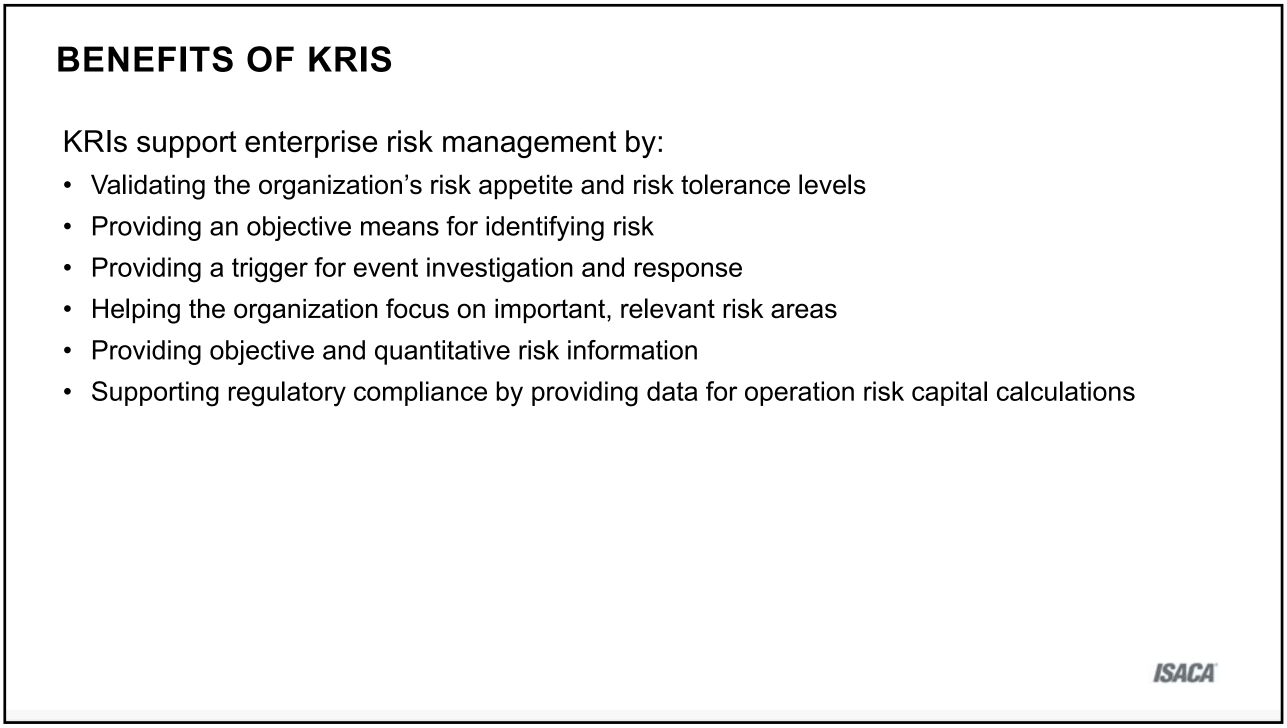
EFFECTIVE KRIS

To maximize the effectiveness of KRIs, the risk practitioner should work with all relevant stakeholders during development, ensuring greater buy-in and ownership.

- KRIs should be identified for all stakeholders, not solely for IT.
- IT-focused KRIs should be aligned with other metrics used in the organization in order to facilitate stakeholder reporting.

An effective KRI has the following characteristics:

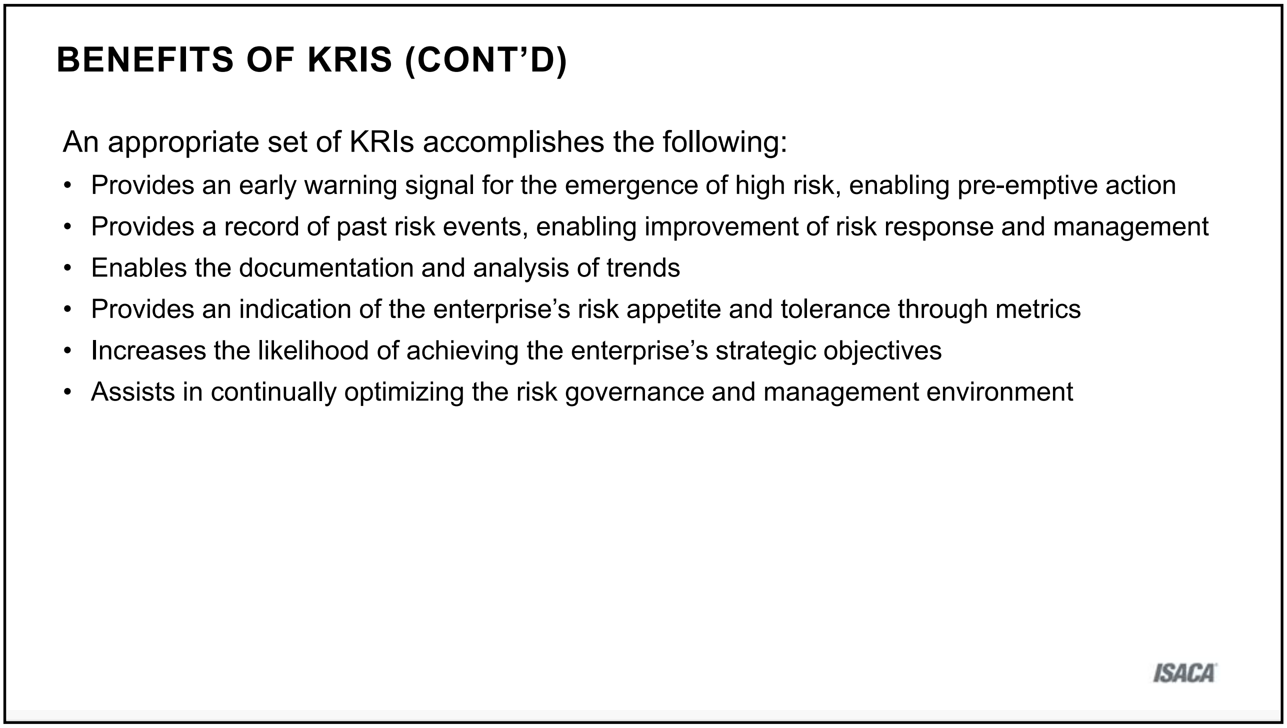
- It is linked to a specific risk.
- It is based on clear specifications to promote accuracy.
- It is easily measured.
- It is based on data that can be aggregated, compared and interpreted.
- It provides results that can be compared over time.
- It is linked to risk management goals.



BENEFITS OF KRIS

KRIs support enterprise risk management by:

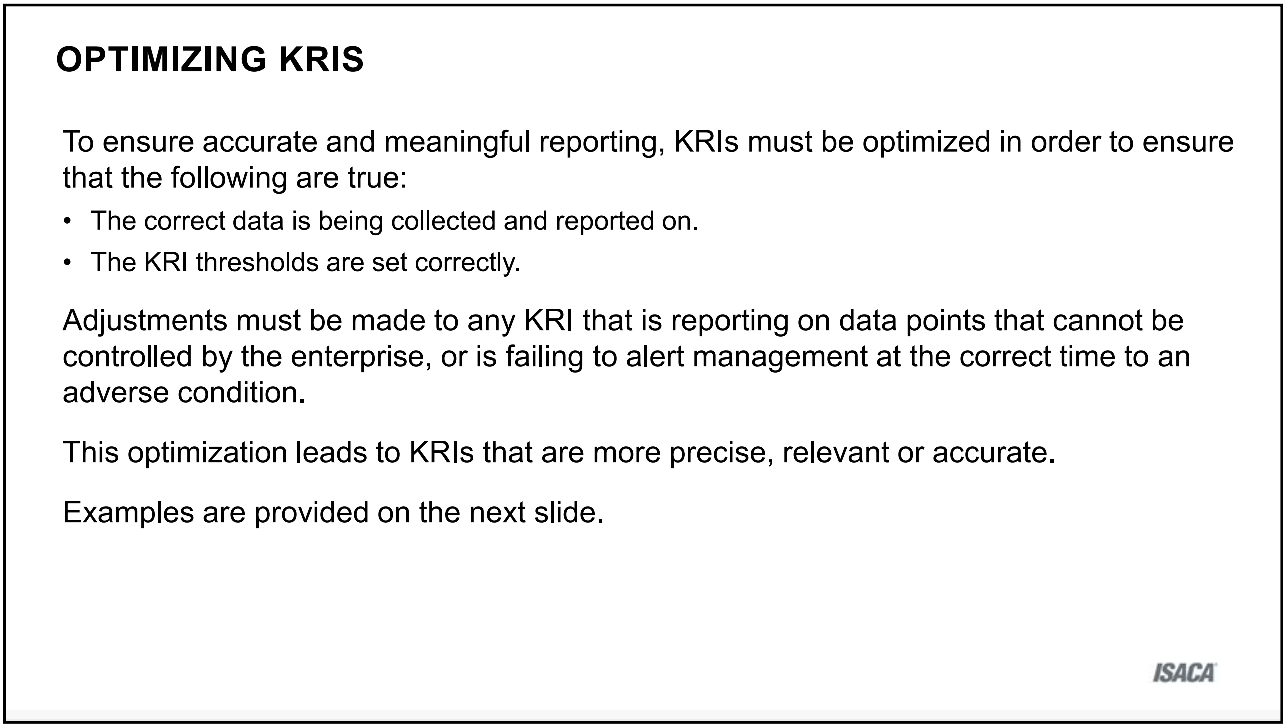
- Validating the organization’s risk appetite and risk tolerance levels
- Providing an objective means for identifying risk
- Providing a trigger for event investigation and response
- Helping the organization focus on important, relevant risk areas
- Providing objective and quantitative risk information
- Supporting regulatory compliance by providing data for operation risk capital calculations



BENEFITS OF KRIS (CONT'D)

An appropriate set of KRIs accomplishes the following:

- Provides an early warning signal for the emergence of high risk, enabling pre-emptive action
- Provides a record of past risk events, enabling improvement of risk response and management
- Enables the documentation and analysis of trends
- Provides an indication of the enterprise's risk appetite and tolerance through metrics
- Increases the likelihood of achieving the enterprise's strategic objectives
- Assists in continually optimizing the risk governance and management environment



OPTIMIZING KRIS

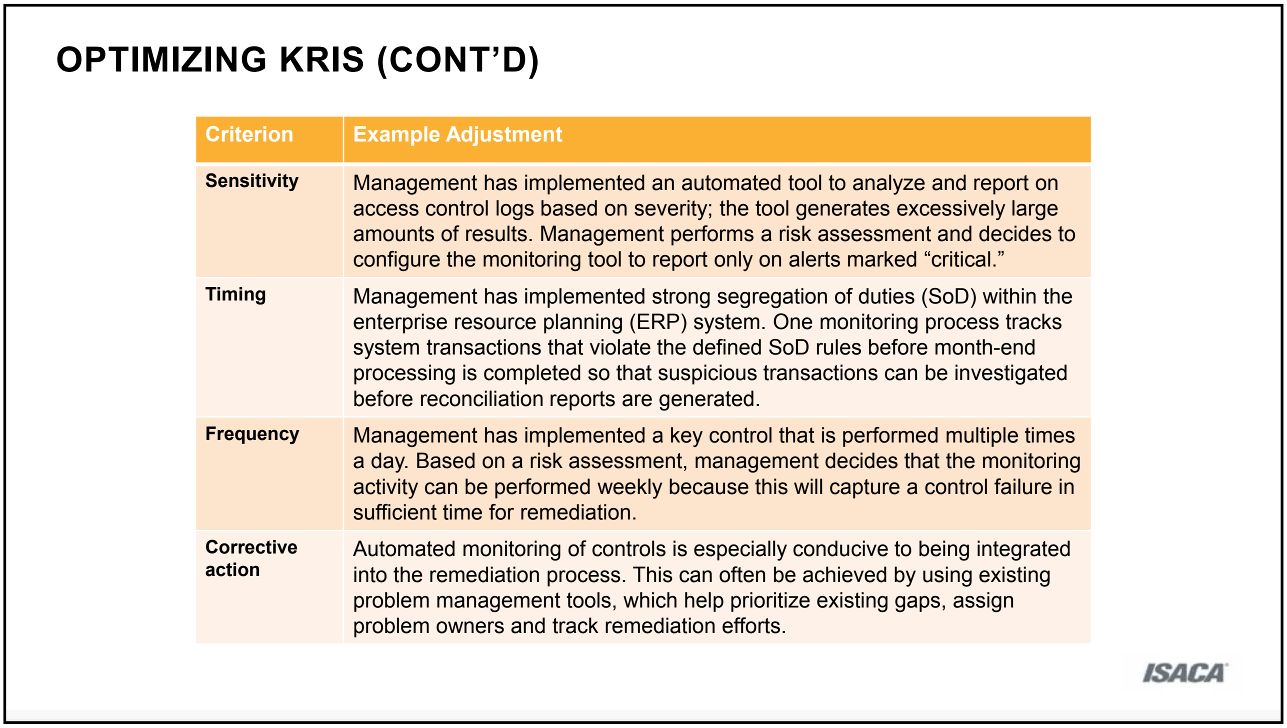
To ensure accurate and meaningful reporting, KRIs must be optimized in order to ensure that the following are true:

- The correct data is being collected and reported on.
- The KRI thresholds are set correctly.

Adjustments must be made to any KRI that is reporting on data points that cannot be controlled by the enterprise, or is failing to alert management at the correct time to an adverse condition.

This optimization leads to KRIs that are more precise, relevant or accurate.

Examples are provided on the next slide.



OPTIMIZING KRIS (CONT'D)

Criterion	Example Adjustment
Sensitivity	Management has implemented an automated tool to analyze and report on access control logs based on severity; the tool generates excessively large amounts of results. Management performs a risk assessment and decides to configure the monitoring tool to report only on alerts marked "critical."
Timing	Management has implemented strong segregation of duties (SoD) within the enterprise resource planning (ERP) system. One monitoring process tracks system transactions that violate the defined SoD rules before month-end processing is completed so that suspicious transactions can be investigated before reconciliation reports are generated.
Frequency	Management has implemented a key control that is performed multiple times a day. Based on a risk assessment, management decides that the monitoring activity can be performed weekly because this will capture a control failure in sufficient time for remediation.
Corrective action	Automated monitoring of controls is especially conducive to being integrated into the remediation process. This can often be achieved by using existing problem management tools, which help prioritize existing gaps, assign problem owners and track remediation efforts.

ISACA

TASK 4.1 SUMMARY

Define and establish key risk indicators (KRIs) and thresholds based on available data, to enable monitoring of changes in risk.

Risk governance ensures that risk management controls are implemented and operating correctly.

TASK 4.1 ACTIVITY

Using the risk scenario you have built throughout this course, complete Part V of the risk register.

Part V—Risk Indicators	
Key risk indicators for this risk	1. 2. 3. 4.

DISCUSSION QUESTION

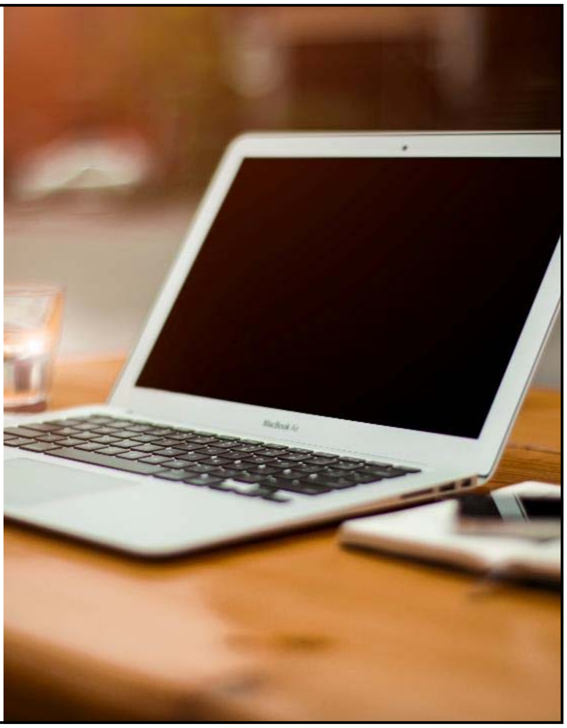
Reliability of a key risk indicator (KRI) would indicate that the metric:

A. performs within the appropriate thresholds.

B. tests the target at predetermined intervals.

C. flags exceptions every time they occur.

D. initiates corrective action.



DISCUSSION QUESTION

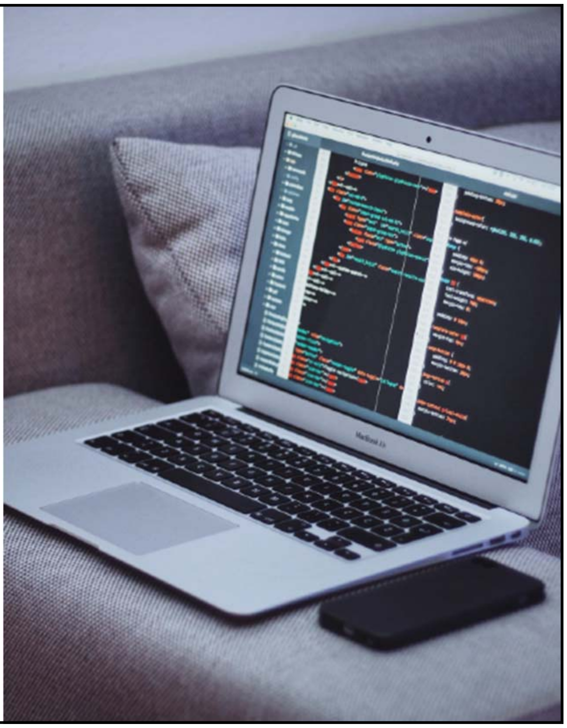
Which of the following is MOST critical when system configuration files for a critical enterprise application system are being reviewed?

A. Configuration files are frequently changed.

B. Changes to configuration files are recorded.

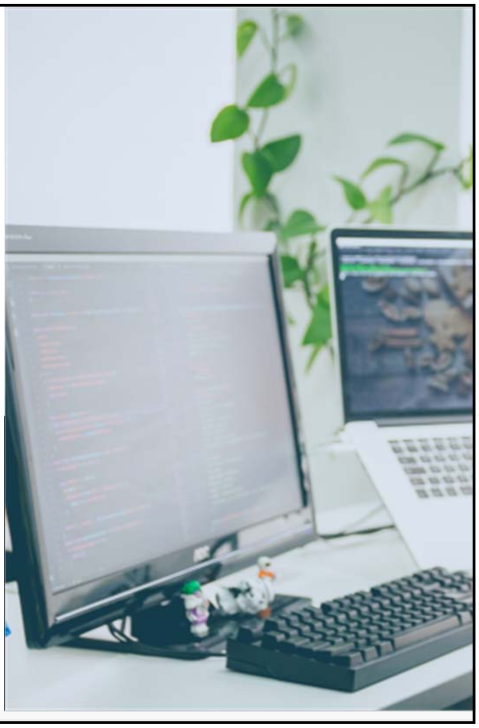
C. Access to configuration files is not restricted.

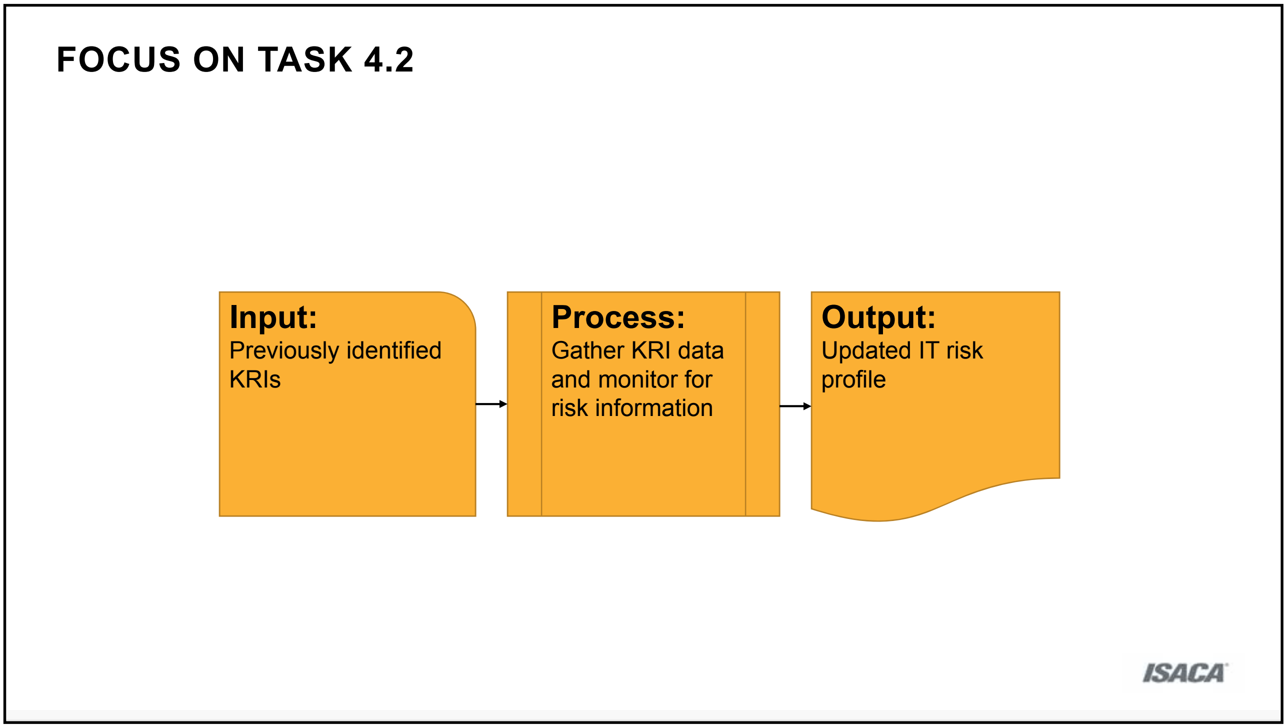
D. Configuration values do not impact system efficiency.



TASK 4.2

Monitor and analyze key risk indicators (KRIs) to identify changes or trends in the IT risk profile.





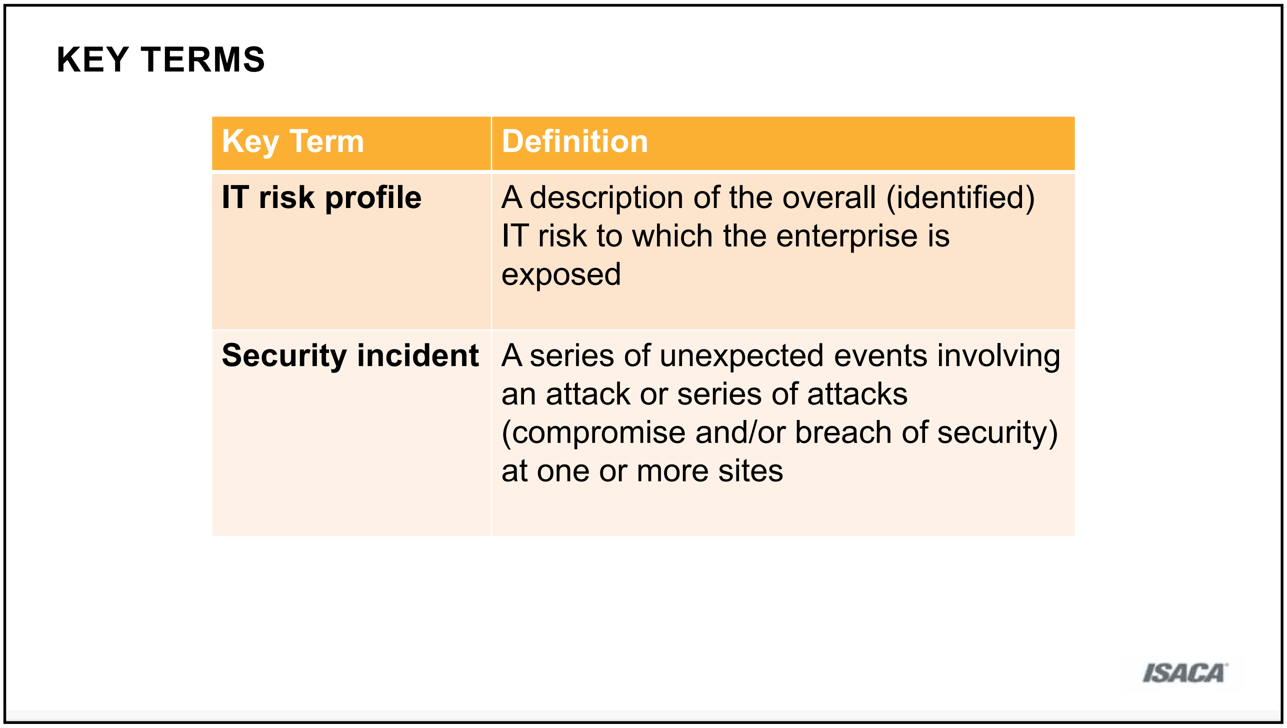
FOCUS ON TASK 4.2

Input:
Previously identified KRIs

Process:
Gather KRI data and monitor for risk information

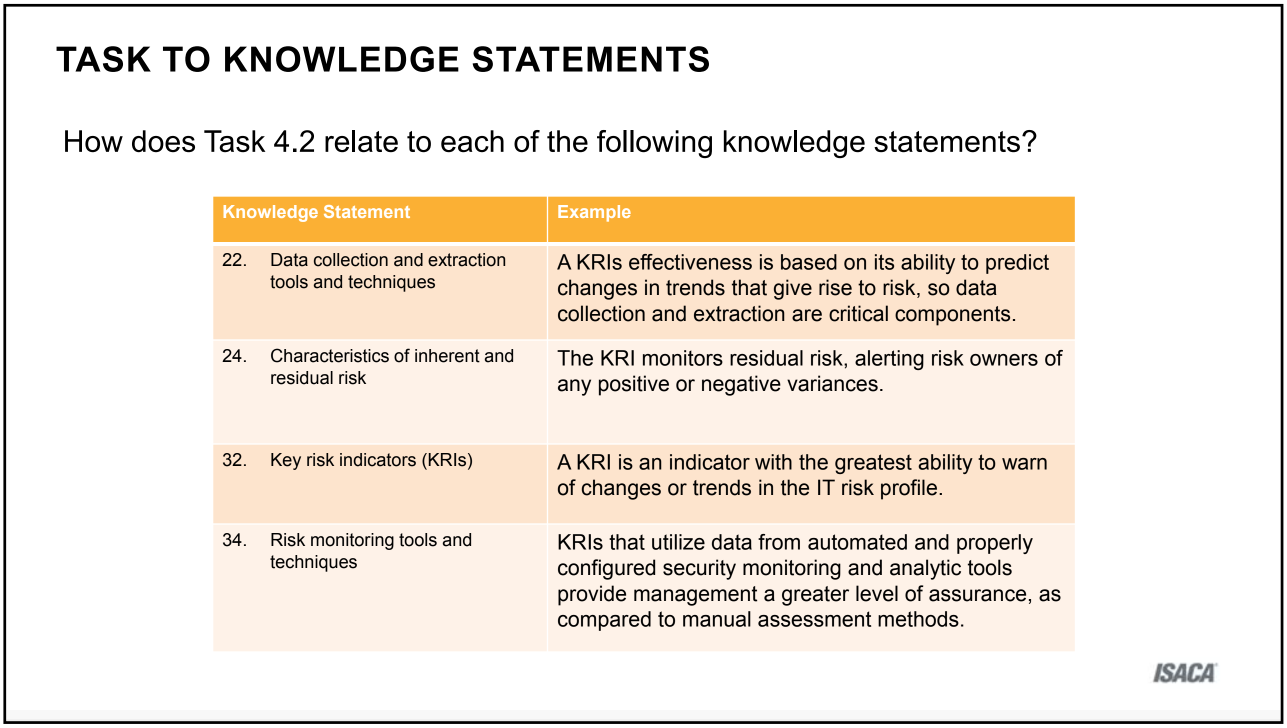
Output:
Updated IT risk profile

ISACA



KEY TERMS

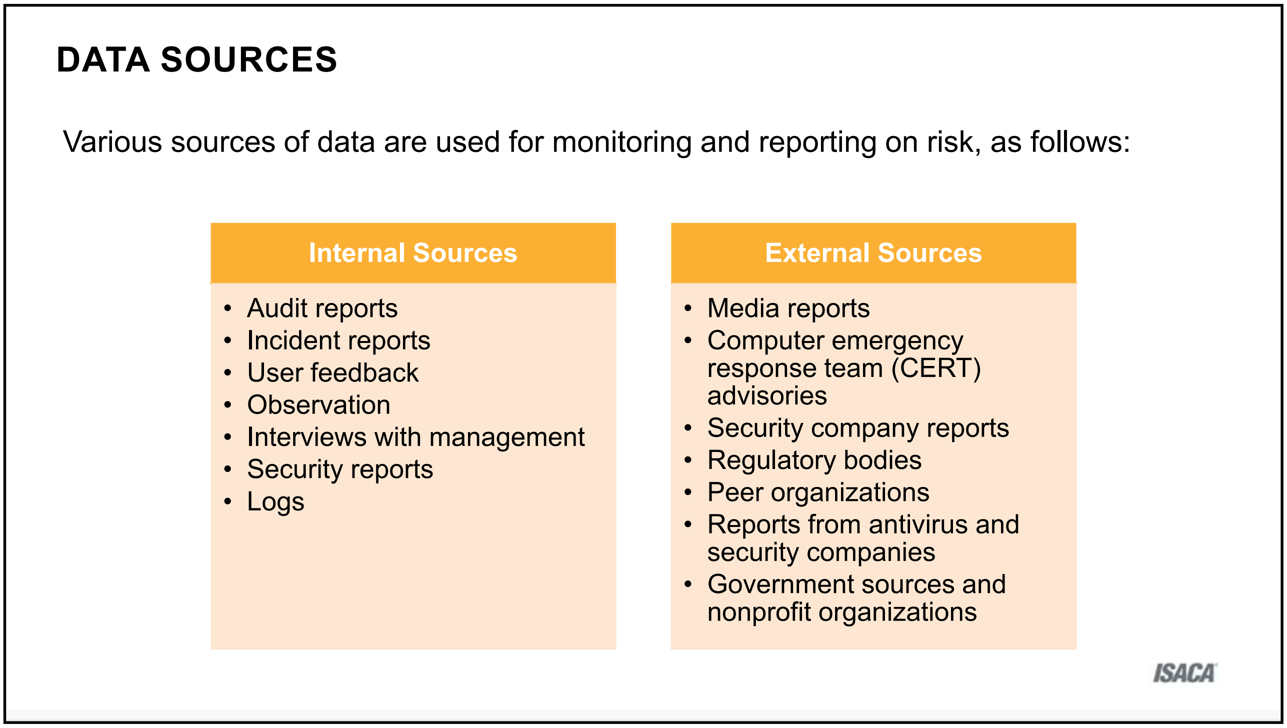
Key Term	Definition
IT risk profile	A description of the overall (identified) IT risk to which the enterprise is exposed
Security incident	A series of unexpected events involving an attack or series of attacks (compromise and/or breach of security) at one or more sites



TASK TO KNOWLEDGE STATEMENTS

How does Task 4.2 relate to each of the following knowledge statements?

Knowledge Statement	Example
22. Data collection and extraction tools and techniques	A KRIs effectiveness is based on its ability to predict changes in trends that give rise to risk, so data collection and extraction are critical components.
24. Characteristics of inherent and residual risk	The KRI monitors residual risk, alerting risk owners of any positive or negative variances.
32. Key risk indicators (KRIs)	A KRI is an indicator with the greatest ability to warn of changes or trends in the IT risk profile.
34. Risk monitoring tools and techniques	KRIs that utilize data from automated and properly configured security monitoring and analytic tools provide management a greater level of assurance, as compared to manual assessment methods.



DATA SOURCES

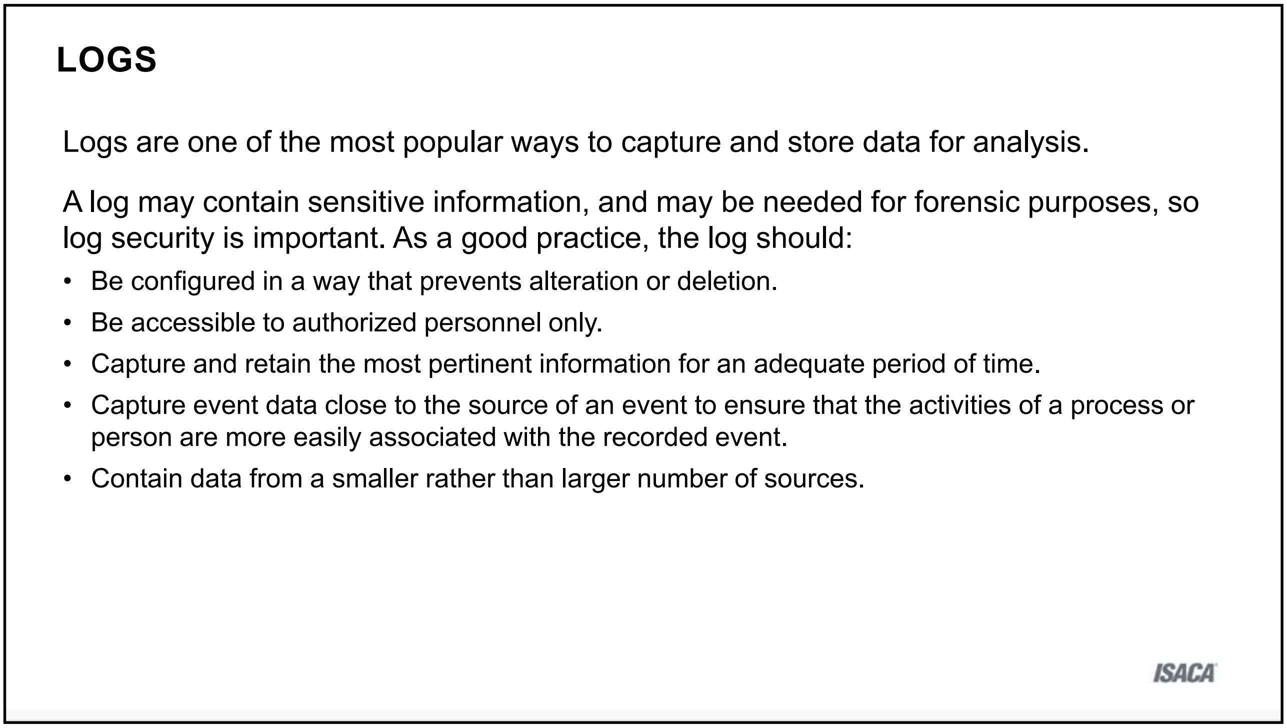
Various sources of data are used for monitoring and reporting on risk, as follows:

Internal Sources

- Audit reports
- Incident reports
- User feedback
- Observation
- Interviews with management
- Security reports
- Logs

External Sources

- Media reports
- Computer emergency response team (CERT) advisories
- Security company reports
- Regulatory bodies
- Peer organizations
- Reports from antivirus and security companies
- Government sources and nonprofit organizations



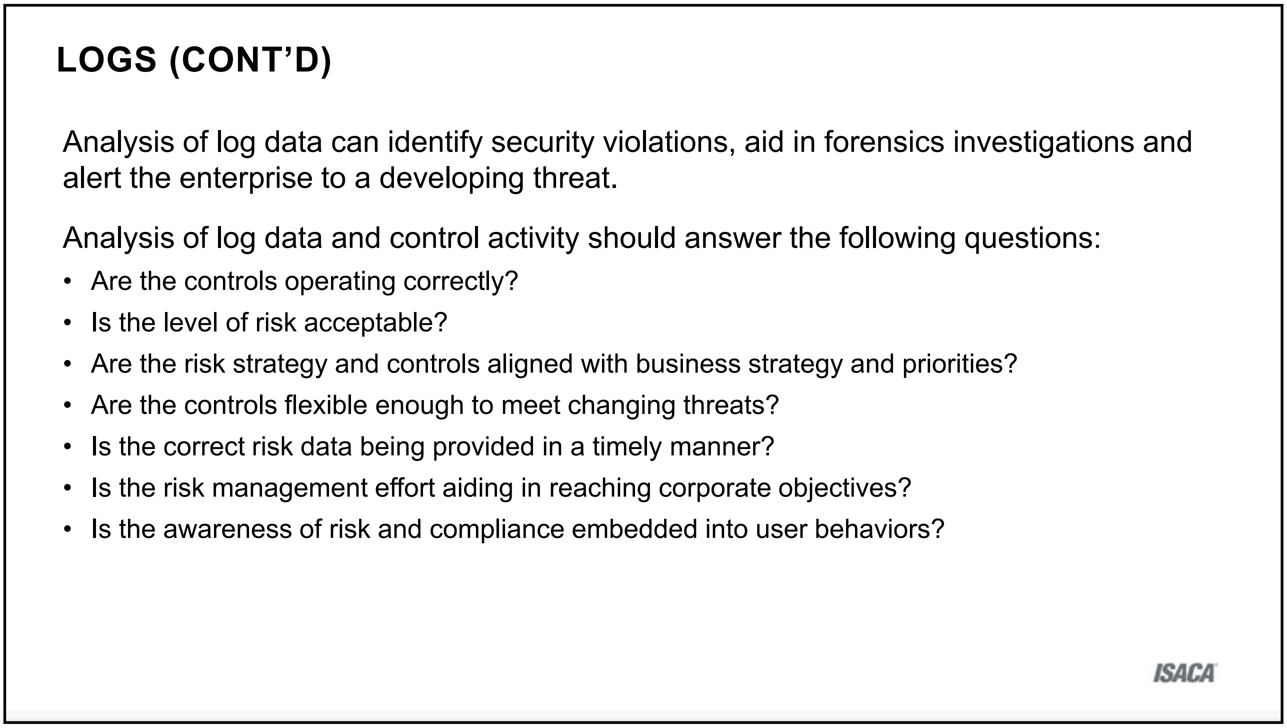
LOGS

Logs are one of the most popular ways to capture and store data for analysis.

A log may contain sensitive information, and may be needed for forensic purposes, so log security is important. As a good practice, the log should:

- Be configured in a way that prevents alteration or deletion.
- Be accessible to authorized personnel only.
- Capture and retain the most pertinent information for an adequate period of time.
- Capture event data close to the source of an event to ensure that the activities of a process or person are more easily associated with the recorded event.
- Contain data from a smaller rather than larger number of sources.

ISACA

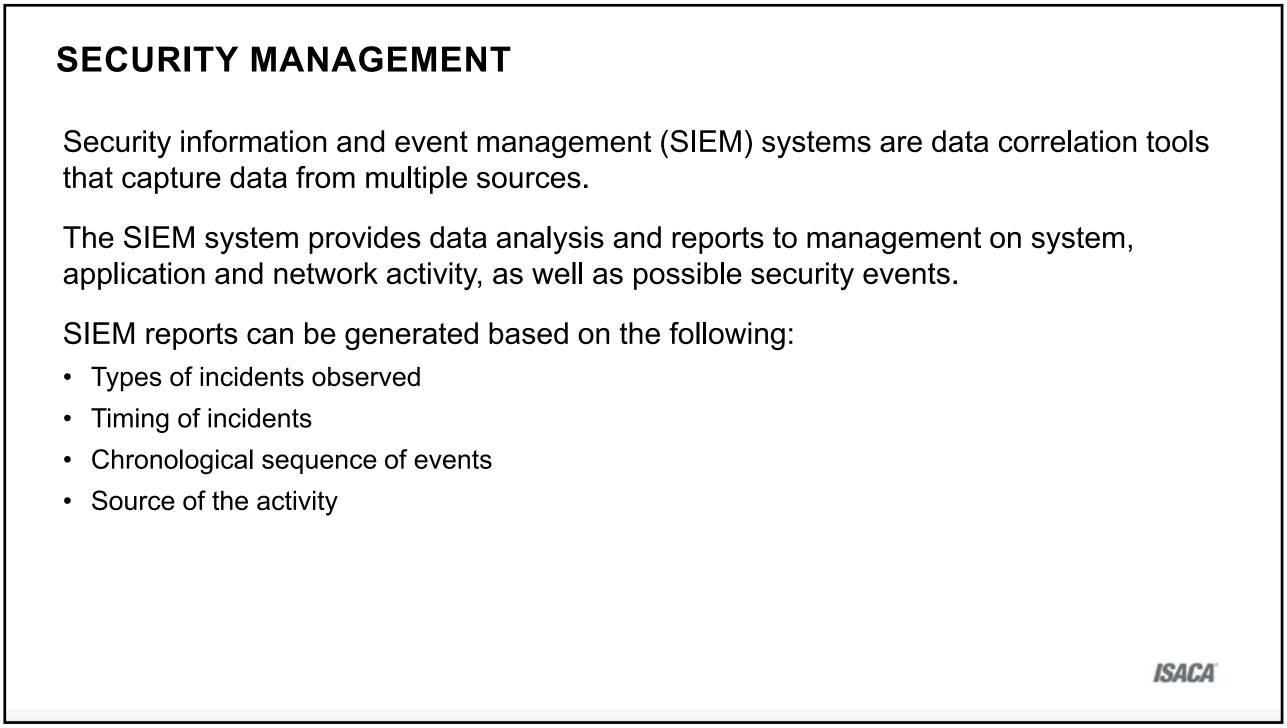


LOGS (CONT'D)

Analysis of log data can identify security violations, aid in forensics investigations and alert the enterprise to a developing threat.

Analysis of log data and control activity should answer the following questions:

- Are the controls operating correctly?
- Is the level of risk acceptable?
- Are the risk strategy and controls aligned with business strategy and priorities?
- Are the controls flexible enough to meet changing threats?
- Is the correct risk data being provided in a timely manner?
- Is the risk management effort aiding in reaching corporate objectives?
- Is the awareness of risk and compliance embedded into user behaviors?



SECURITY MANAGEMENT

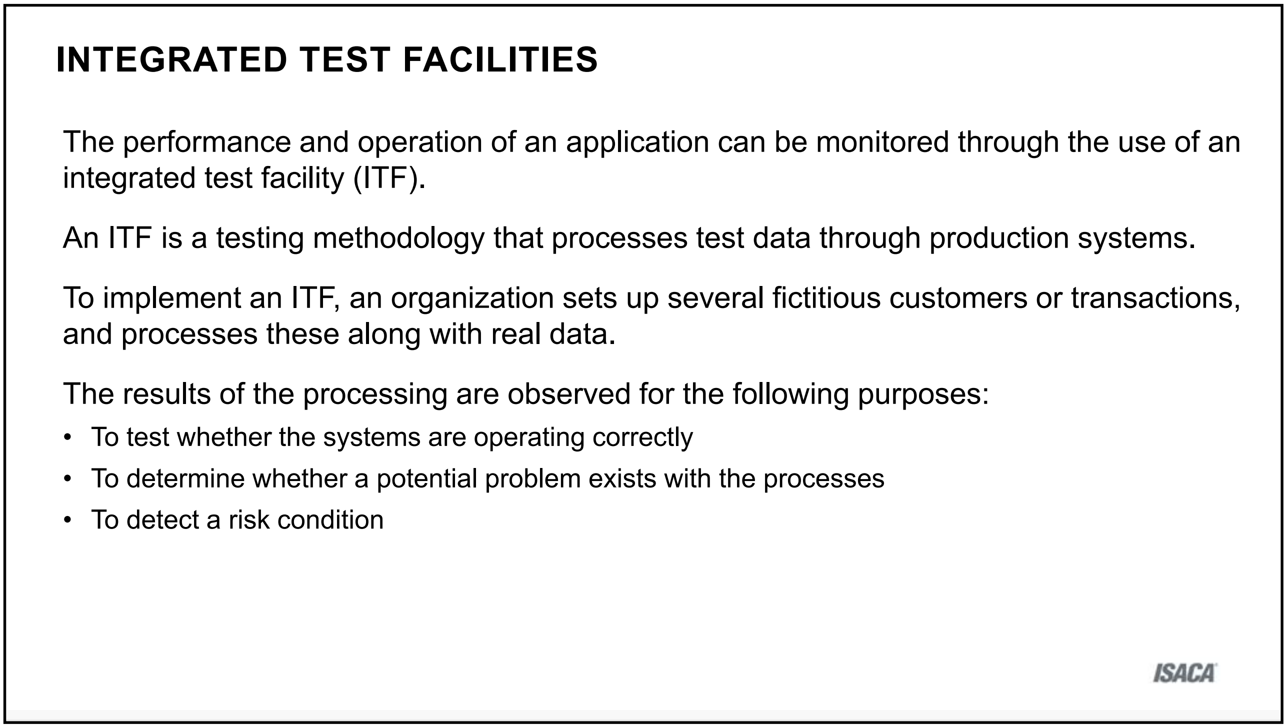
Security information and event management (SIEM) systems are data correlation tools that capture data from multiple sources.

The SIEM system provides data analysis and reports to management on system, application and network activity, as well as possible security events.

SIEM reports can be generated based on the following:

- Types of incidents observed
- Timing of incidents
- Chronological sequence of events
- Source of the activity

ISACA



INTEGRATED TEST FACILITIES

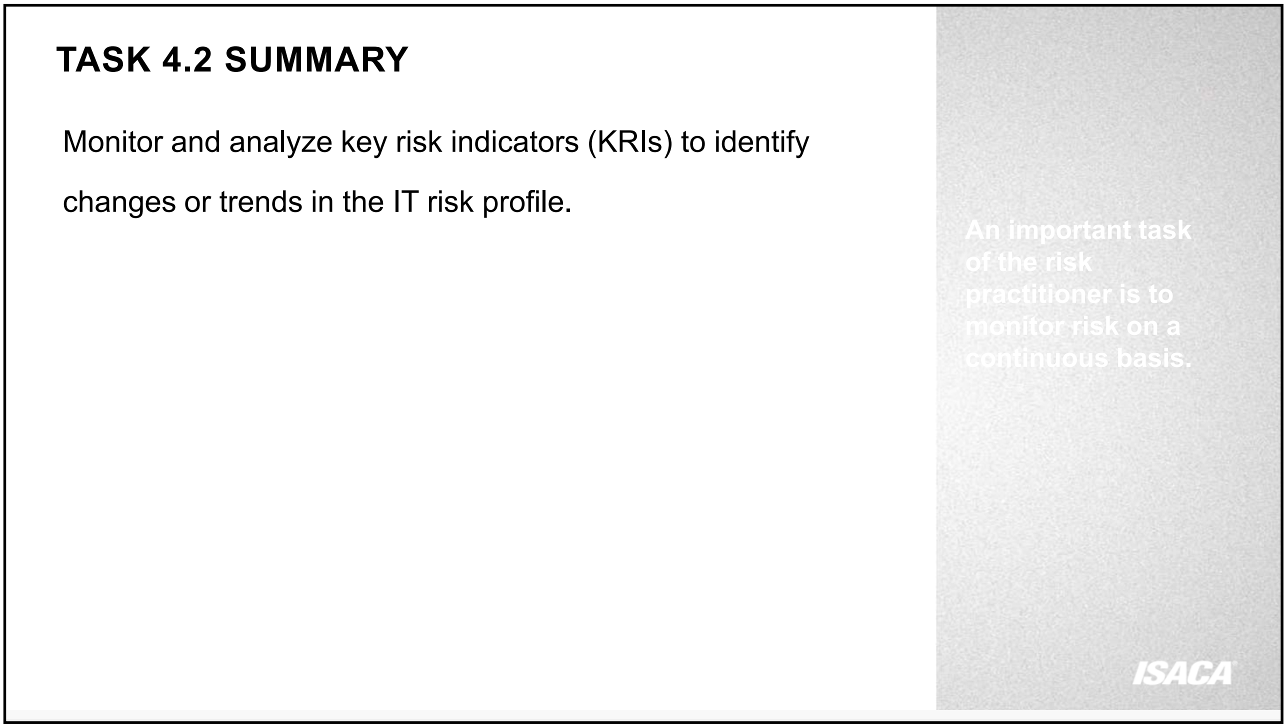
The performance and operation of an application can be monitored through the use of an integrated test facility (ITF).

An ITF is a testing methodology that processes test data through production systems.

To implement an ITF, an organization sets up several fictitious customers or transactions, and processes these along with real data.

The results of the processing are observed for the following purposes:

- To test whether the systems are operating correctly
- To determine whether a potential problem exists with the processes
- To detect a risk condition



TASK 4.2 SUMMARY

Monitor and analyze key risk indicators (KRIs) to identify changes or trends in the IT risk profile.

An important task of the risk practitioner is to monitor risk on a continuous basis.

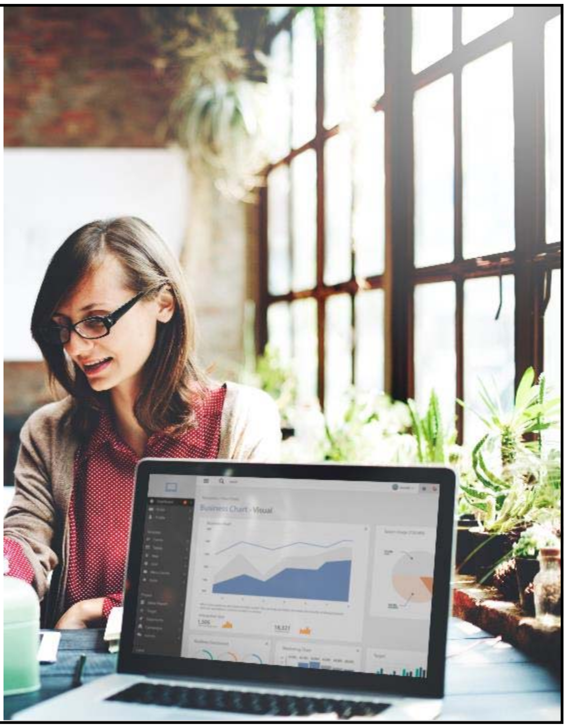
TASK 4.2 DISCUSSION

Discuss the following questions:

A. In what ways does setting thresholds aid in the monitoring of KRI data?

B. What process or processes should be in place to respond when a threshold is reached?

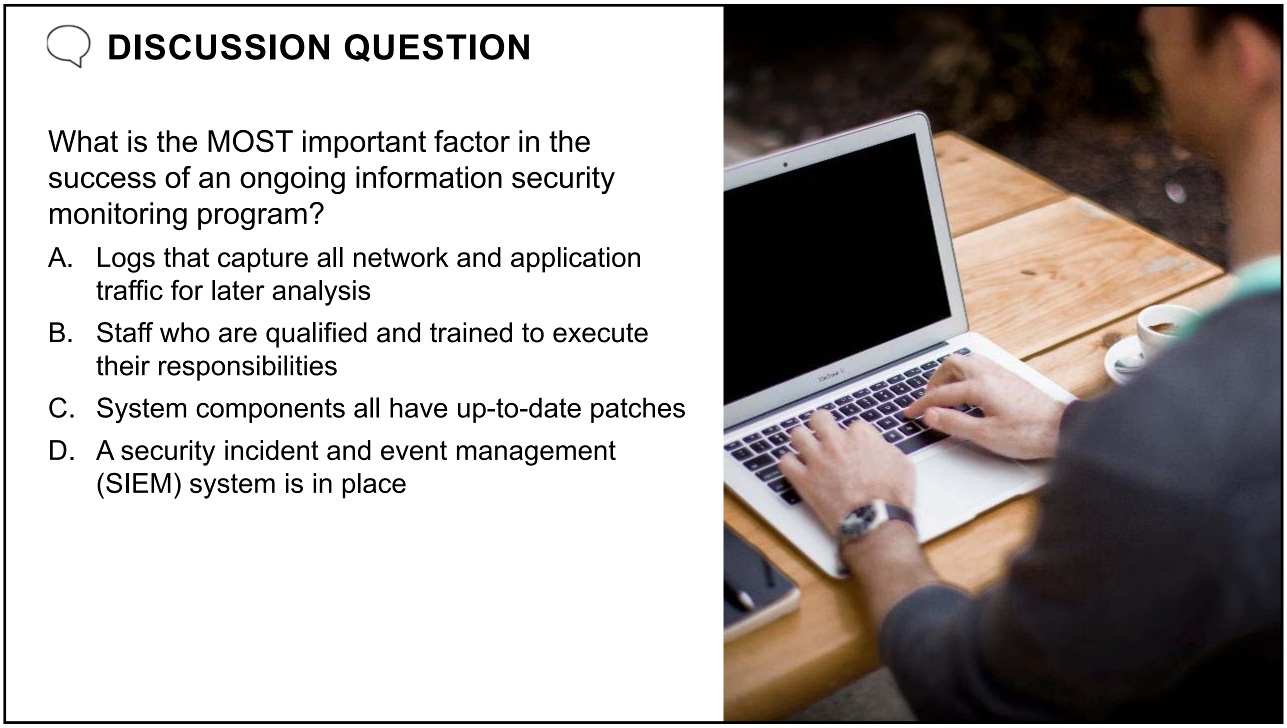
C. How is the IT risk profile updated? What information is needed for this update?



DISCUSSION QUESTION

Which of the following metrics is the MOST useful in measuring the monitoring of violation logs?

A. Penetration attempts investigated
B. Violation log reports produced
C. Violation log entries
D. Frequency of corrective actions taken



DISCUSSION QUESTION

What is the MOST important factor in the success of an ongoing information security monitoring program?

A. Logs that capture all network and application traffic for later analysis

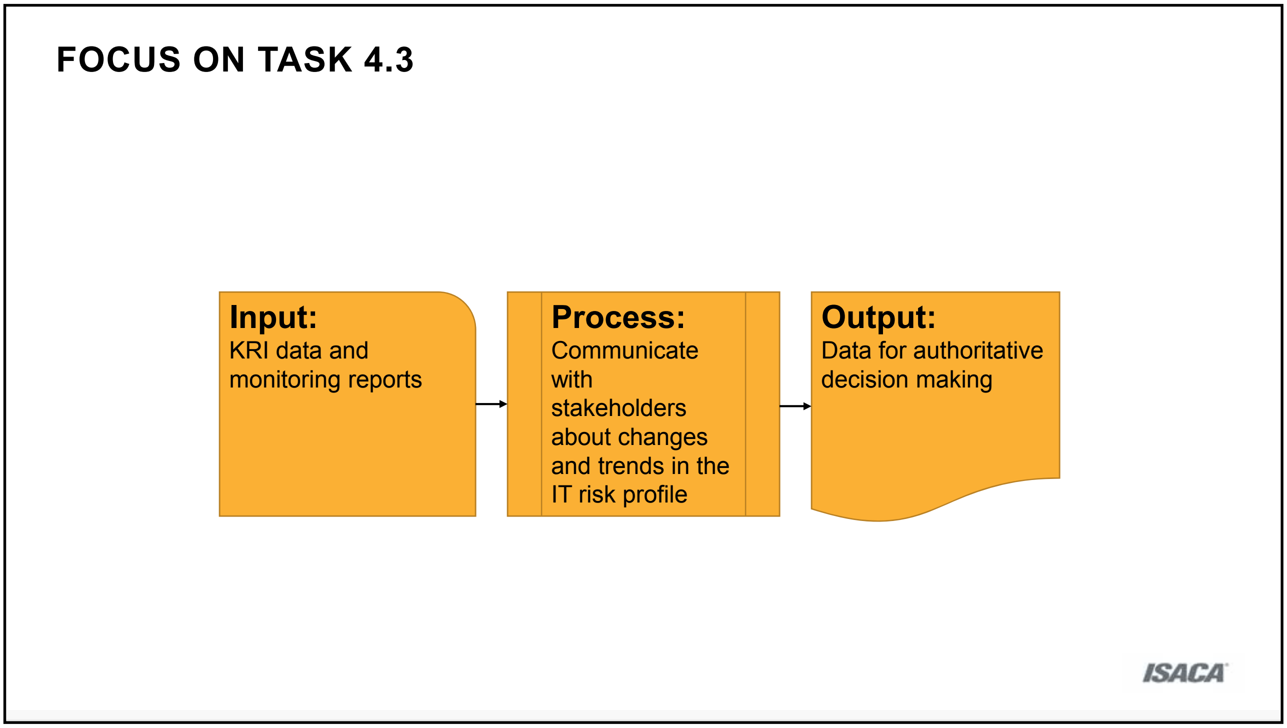
B. Staff who are qualified and trained to execute their responsibilities

C. System components all have up-to-date patches

D. A security incident and event management (SIEM) system is in place

TASK 4.3

Report on changes or trends related to the IT risk profile to assist management and relevant stakeholders in decision making.

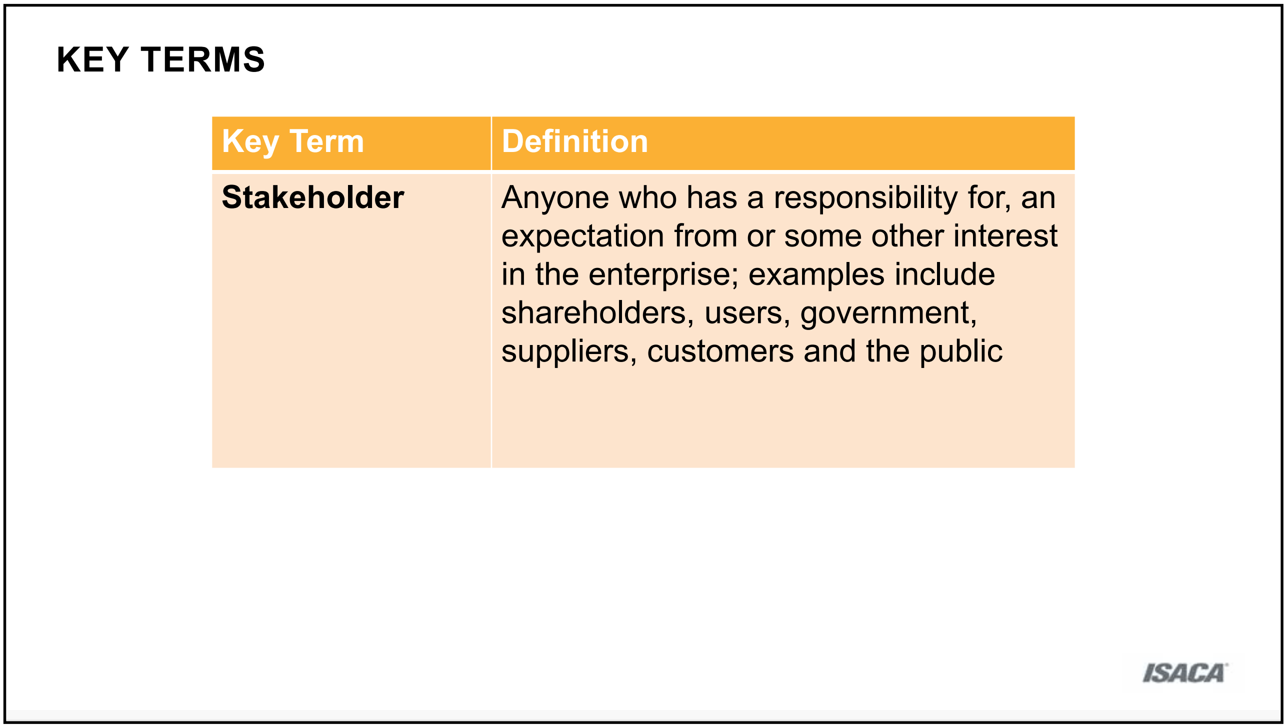


FOCUS ON TASK 4.3

Input:
KRI data and monitoring reports

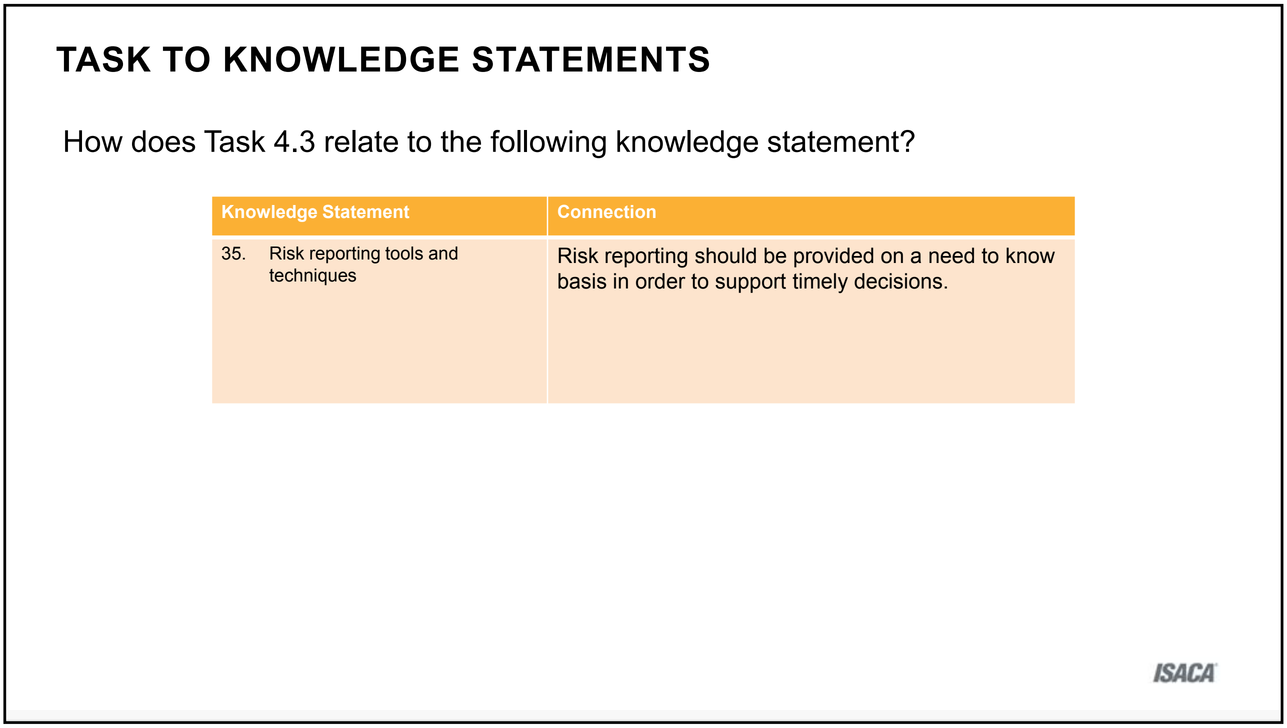
Process:
Communicate with stakeholders about changes and trends in the IT risk profile

Output:
Data for authoritative decision making



KEY TERMS

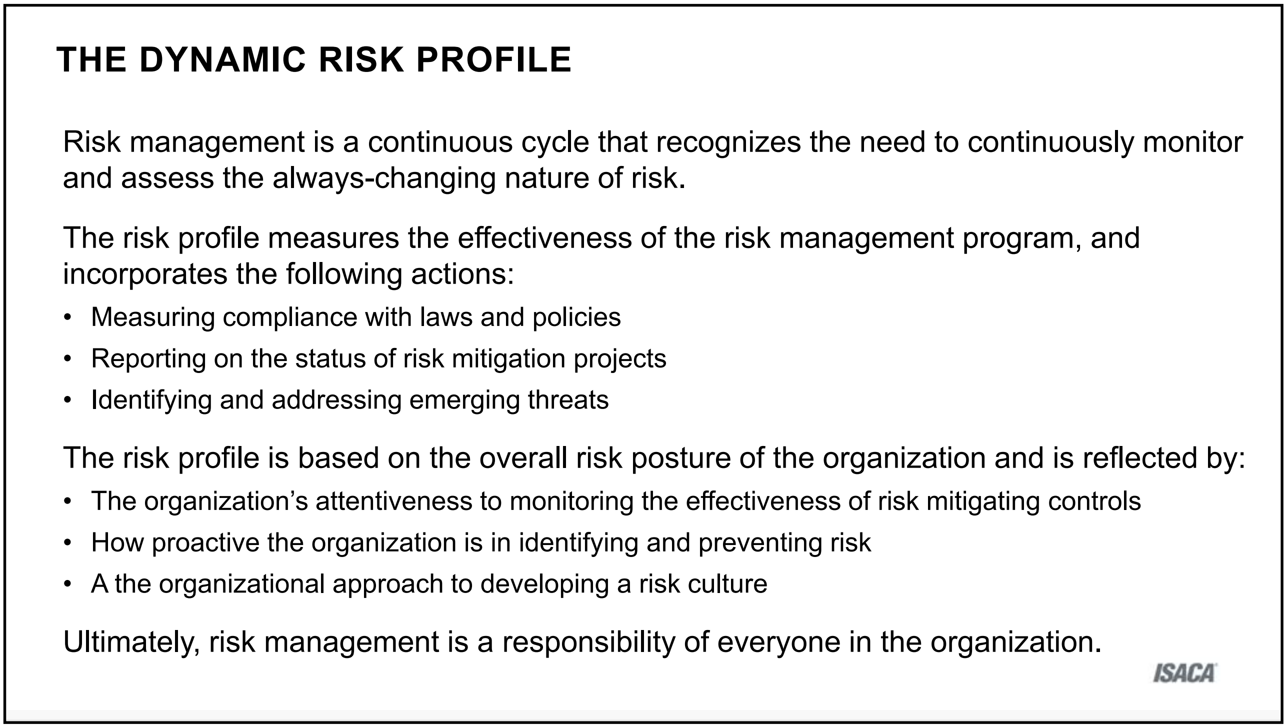
Key Term	Definition
Stakeholder	Anyone who has a responsibility for, an expectation from or some other interest in the enterprise; examples include shareholders, users, government, suppliers, customers and the public



TASK TO KNOWLEDGE STATEMENTS

How does Task 4.3 relate to the following knowledge statement?

Knowledge Statement	Connection
35. Risk reporting tools and techniques	Risk reporting should be provided on a need to know basis in order to support timely decisions.



THE DYNAMIC RISK PROFILE

Risk management is a continuous cycle that recognizes the need to continuously monitor and assess the always-changing nature of risk.

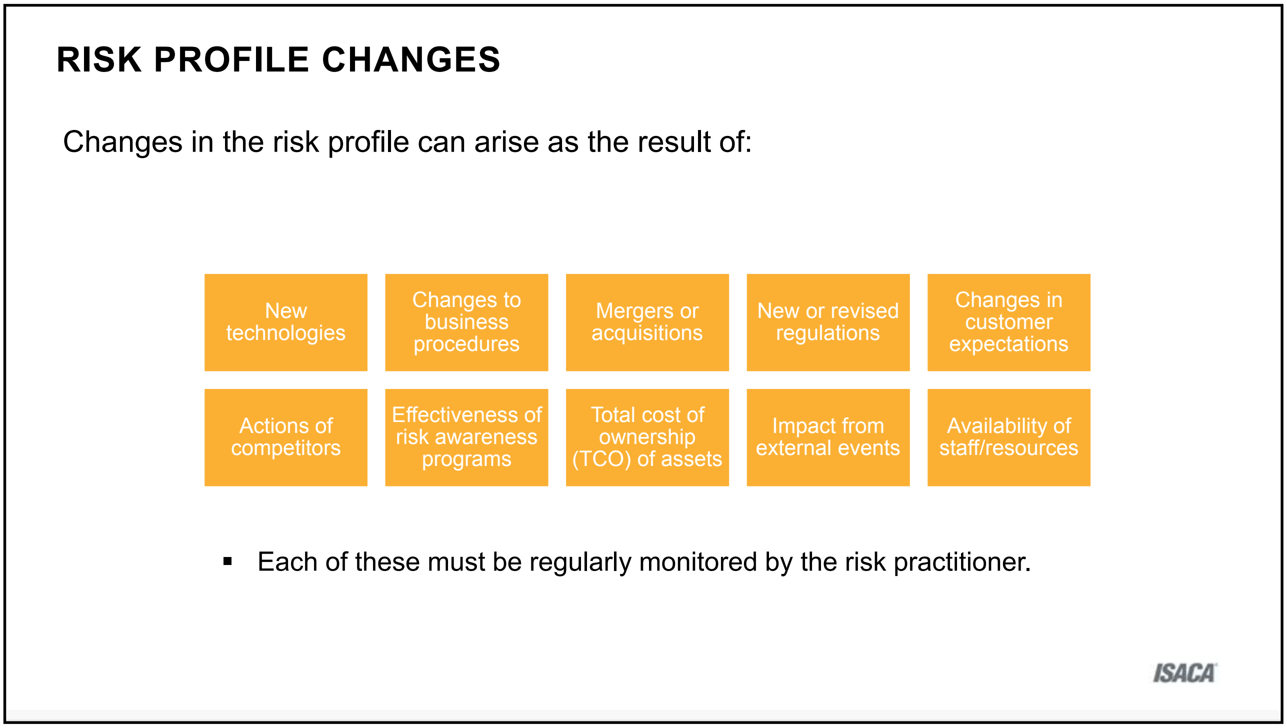
The risk profile measures the effectiveness of the risk management program, and incorporates the following actions:

- Measuring compliance with laws and policies
- Reporting on the status of risk mitigation projects
- Identifying and addressing emerging threats

The risk profile is based on the overall risk posture of the organization and is reflected by:

- The organization’s attentiveness to monitoring the effectiveness of risk mitigating controls
- How proactive the organization is in identifying and preventing risk
- A the organizational approach to developing a risk culture

Ultimately, risk management is a responsibility of everyone in the organization.



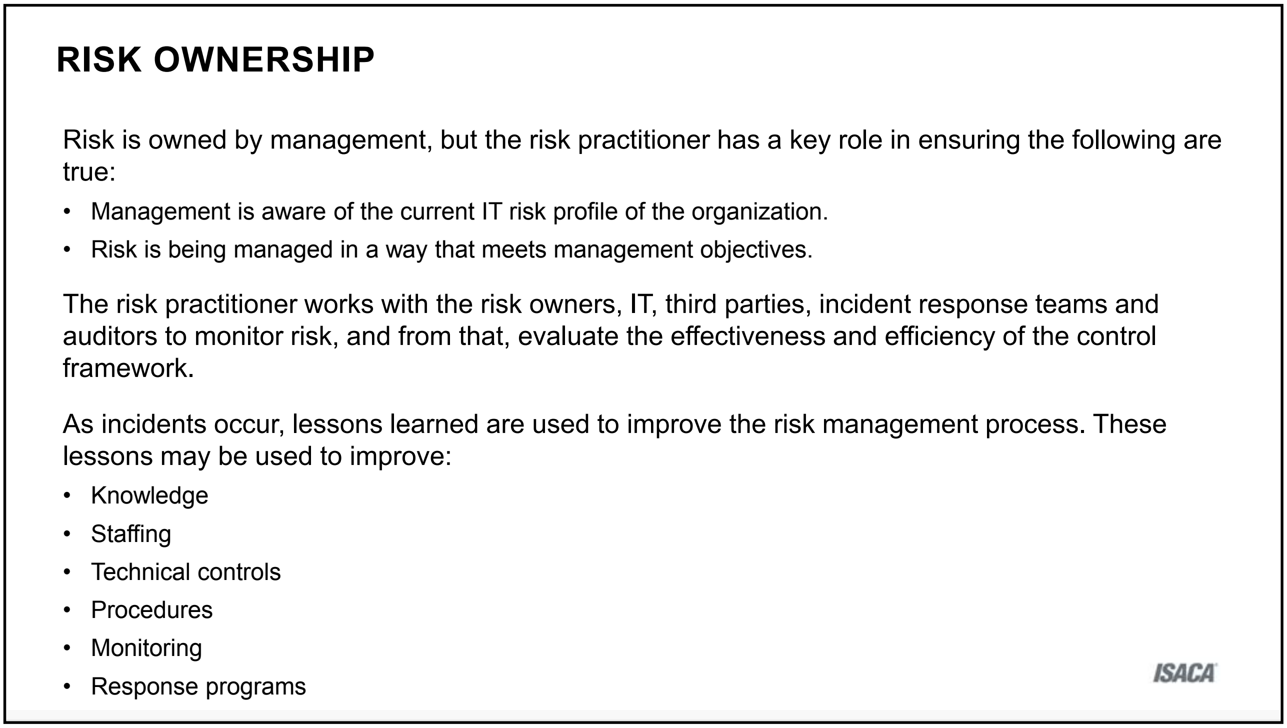
RISK PROFILE CHANGES

Changes in the risk profile can arise as the result of:

New technologies	Changes to business procedures	Mergers or acquisitions	New or revised regulations	Changes in customer expectations
Actions of competitors	Effectiveness of risk awareness programs	Total cost of ownership (TCO) of assets	Impact from external events	Availability of staff/resources

- Each of these must be regularly monitored by the risk practitioner.

ISACA



RISK OWNERSHIP

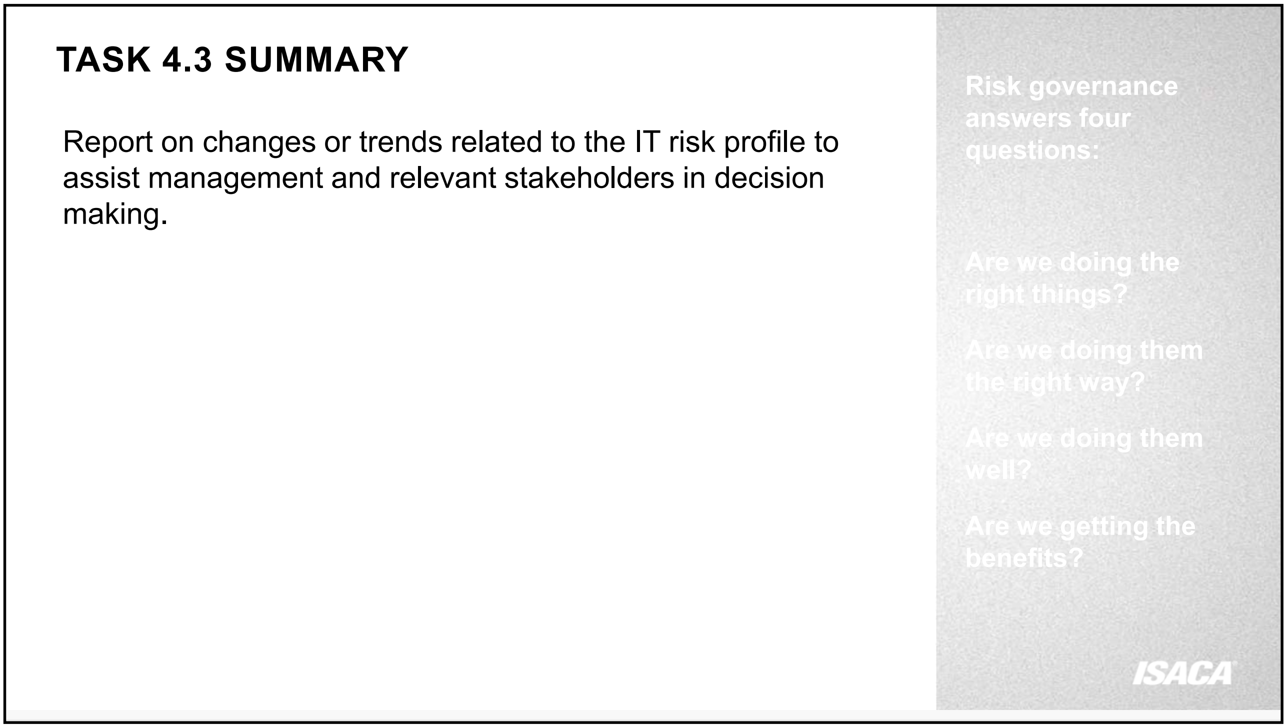
Risk is owned by management, but the risk practitioner has a key role in ensuring the following are true:

- Management is aware of the current IT risk profile of the organization.
- Risk is being managed in a way that meets management objectives.

The risk practitioner works with the risk owners, IT, third parties, incident response teams and auditors to monitor risk, and from that, evaluate the effectiveness and efficiency of the control framework.

As incidents occur, lessons learned are used to improve the risk management process. These lessons may be used to improve:

- Knowledge
- Staffing
- Technical controls
- Procedures
- Monitoring
- Response programs



TASK 4.3 SUMMARY

Report on changes or trends related to the IT risk profile to assist management and relevant stakeholders in decision making.

Risk governance answers four questions:

Are we doing the right things?

Are we doing them the right way?

Are we doing them well?

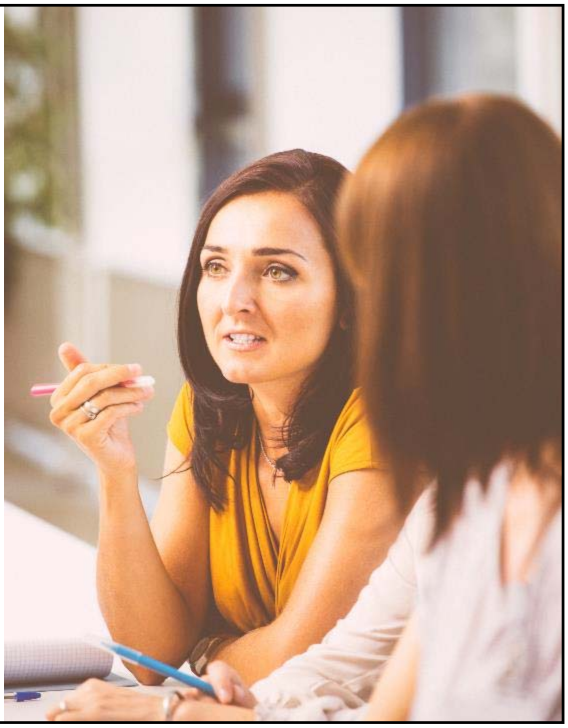
Are we getting the benefits?

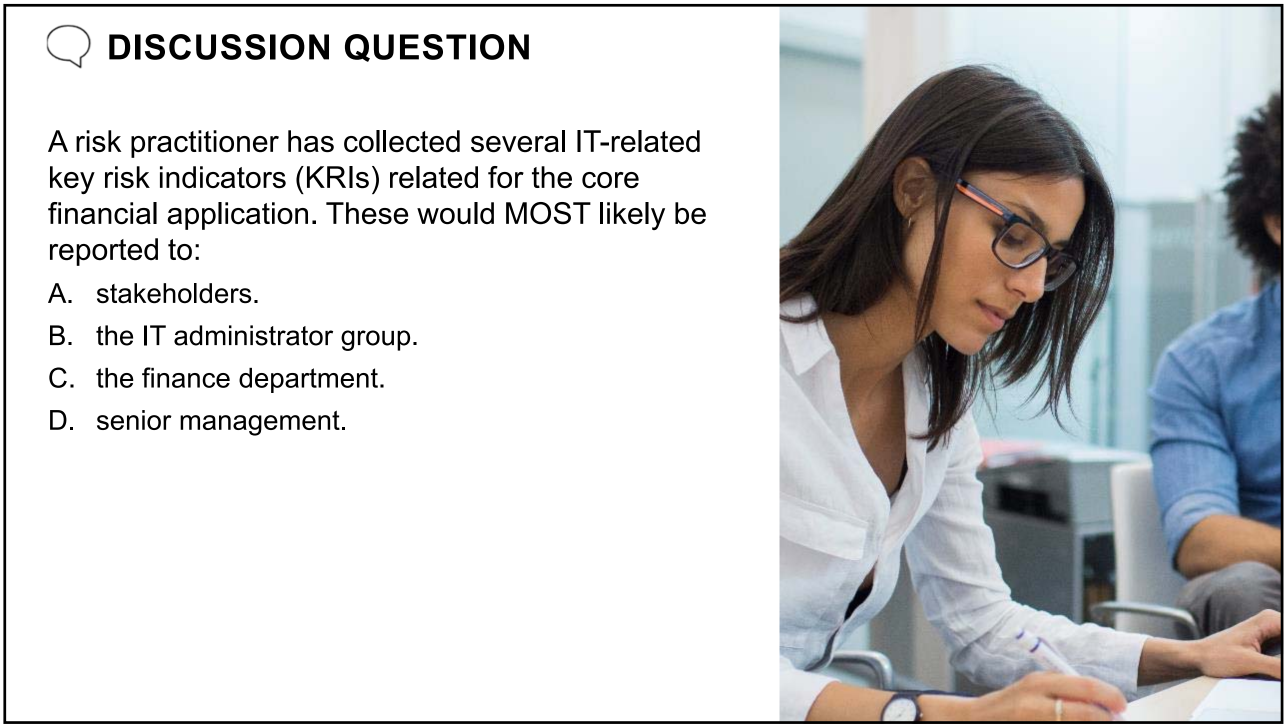
ISACA

TASK 4.3 DISCUSSION

In what ways does the risk profile support managerial decision making?

What aspects of organizational management might be impacted by changes in the risk profile?





DISCUSSION QUESTION

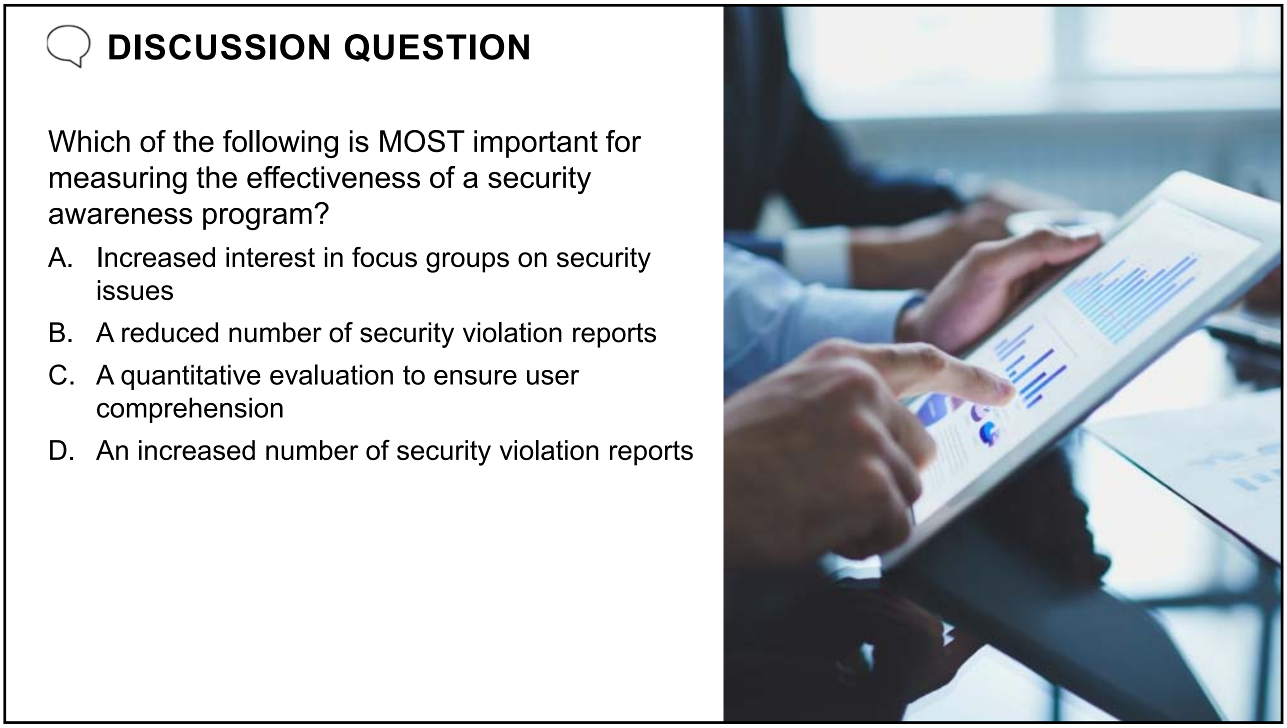
A risk practitioner has collected several IT-related key risk indicators (KRIs) related for the core financial application. These would MOST likely be reported to:

A. stakeholders.

B. the IT administrator group.

C. the finance department.

D. senior management.



DISCUSSION QUESTION

Which of the following is MOST important for measuring the effectiveness of a security awareness program?

A. Increased interest in focus groups on security issues

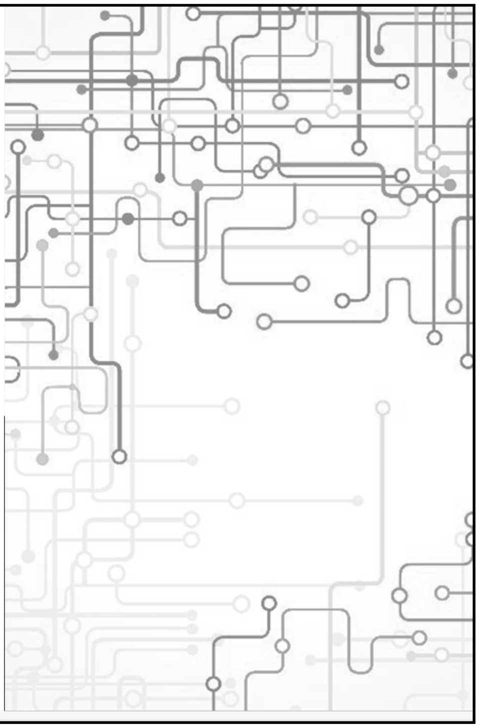
B. A reduced number of security violation reports

C. A quantitative evaluation to ensure user comprehension

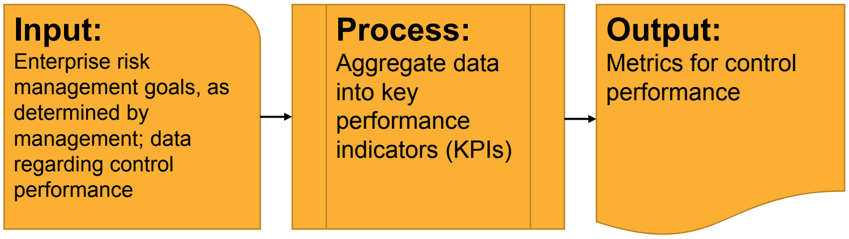
D. An increased number of security violation reports

TASK 4.4

Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of control performance.



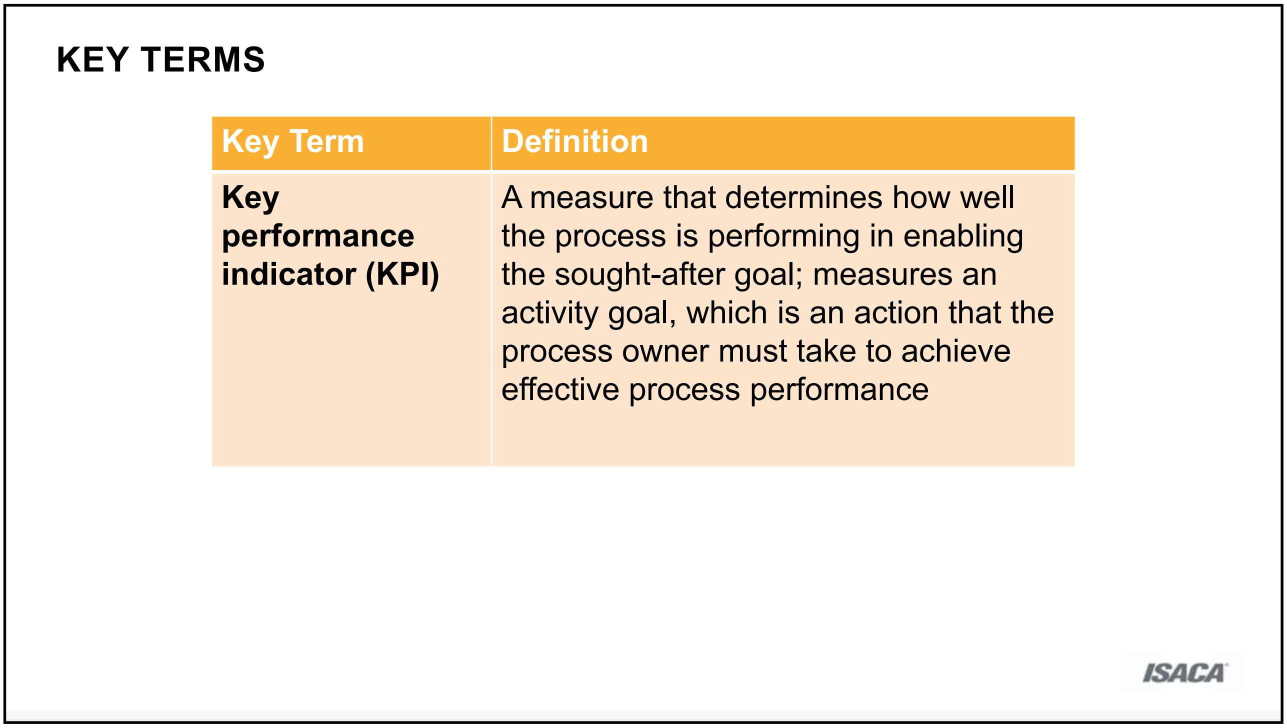
FOCUS ON TASK 4.4



Input:
Enterprise risk management goals, as determined by management; data regarding control performance

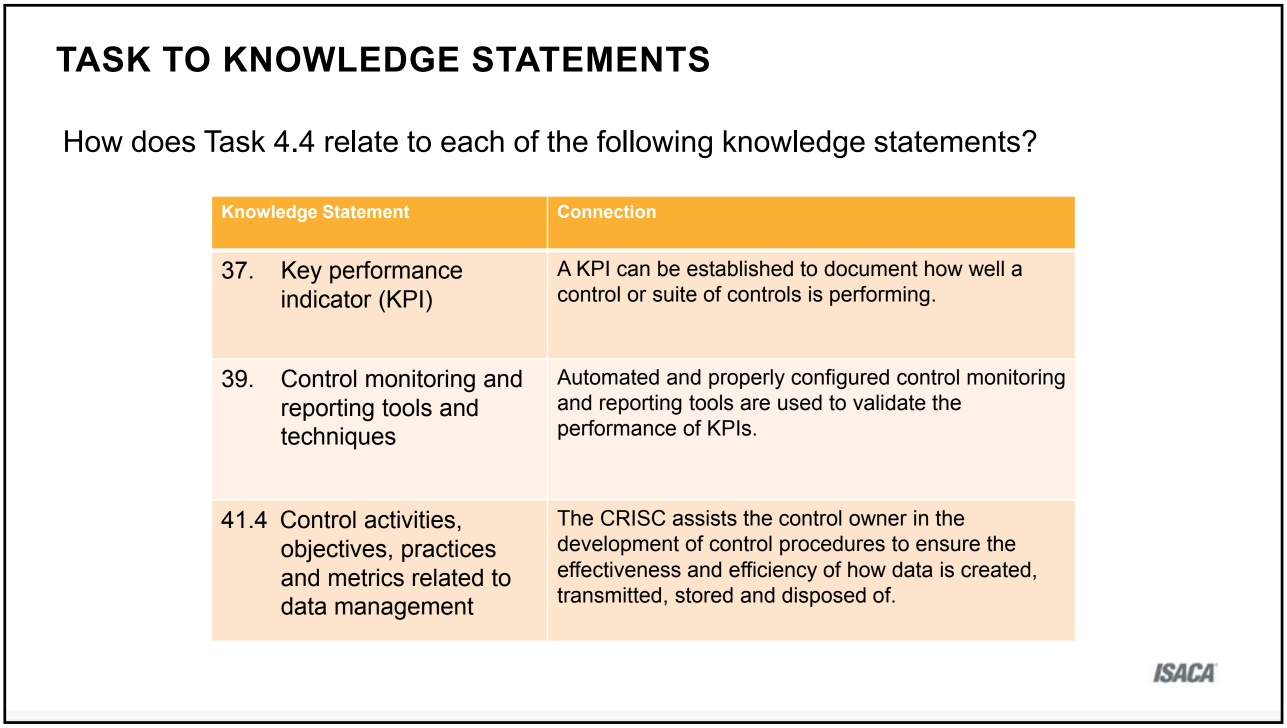
Process:
Aggregate data into key performance indicators (KPIs)

Output:
Metrics for control performance



KEY TERMS

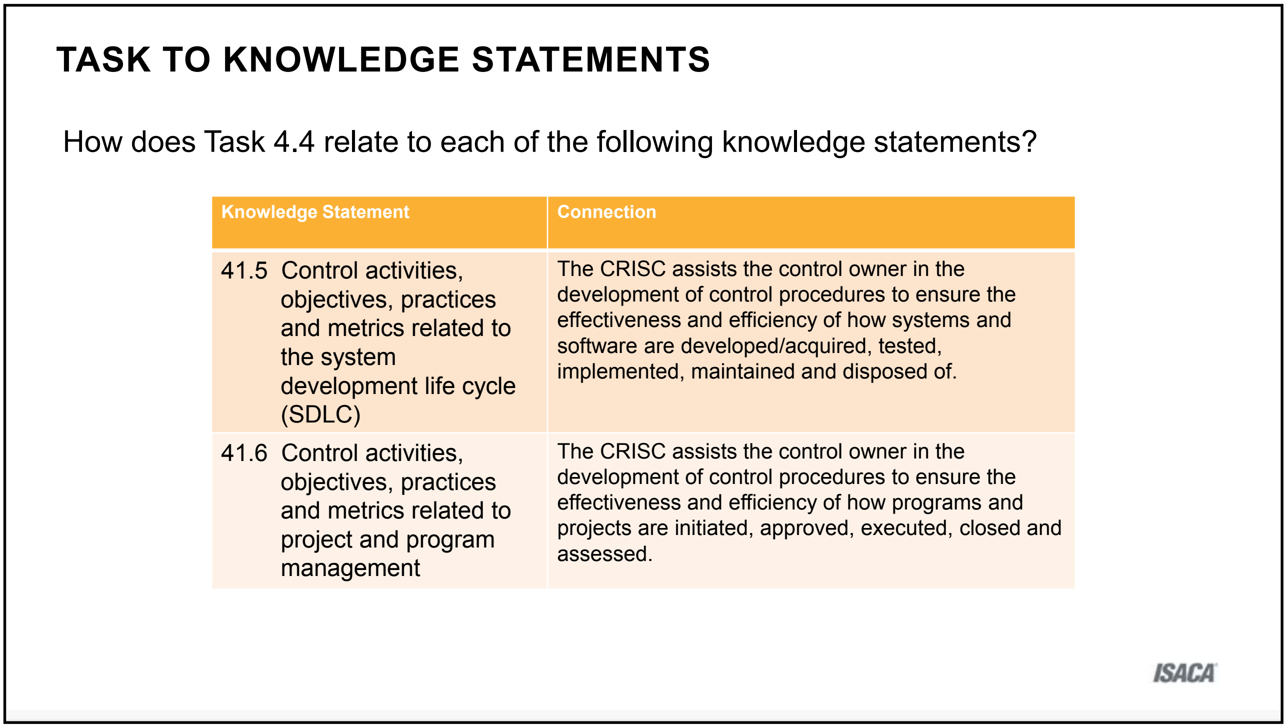
Key Term	Definition
Key performance indicator (KPI)	A measure that determines how well the process is performing in enabling the sought-after goal; measures an activity goal, which is an action that the process owner must take to achieve effective process performance



TASK TO KNOWLEDGE STATEMENTS

How does Task 4.4 relate to each of the following knowledge statements?

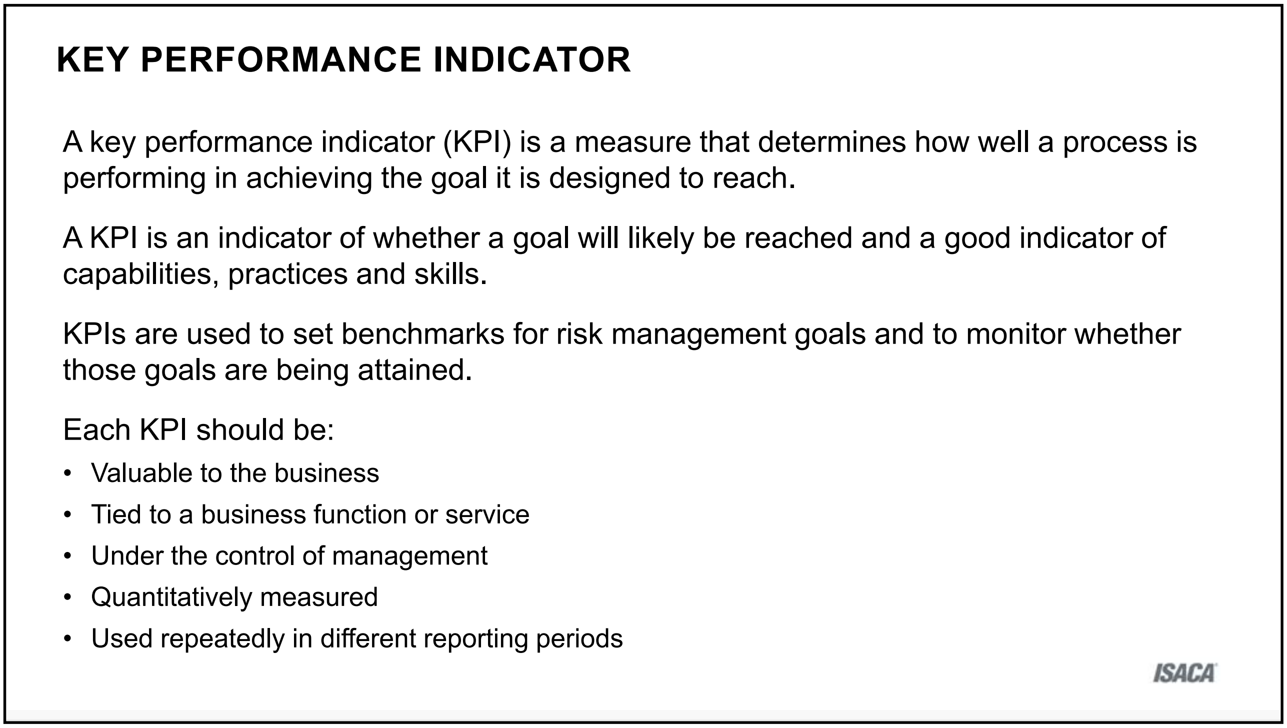
Knowledge Statement	Connection
37. Key performance indicator (KPI)	A KPI can be established to document how well a control or suite of controls is performing.
39. Control monitoring and reporting tools and techniques	Automated and properly configured control monitoring and reporting tools are used to validate the performance of KPIs.
41.4 Control activities, objectives, practices and metrics related to data management	The CRISC assists the control owner in the development of control procedures to ensure the effectiveness and efficiency of how data is created, transmitted, stored and disposed of.



TASK TO KNOWLEDGE STATEMENTS

How does Task 4.4 relate to each of the following knowledge statements?

Knowledge Statement	Connection
41.5 Control activities, objectives, practices and metrics related to the system development life cycle (SDLC)	The CRISC assists the control owner in the development of control procedures to ensure the effectiveness and efficiency of how systems and software are developed/acquired, tested, implemented, maintained and disposed of.
41.6 Control activities, objectives, practices and metrics related to project and program management	The CRISC assists the control owner in the development of control procedures to ensure the effectiveness and efficiency of how programs and projects are initiated, approved, executed, closed and assessed.



KEY PERFORMANCE INDICATOR

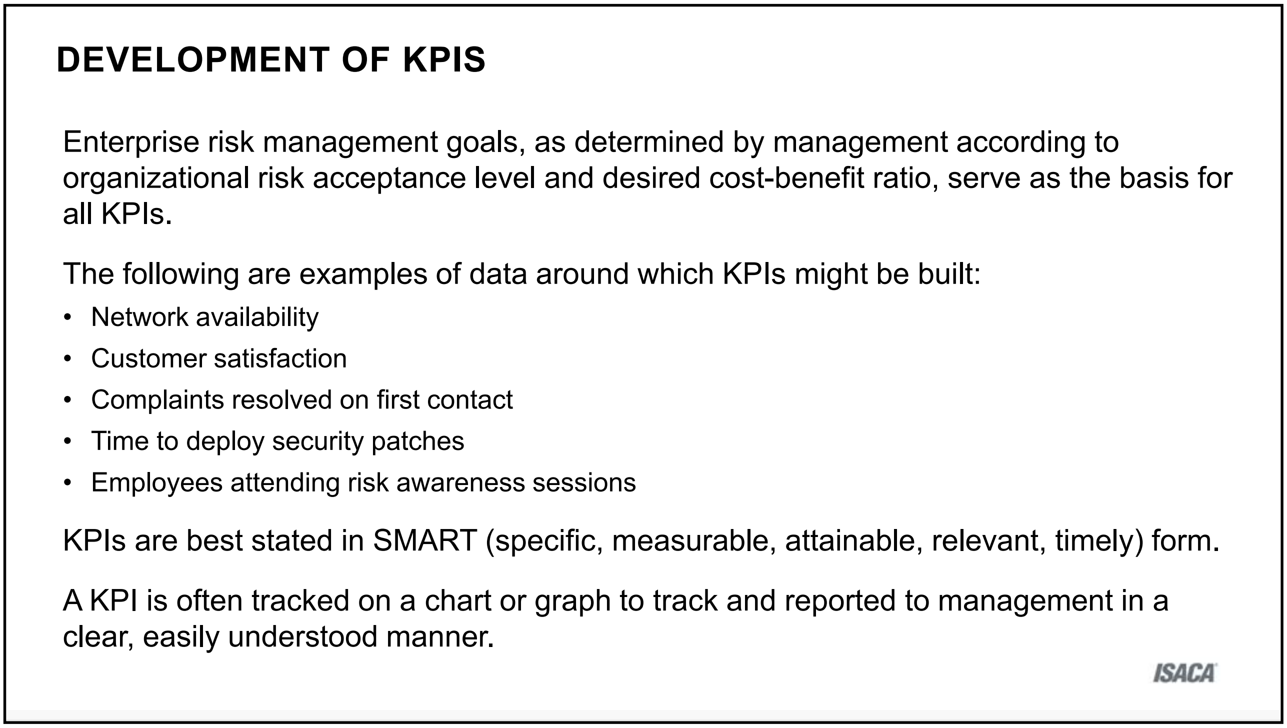
A key performance indicator (KPI) is a measure that determines how well a process is performing in achieving the goal it is designed to reach.

A KPI is an indicator of whether a goal will likely be reached and a good indicator of capabilities, practices and skills.

KPIs are used to set benchmarks for risk management goals and to monitor whether those goals are being attained.

Each KPI should be:

- Valuable to the business
- Tied to a business function or service
- Under the control of management
- Quantitatively measured
- Used repeatedly in different reporting periods



DEVELOPMENT OF KPIS

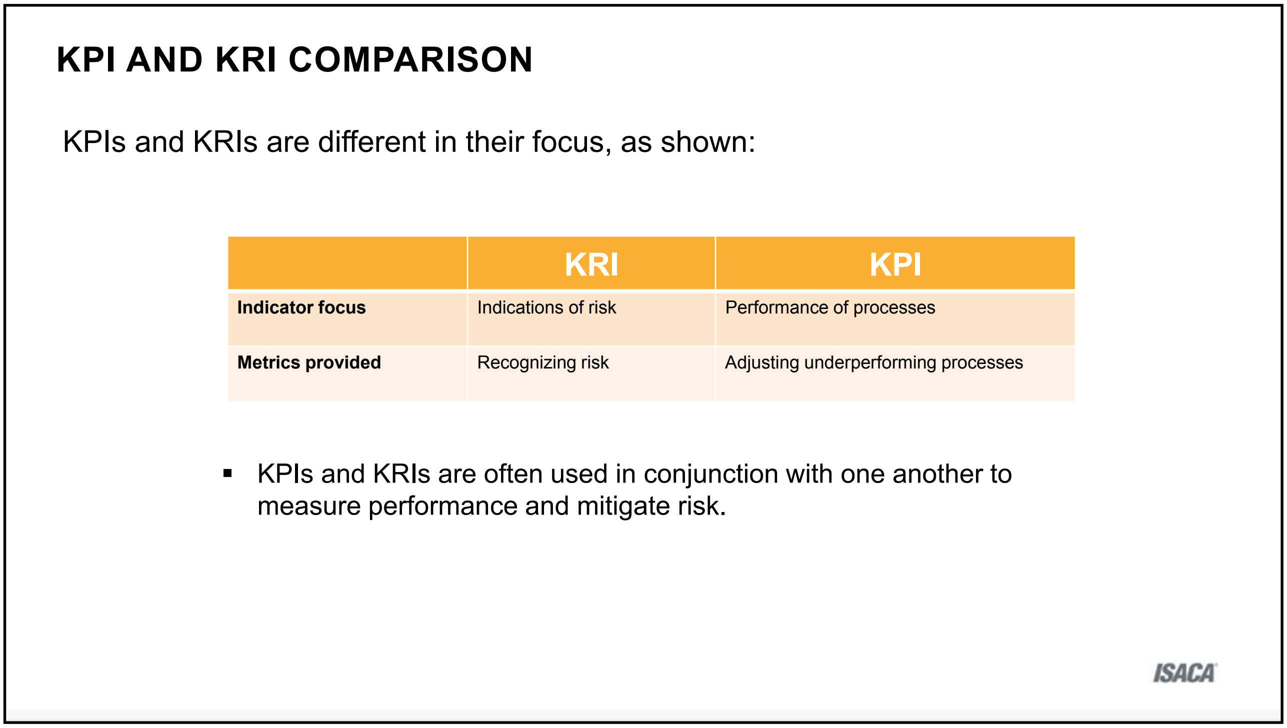
Enterprise risk management goals, as determined by management according to organizational risk acceptance level and desired cost-benefit ratio, serve as the basis for all KPIs.

The following are examples of data around which KPIs might be built:

- Network availability
- Customer satisfaction
- Complaints resolved on first contact
- Time to deploy security patches
- Employees attending risk awareness sessions

KPIs are best stated in SMART (specific, measurable, attainable, relevant, timely) form.

A KPI is often tracked on a chart or graph to track and reported to management in a clear, easily understood manner.

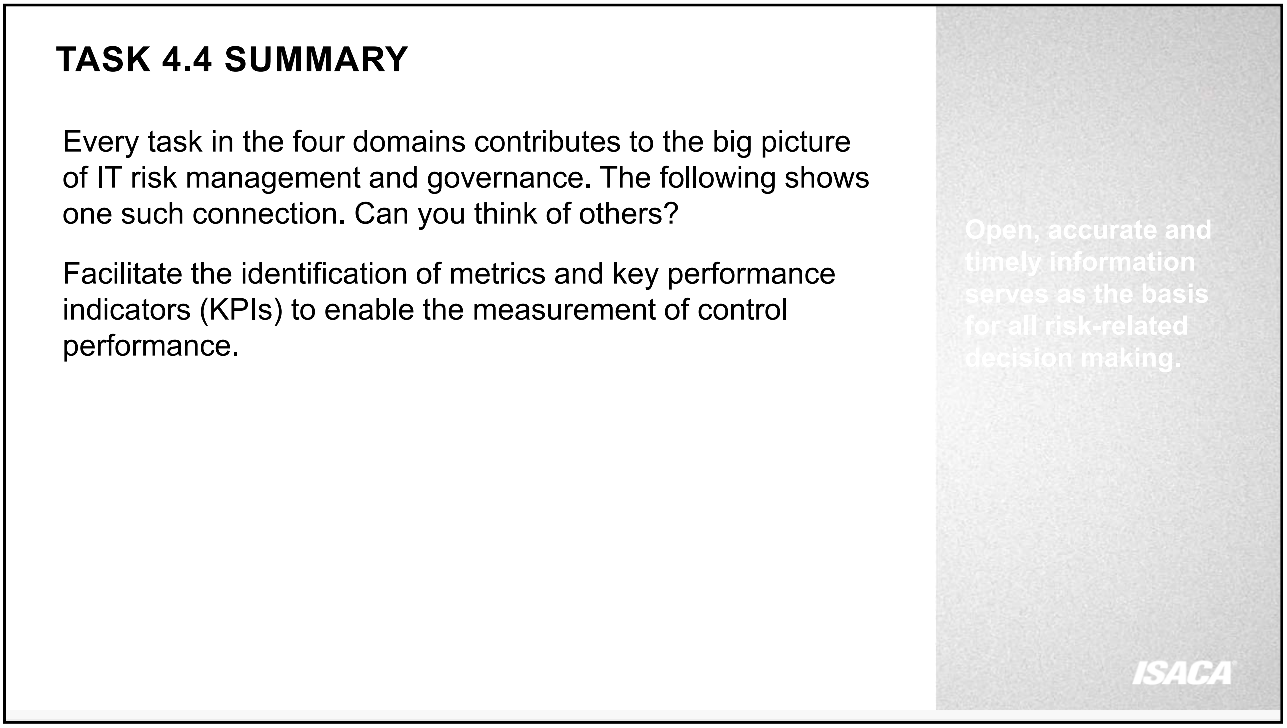


KPI AND KRI COMPARISON

KPIs and KRIs are different in their focus, as shown:

	KRI	KPI
Indicator focus	Indications of risk	Performance of processes
Metrics provided	Recognizing risk	Adjusting underperforming processes

- KPIs and KRIs are often used in conjunction with one another to measure performance and mitigate risk.



TASK 4.4 SUMMARY

Every task in the four domains contributes to the big picture of IT risk management and governance. The following shows one such connection. Can you think of others?

Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of control performance.

Open, accurate and timely information serves as the basis for all risk-related decision making.

TASK 4.4 DISCUSSION

Thinking about the various types of logs and the data they provide, discuss how logs might support the KPI metrics.

What data is important to analyze in each type of log?

What other tools could be used in the KPI monitoring process?

DISCUSSION QUESTION

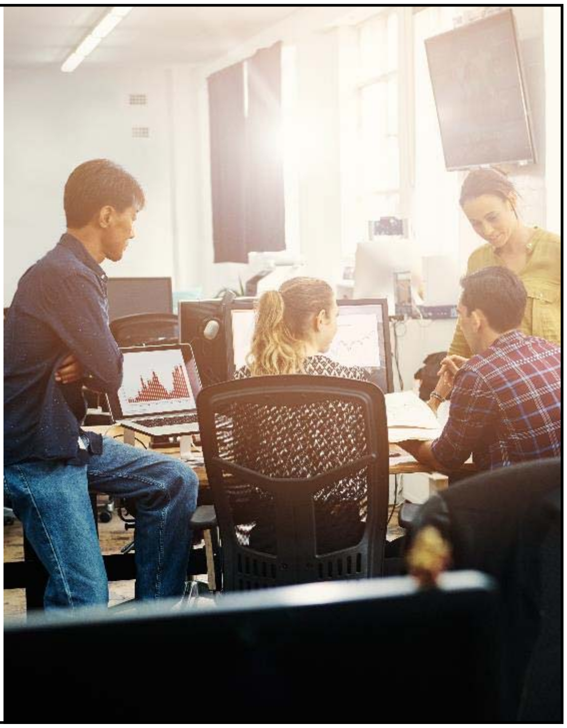
Risk monitoring provides timely information on the actual status of the enterprise with regard to risk. Which of the following choices provides an overall risk status of the enterprise?

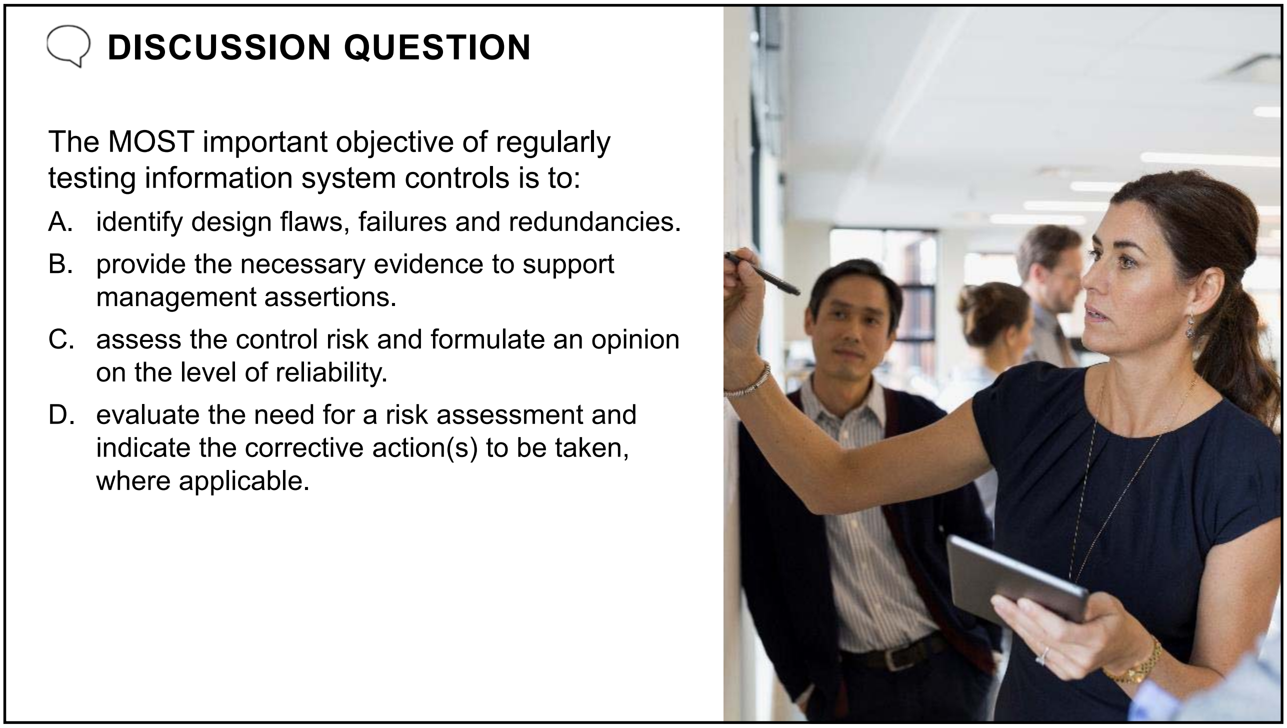
A. Risk management

B. Risk analysis

C. Risk appetite

D. Risk profile





DISCUSSION QUESTION

The MOST important objective of regularly testing information system controls is to:

A. identify design flaws, failures and redundancies.

B. provide the necessary evidence to support management assertions.

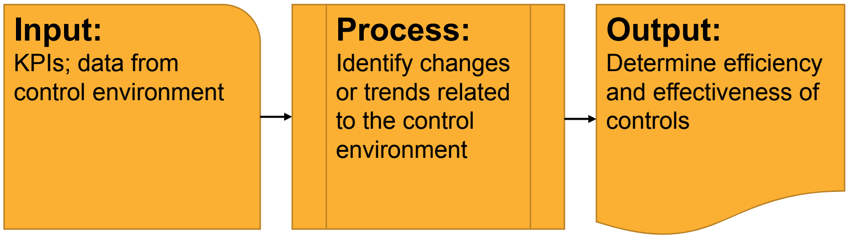
C. assess the control risk and formulate an opinion on the level of reliability.

D. evaluate the need for a risk assessment and indicate the corrective action(s) to be taken, where applicable.

TASK 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.

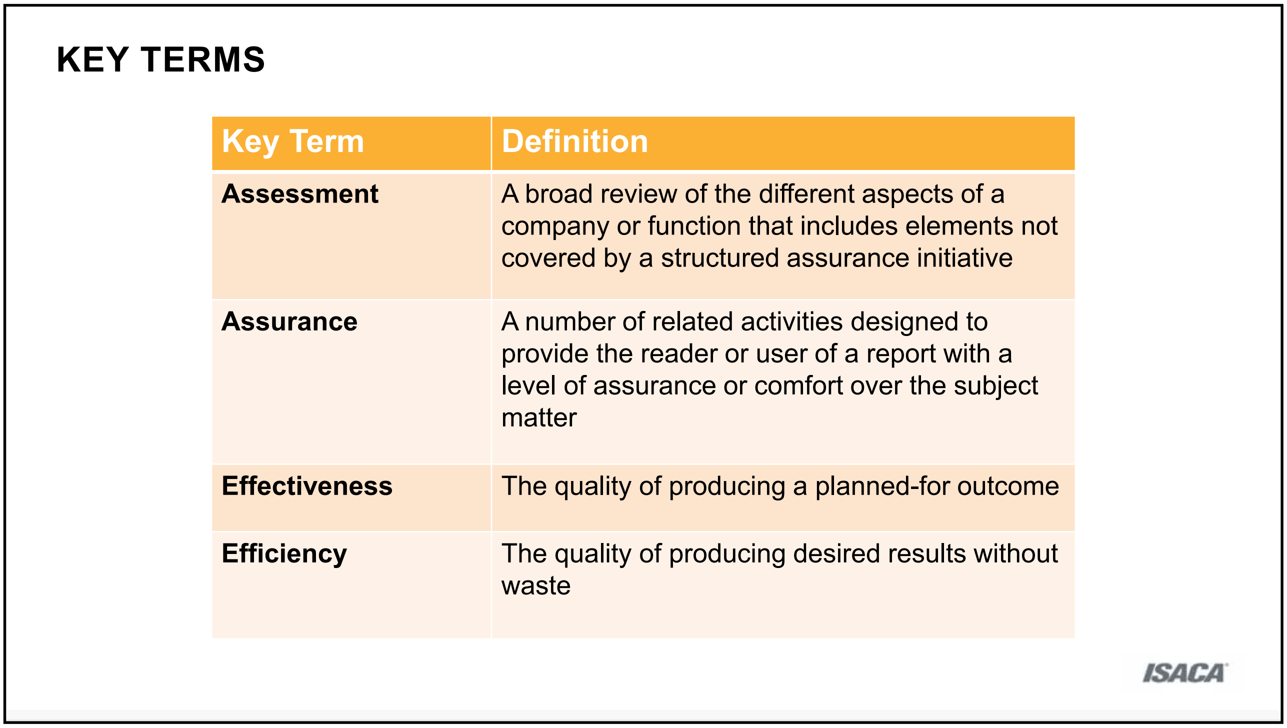
FOCUS ON TASK 4.5



Input:
KPIs; data from control environment

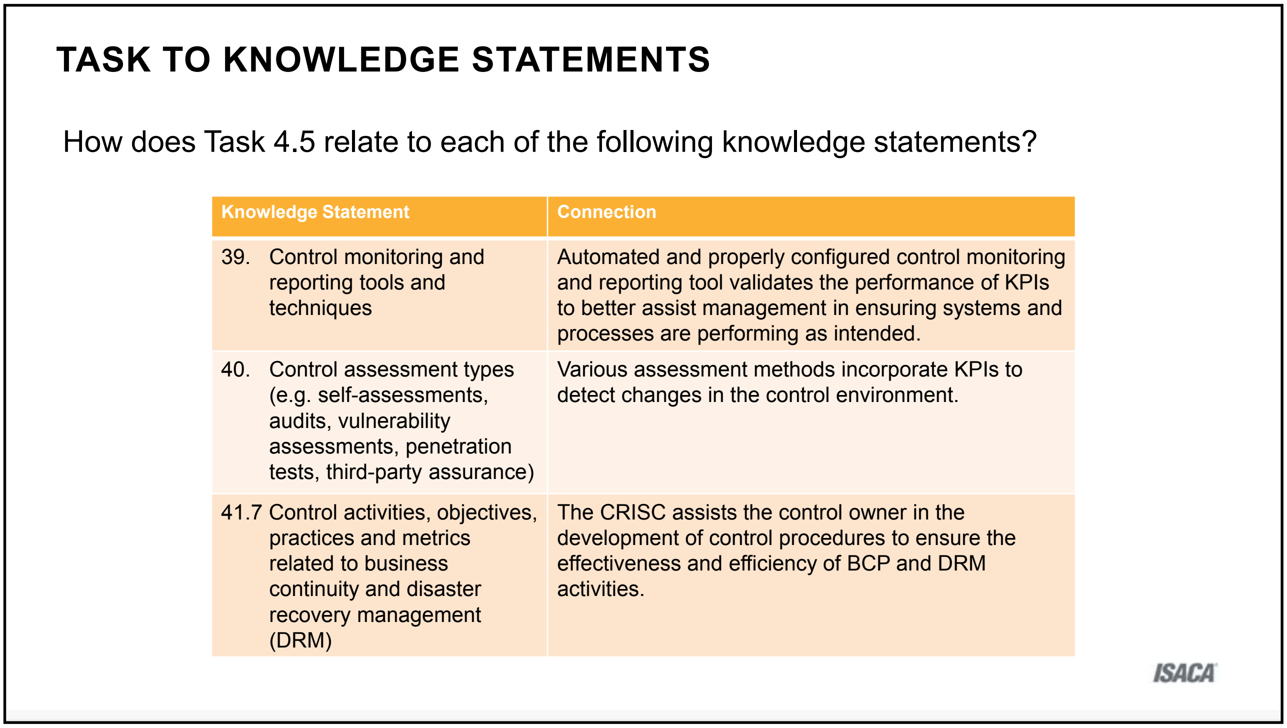
Process:
Identify changes or trends related to the control environment

Output:
Determine efficiency and effectiveness of controls



KEY TERMS

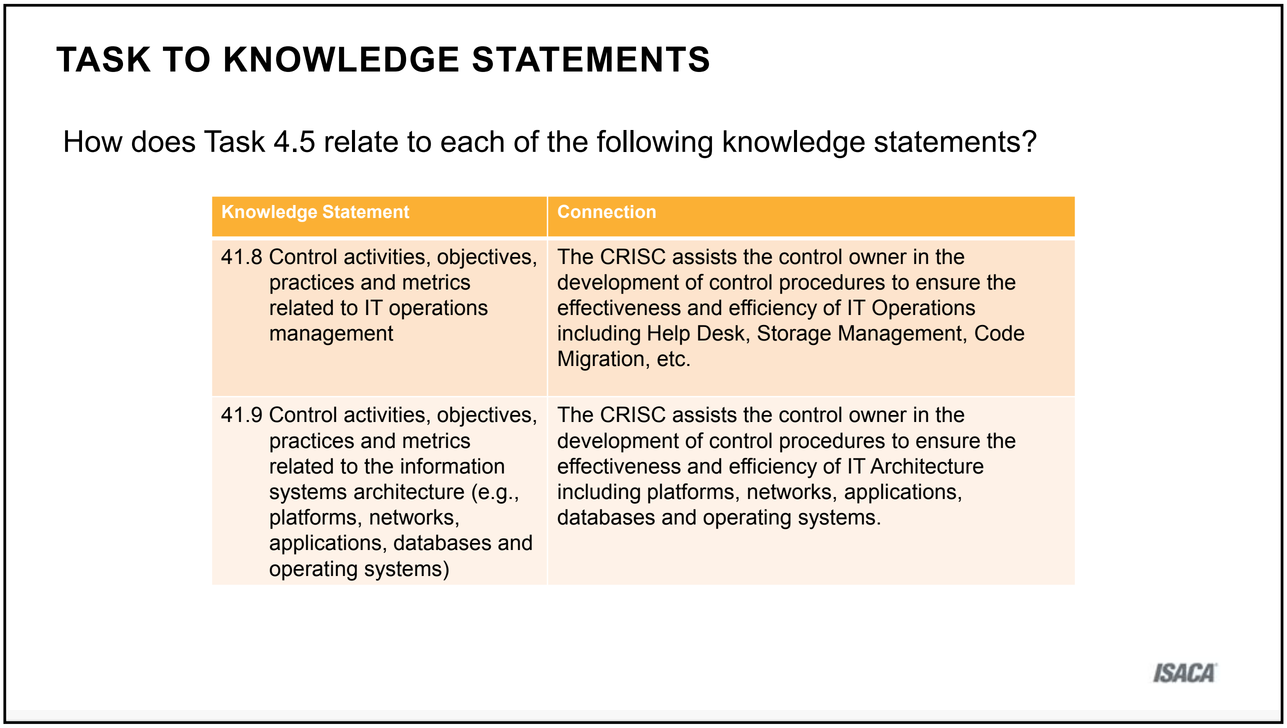
Key Term	Definition
Assessment	A broad review of the different aspects of a company or function that includes elements not covered by a structured assurance initiative
Assurance	A number of related activities designed to provide the reader or user of a report with a level of assurance or comfort over the subject matter
Effectiveness	The quality of producing a planned-for outcome
Efficiency	The quality of producing desired results without waste



TASK TO KNOWLEDGE STATEMENTS

How does Task 4.5 relate to each of the following knowledge statements?

Knowledge Statement	Connection
39. Control monitoring and reporting tools and techniques	Automated and properly configured control monitoring and reporting tool validates the performance of KPIs to better assist management in ensuring systems and processes are performing as intended.
40. Control assessment types (e.g. self-assessments, audits, vulnerability assessments, penetration tests, third-party assurance)	Various assessment methods incorporate KPIs to detect changes in the control environment.
41.7 Control activities, objectives, practices and metrics related to business continuity and disaster recovery management (DRM)	The CRISC assists the control owner in the development of control procedures to ensure the effectiveness and efficiency of BCP and DRM activities.

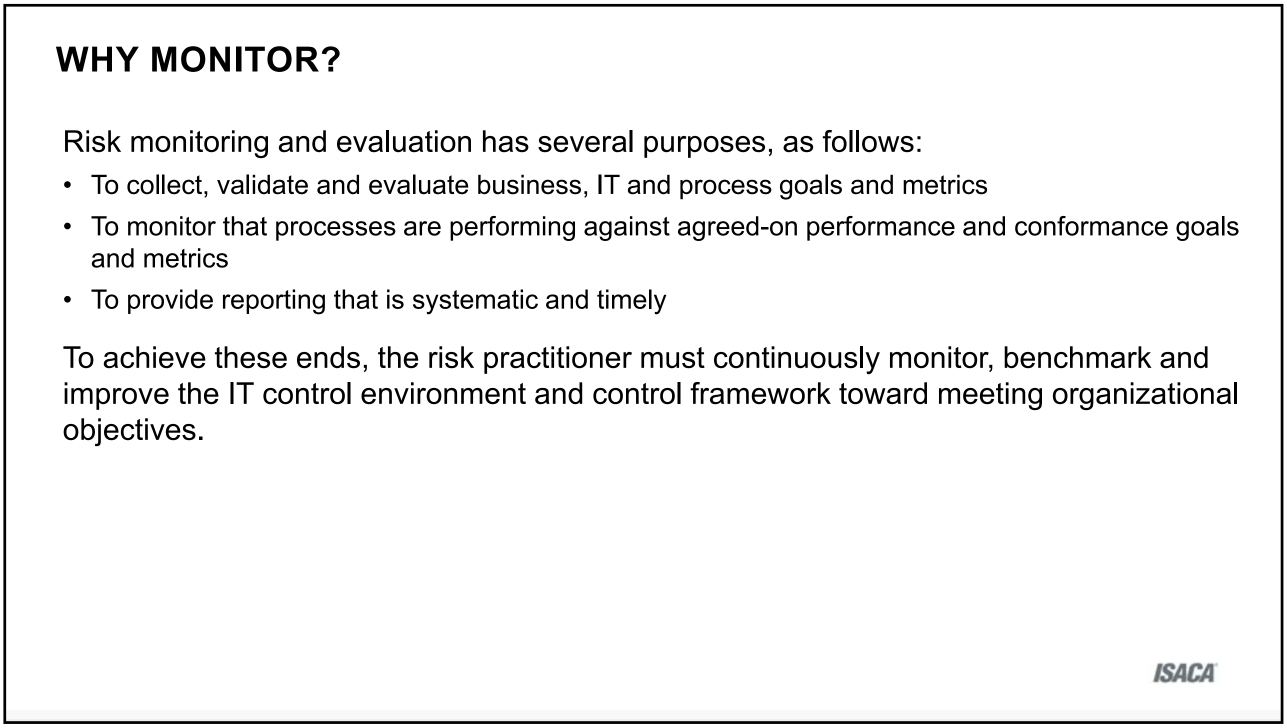


TASK TO KNOWLEDGE STATEMENTS

How does Task 4.5 relate to each of the following knowledge statements?

Knowledge Statement	Connection
41.8 Control activities, objectives, practices and metrics related to IT operations management	The CRISC assists the control owner in the development of control procedures to ensure the effectiveness and efficiency of IT Operations including Help Desk, Storage Management, Code Migration, etc.
41.9 Control activities, objectives, practices and metrics related to the information systems architecture (e.g., platforms, networks, applications, databases and operating systems)	The CRISC assists the control owner in the development of control procedures to ensure the effectiveness and efficiency of IT Architecture including platforms, networks, applications, databases and operating systems.

ISACA

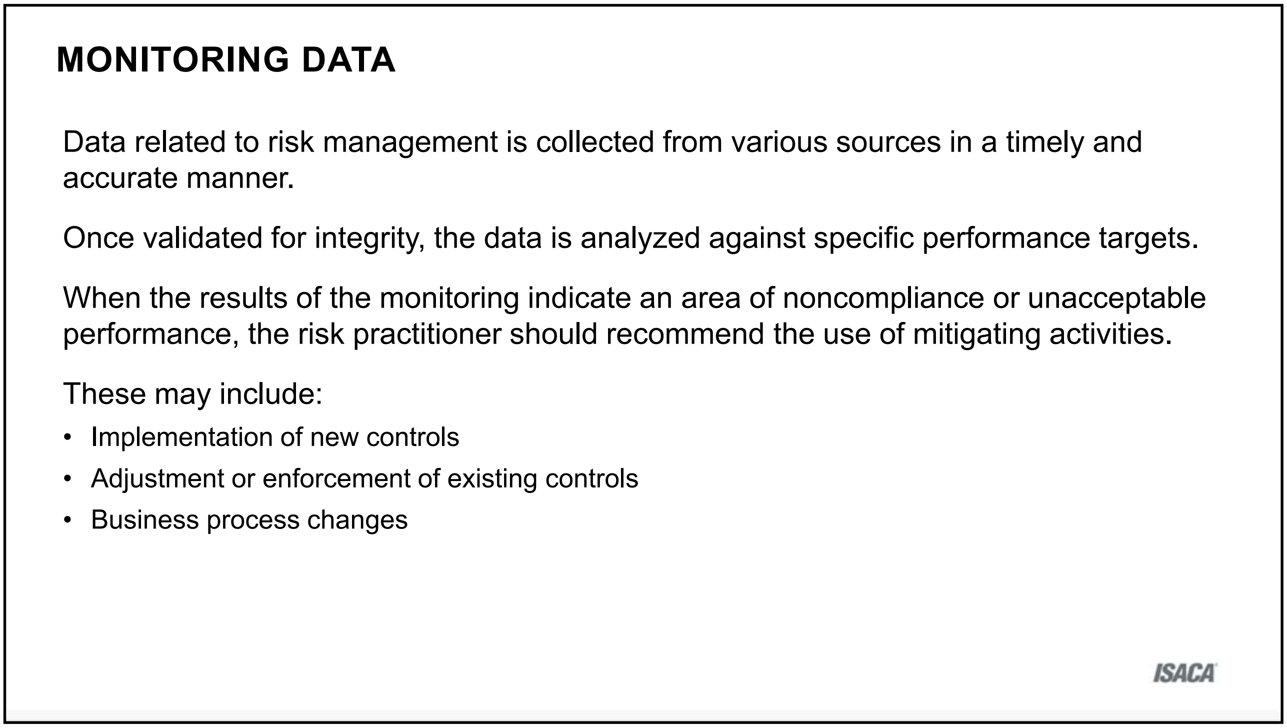


WHY MONITOR?

Risk monitoring and evaluation has several purposes, as follows:

- To collect, validate and evaluate business, IT and process goals and metrics
- To monitor that processes are performing against agreed-on performance and conformance goals and metrics
- To provide reporting that is systematic and timely

To achieve these ends, the risk practitioner must continuously monitor, benchmark and improve the IT control environment and control framework toward meeting organizational objectives.



MONITORING DATA

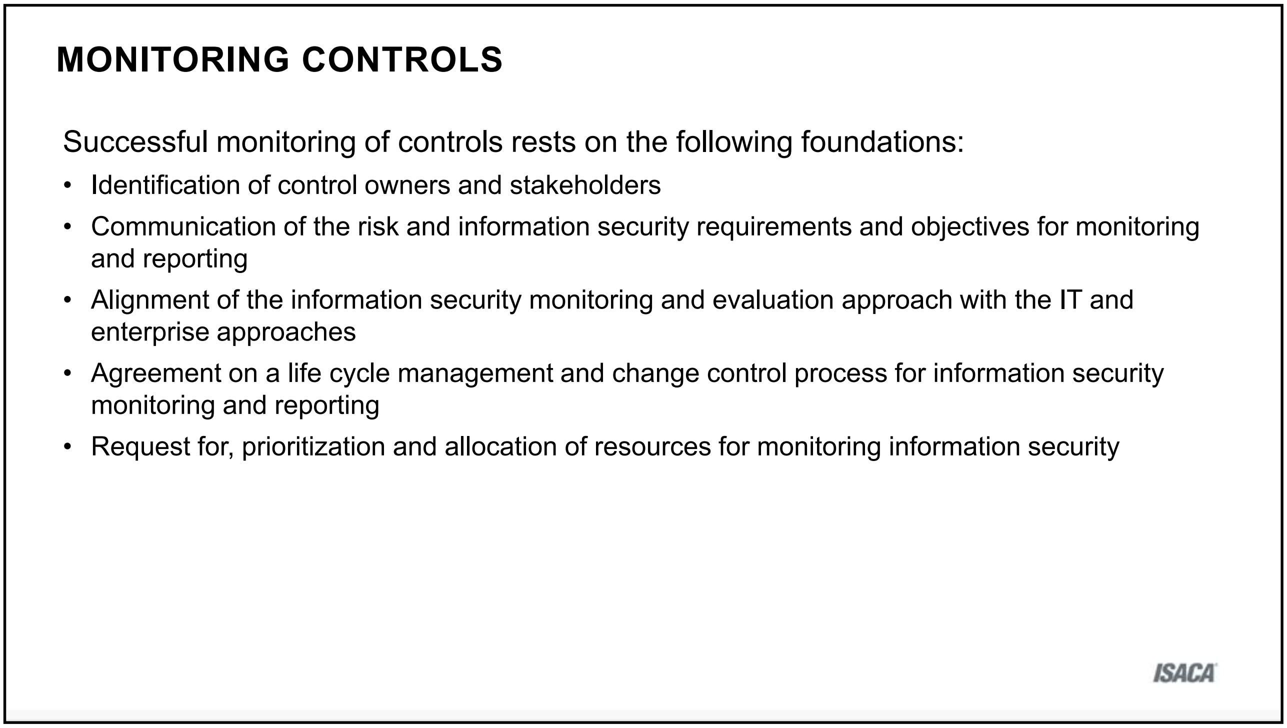
Data related to risk management is collected from various sources in a timely and accurate manner.

Once validated for integrity, the data is analyzed against specific performance targets.

When the results of the monitoring indicate an area of noncompliance or unacceptable performance, the risk practitioner should recommend the use of mitigating activities.

These may include:

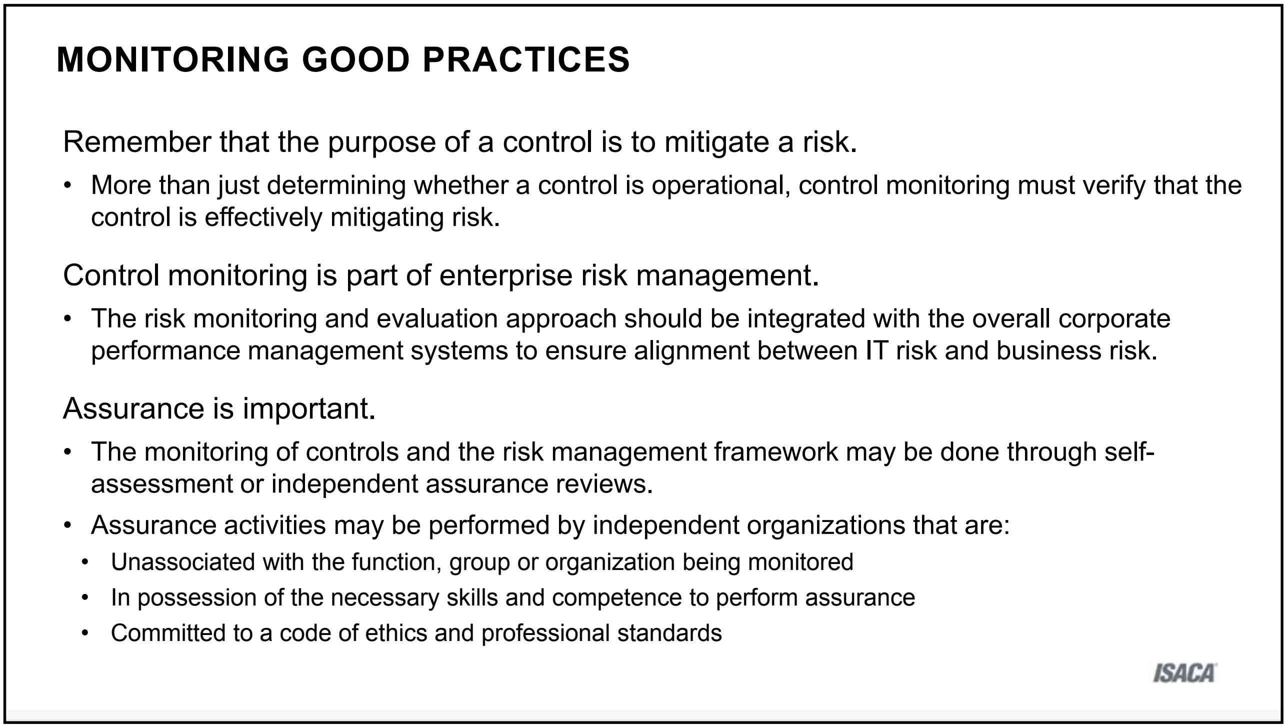
- Implementation of new controls
- Adjustment or enforcement of existing controls
- Business process changes



MONITORING CONTROLS

Successful monitoring of controls rests on the following foundations:

- Identification of control owners and stakeholders
- Communication of the risk and information security requirements and objectives for monitoring and reporting
- Alignment of the information security monitoring and evaluation approach with the IT and enterprise approaches
- Agreement on a life cycle management and change control process for information security monitoring and reporting
- Request for, prioritization and allocation of resources for monitoring information security



MONITORING GOOD PRACTICES

Remember that the purpose of a control is to mitigate a risk.

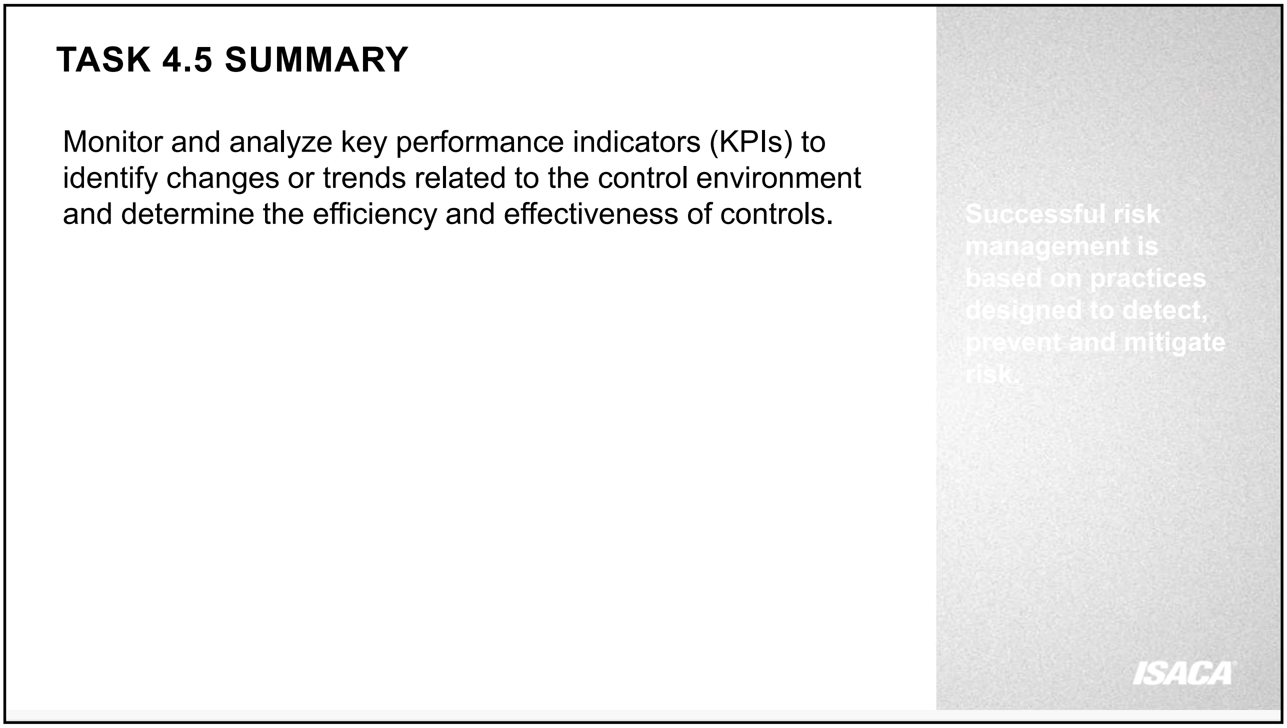
- More than just determining whether a control is operational, control monitoring must verify that the control is effectively mitigating risk.

Control monitoring is part of enterprise risk management.

- The risk monitoring and evaluation approach should be integrated with the overall corporate performance management systems to ensure alignment between IT risk and business risk.

Assurance is important.

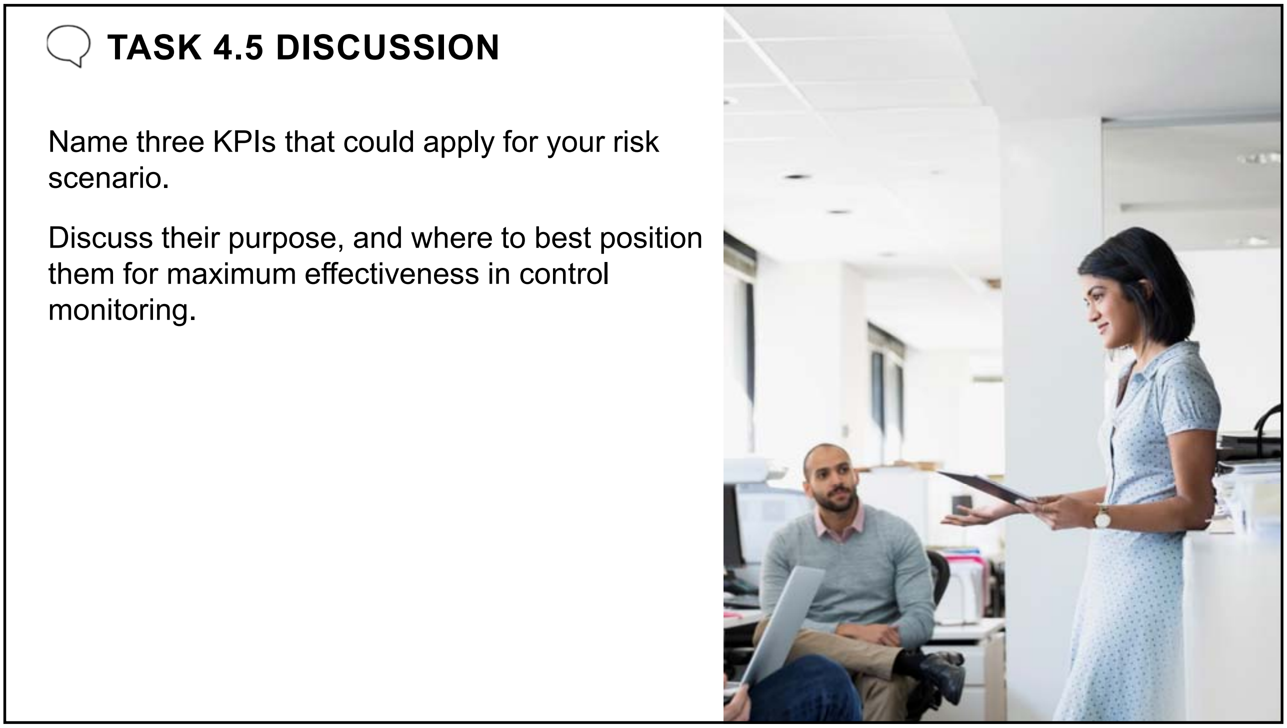
- The monitoring of controls and the risk management framework may be done through self-assessment or independent assurance reviews.
- Assurance activities may be performed by independent organizations that are:
  - Unassociated with the function, group or organization being monitored
  - In possession of the necessary skills and competence to perform assurance
  - Committed to a code of ethics and professional standards



TASK 4.5 SUMMARY

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.

Successful risk management is based on practices designed to detect, prevent and mitigate risk.



TASK 4.5 DISCUSSION

Name three KPIs that could apply for your risk scenario.

Discuss their purpose, and where to best position them for maximum effectiveness in control monitoring.

DISCUSSION QUESTION

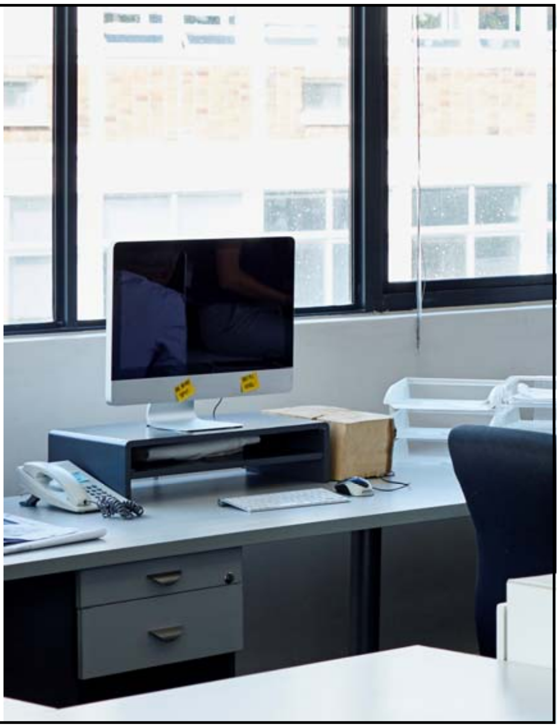
What is the MOST important reason for periodically testing controls?

A. To meet regulatory requirements

B. To meet due care requirements

C. To ensure that control objectives are met

D. To achieve compliance with standard policy



DISCUSSION QUESTION

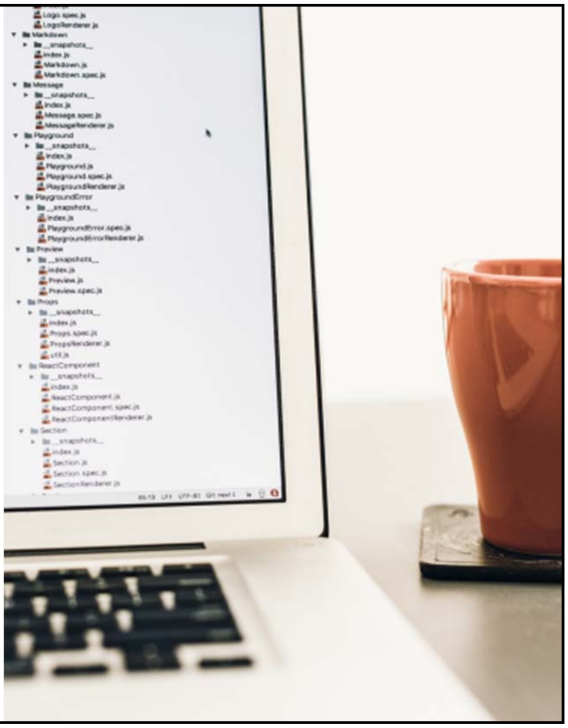
After a risk assessment study, a bank with global operations decided to continue doing business in certain regions of the world where identity theft is widespread. To MOST effectively deal with the risk, the business should:

A. implement monitoring techniques to detect and react to potential fraud.

B. make the customer liable for losses if the customer fails to follow the bank's advice.

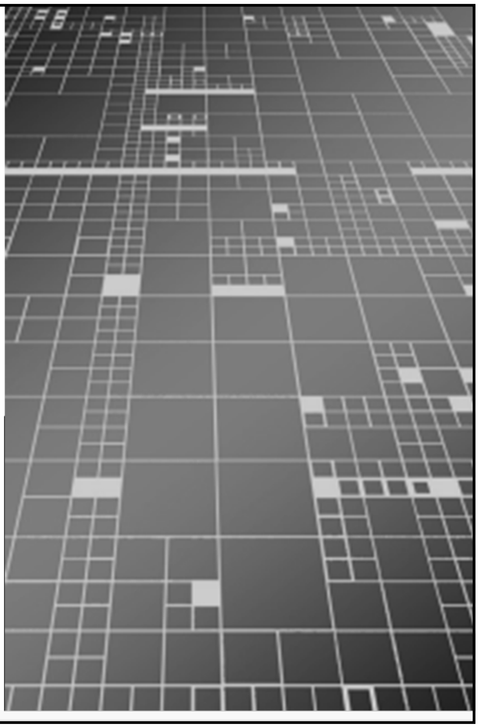
C. increase its customer awareness efforts in those regions.

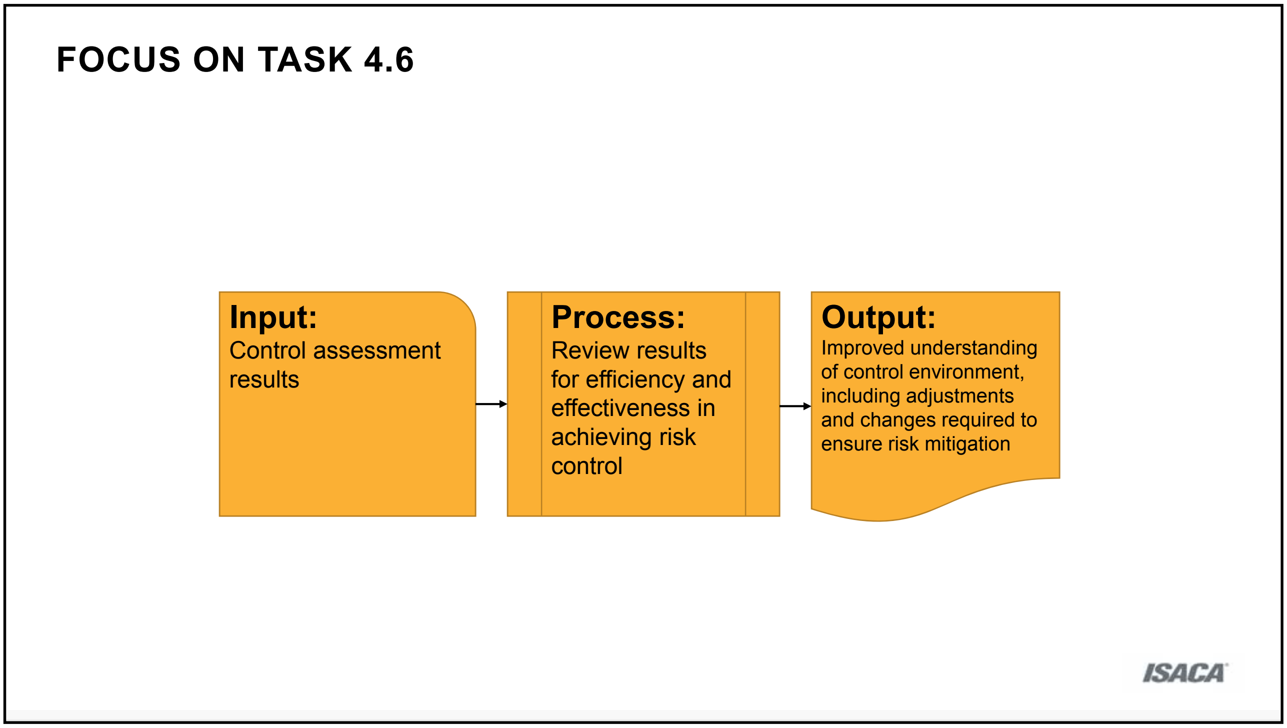
D. outsource credit card processing to a third party.



TASK 4.6

Review the results of control assessments to determine the effectiveness of the control environment.



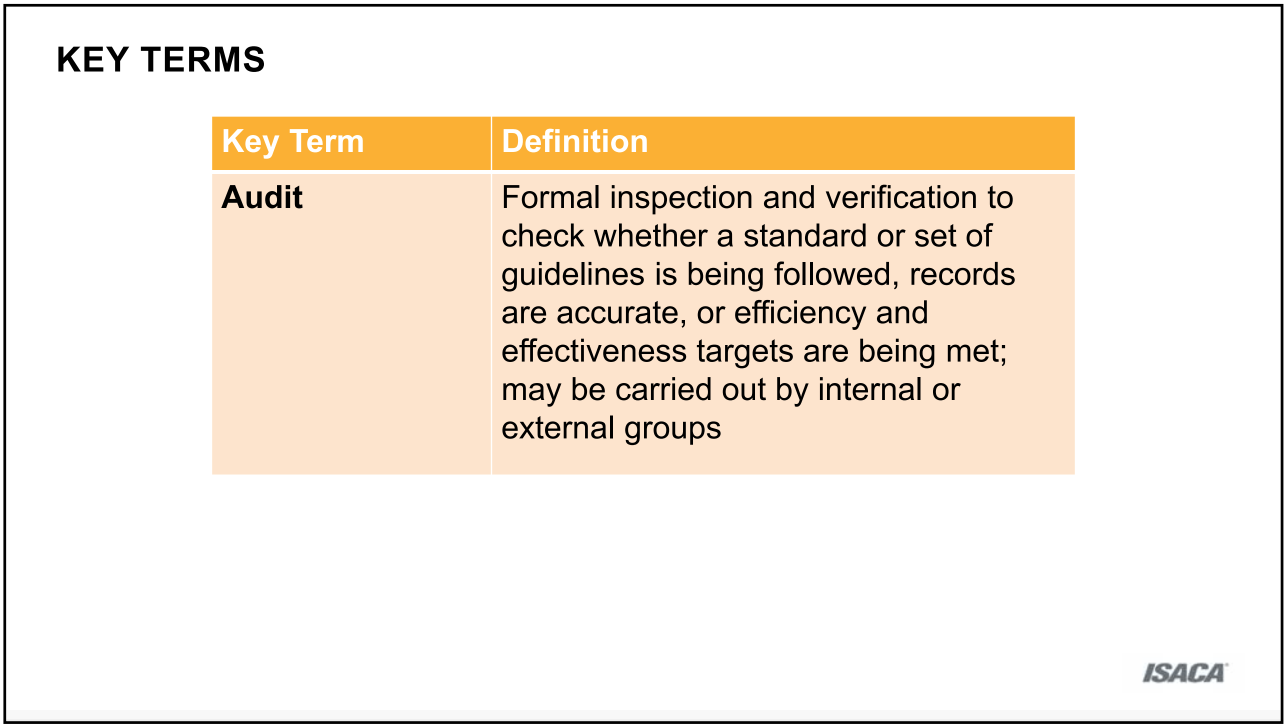


FOCUS ON TASK 4.6

Input:
Control assessment results

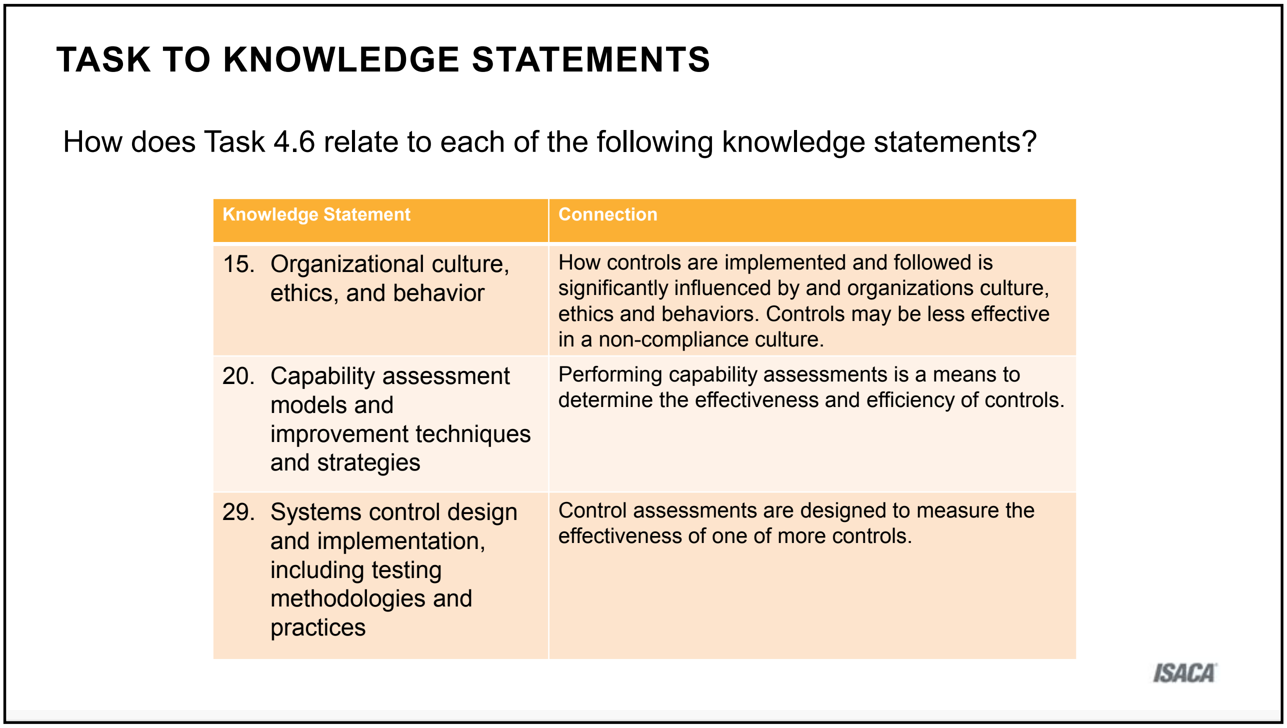
Process:
Review results for efficiency and effectiveness in achieving risk control

Output:
Improved understanding of control environment, including adjustments and changes required to ensure risk mitigation



KEY TERMS

Key Term	Definition
Audit	Formal inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met; may be carried out by internal or external groups

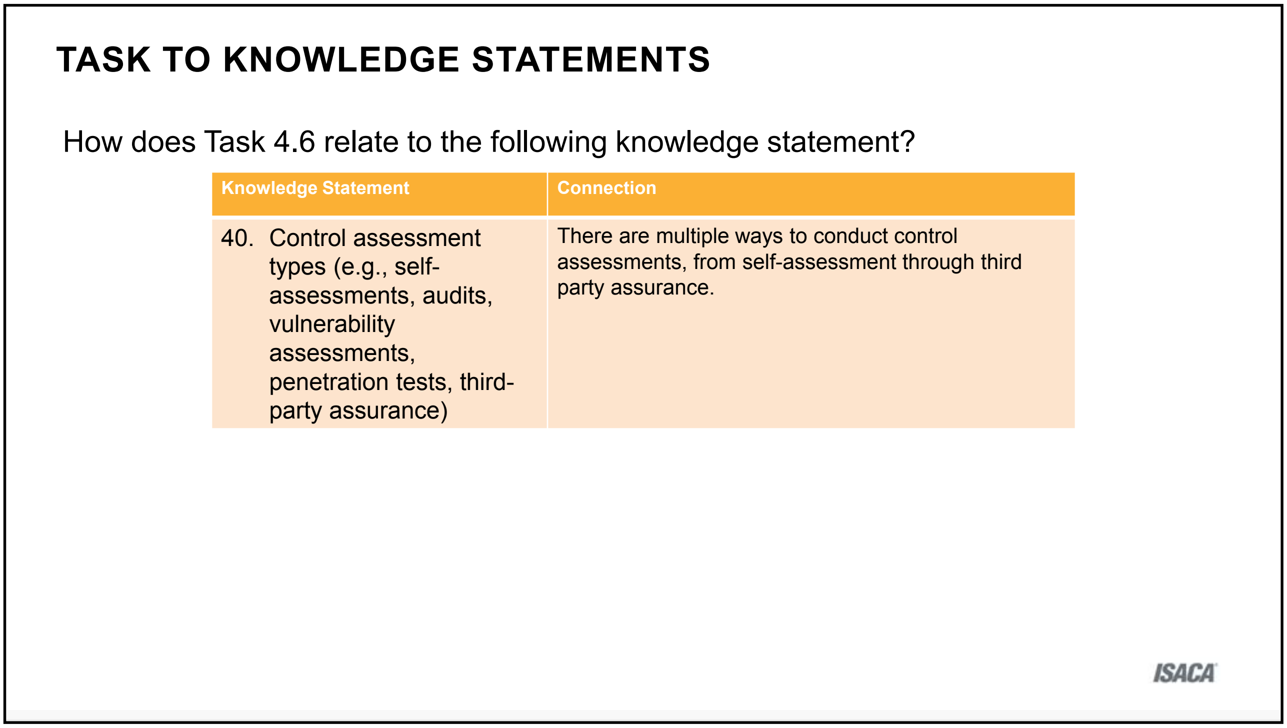


TASK TO KNOWLEDGE STATEMENTS

How does Task 4.6 relate to each of the following knowledge statements?

Knowledge Statement	Connection
15. Organizational culture, ethics, and behavior	How controls are implemented and followed is significantly influenced by and organizations culture, ethics and behaviors. Controls may be less effective in a non-compliance culture.
20. Capability assessment models and improvement techniques and strategies	Performing capability assessments is a means to determine the effectiveness and efficiency of controls.
29. Systems control design and implementation, including testing methodologies and practices	Control assessments are designed to measure the effectiveness of one of more controls.

ISACA

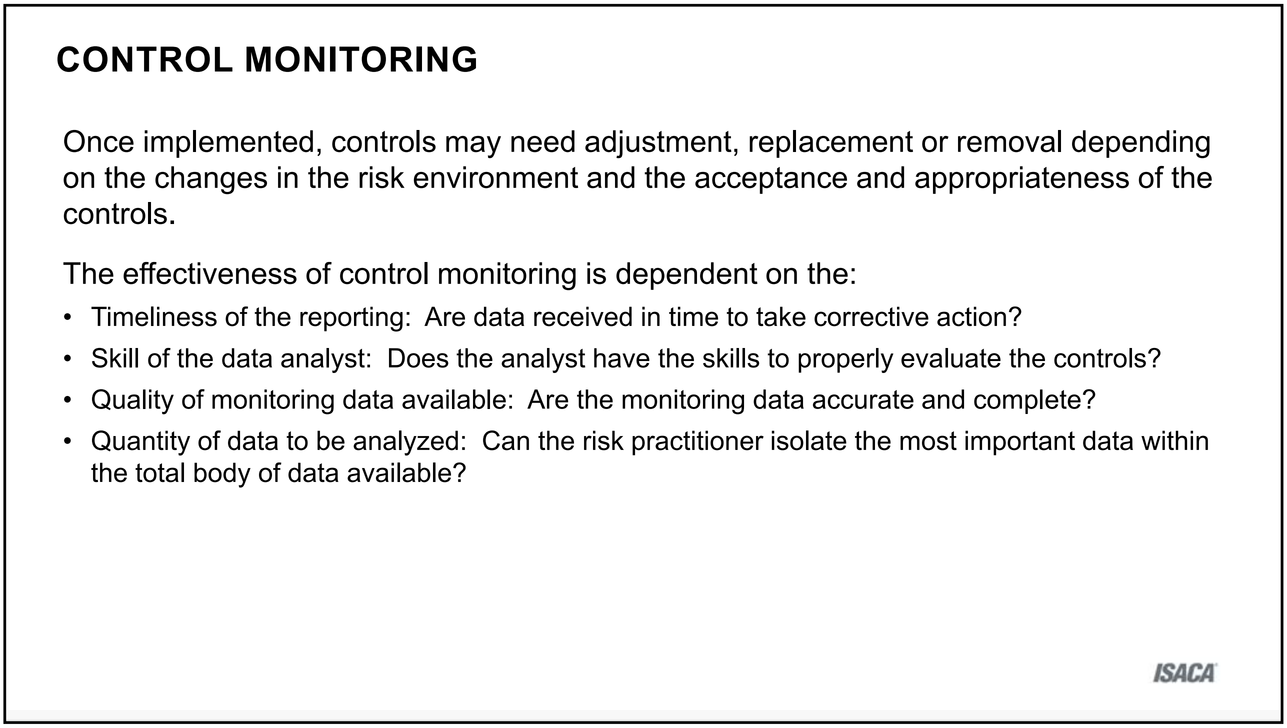


TASK TO KNOWLEDGE STATEMENTS

How does Task 4.6 relate to the following knowledge statement?

Knowledge Statement	Connection
40. Control assessment types (e.g., self-assessments, audits, vulnerability assessments, penetration tests, third-party assurance)	There are multiple ways to conduct control assessments, from self-assessment through third party assurance.

ISACA

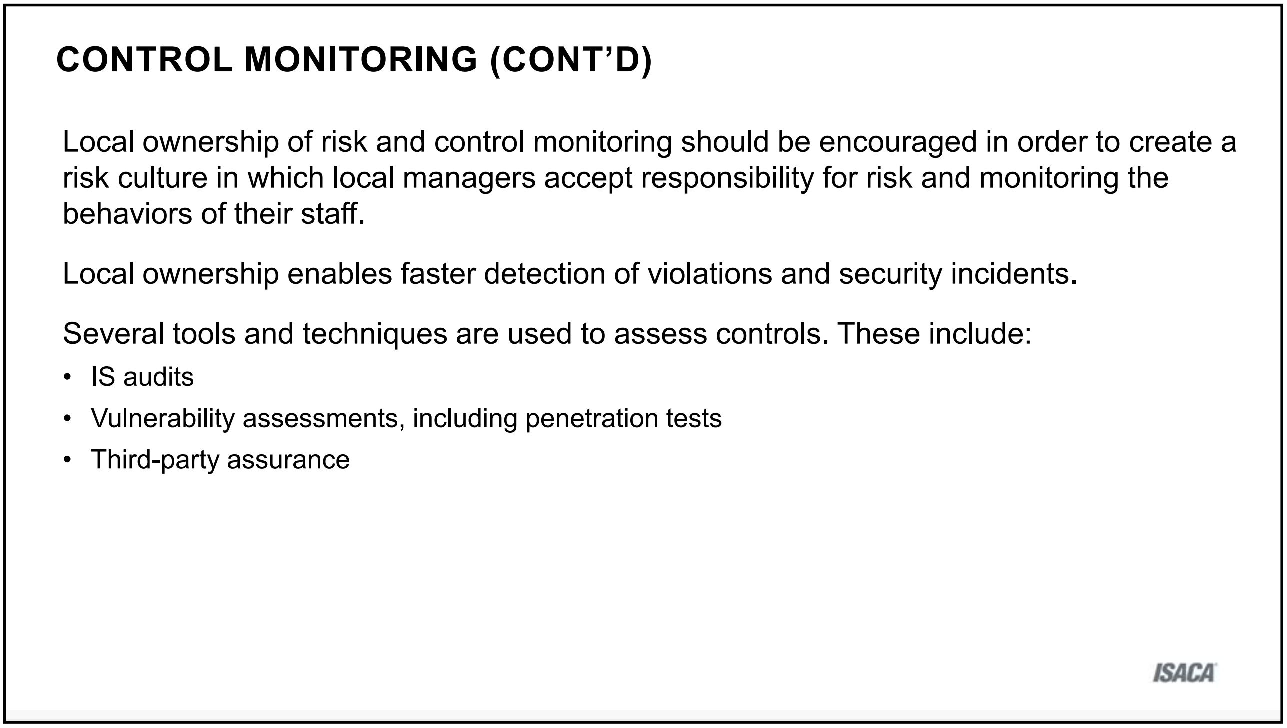


CONTROL MONITORING

Once implemented, controls may need adjustment, replacement or removal depending on the changes in the risk environment and the acceptance and appropriateness of the controls.

The effectiveness of control monitoring is dependent on the:

- Timeliness of the reporting: Are data received in time to take corrective action?
- Skill of the data analyst: Does the analyst have the skills to properly evaluate the controls?
- Quality of monitoring data available: Are the monitoring data accurate and complete?
- Quantity of data to be analyzed: Can the risk practitioner isolate the most important data within the total body of data available?



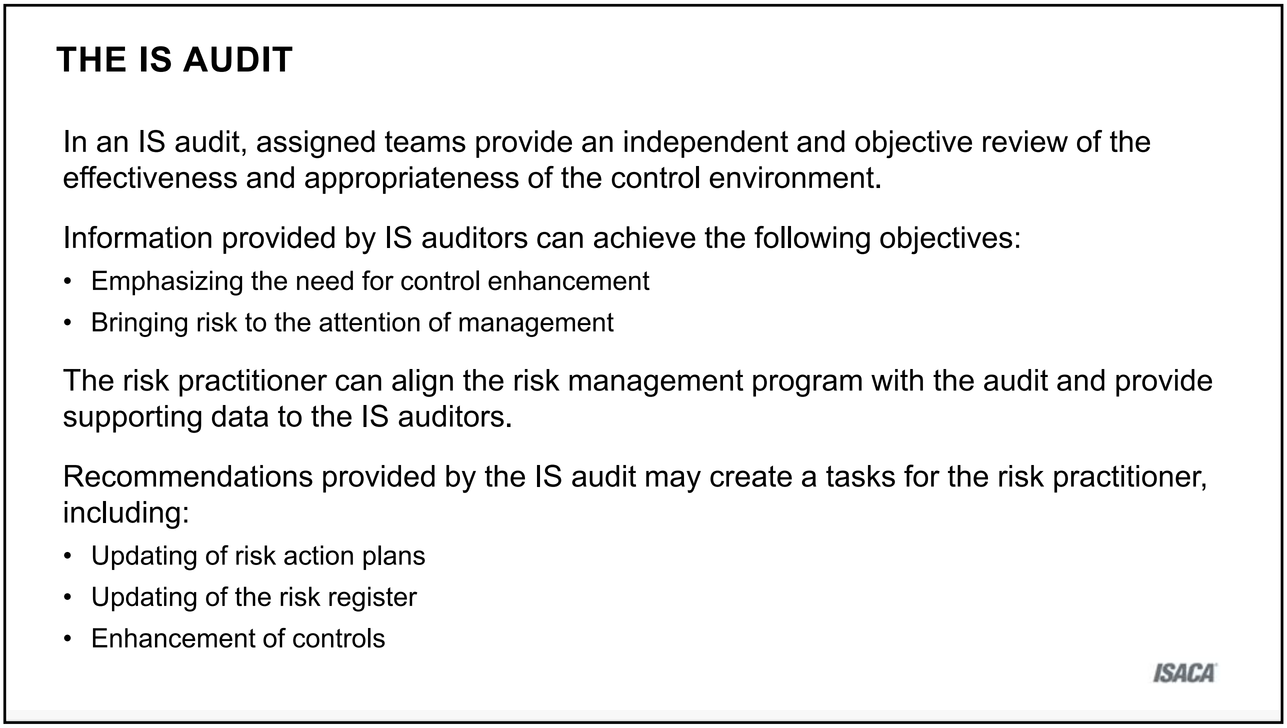
CONTROL MONITORING (CONT’D)

Local ownership of risk and control monitoring should be encouraged in order to create a risk culture in which local managers accept responsibility for risk and monitoring the behaviors of their staff.

Local ownership enables faster detection of violations and security incidents.

Several tools and techniques are used to assess controls. These include:

- IS audits
- Vulnerability assessments, including penetration tests
- Third-party assurance



THE IS AUDIT

In an IS audit, assigned teams provide an independent and objective review of the effectiveness and appropriateness of the control environment.

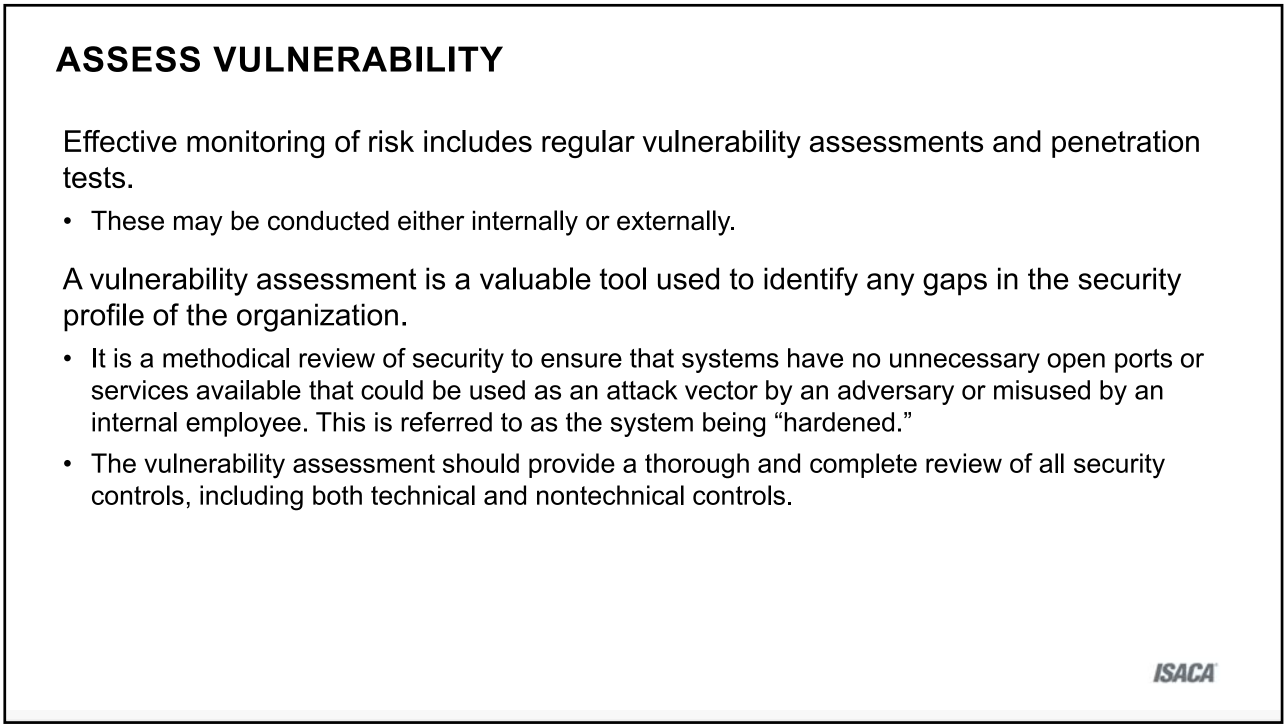
Information provided by IS auditors can achieve the following objectives:

- Emphasizing the need for control enhancement
- Bringing risk to the attention of management

The risk practitioner can align the risk management program with the audit and provide supporting data to the IS auditors.

Recommendations provided by the IS audit may create a tasks for the risk practitioner, including:

- Updating of risk action plans
- Updating of the risk register
- Enhancement of controls



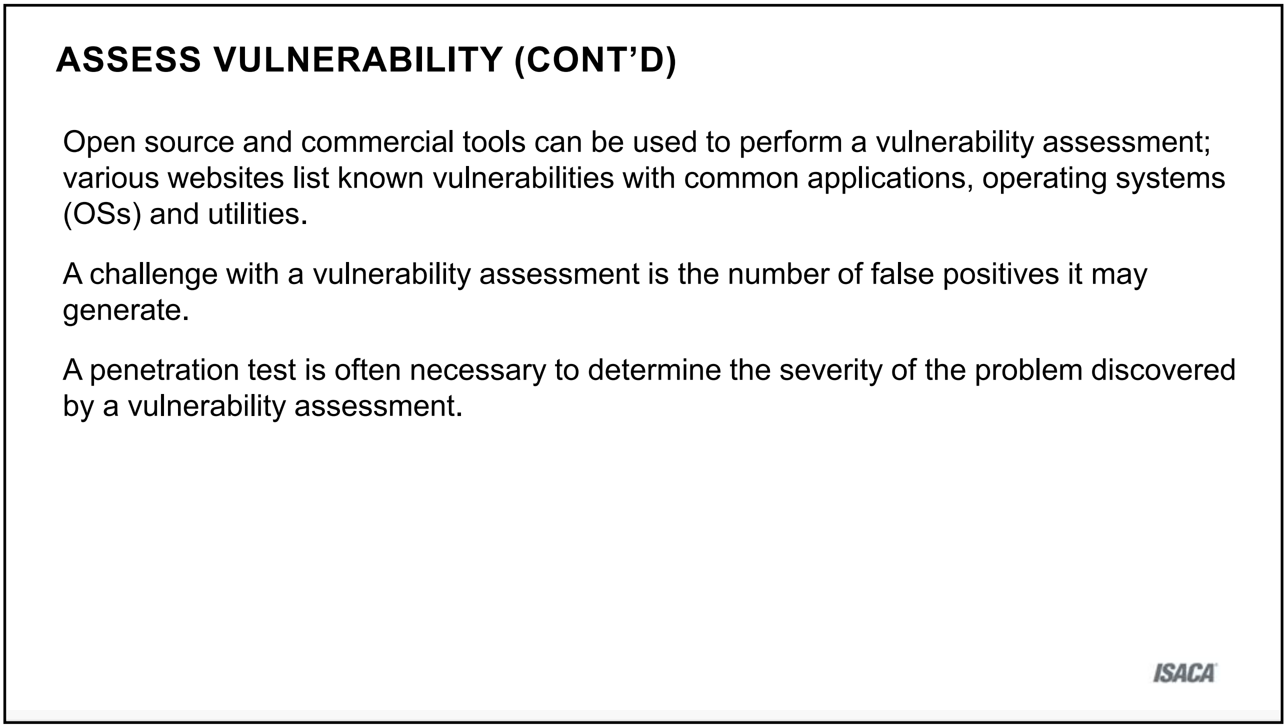
ASSESS VULNERABILITY

Effective monitoring of risk includes regular vulnerability assessments and penetration tests.

- These may be conducted either internally or externally.

A vulnerability assessment is a valuable tool used to identify any gaps in the security profile of the organization.

- It is a methodical review of security to ensure that systems have no unnecessary open ports or services available that could be used as an attack vector by an adversary or misused by an internal employee. This is referred to as the system being “hardened.”
- The vulnerability assessment should provide a thorough and complete review of all security controls, including both technical and nontechnical controls.



ASSESS VULNERABILITY (CONT'D)

Open source and commercial tools can be used to perform a vulnerability assessment; various websites list known vulnerabilities with common applications, operating systems (OSs) and utilities.

A challenge with a vulnerability assessment is the number of false positives it may generate.

A penetration test is often necessary to determine the severity of the problem discovered by a vulnerability assessment.

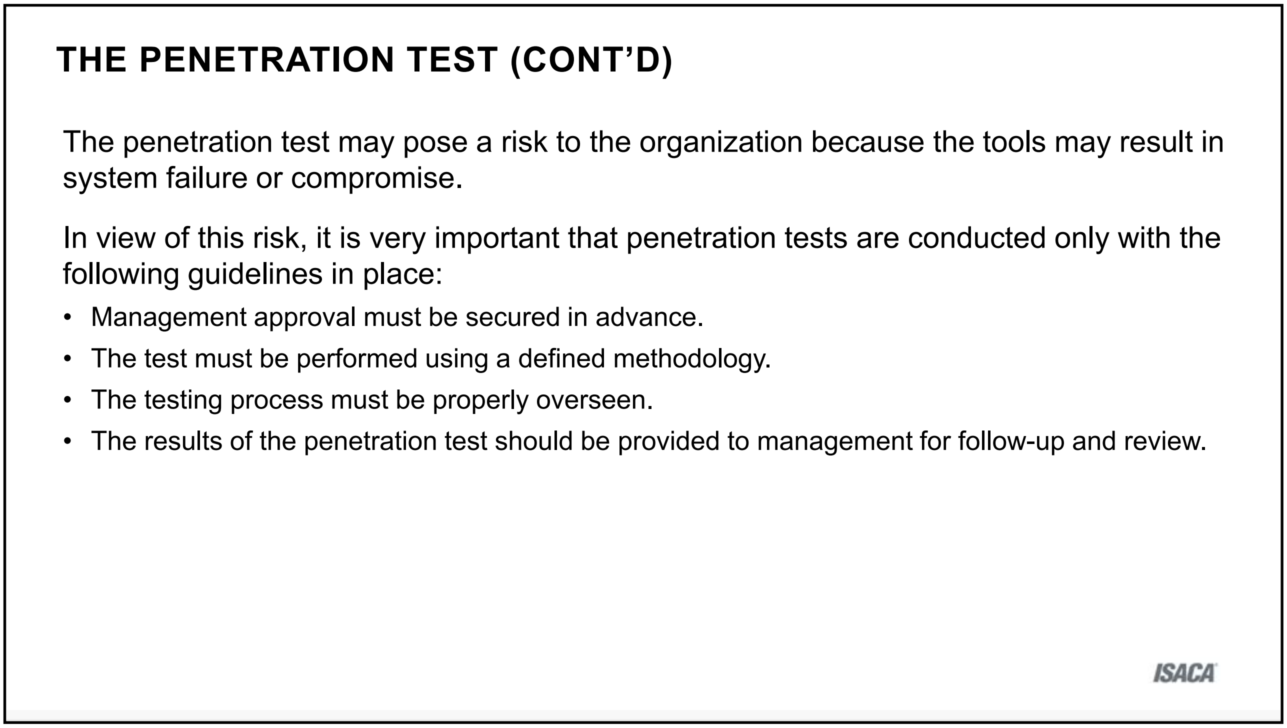
THE PENETRATION TEST

A penetration test is a targeted attempt to break into a system or application, or, in a physical test, to break into a building or secured area.

Using the results of a vulnerability assessment, the tester selects a potential vulnerability and attempts to exploit that vulnerability. The results of this attempt aid in determining the severity of the problem, as follows:

- If the penetration tester is able to break in, then the vulnerability is real and must be mitigated.
- If the tester is unable to break in, then it is likely that the vulnerability does not require mitigation.

Because a penetration tester often uses the same tools used by hackers to try to break into systems the results can be real and meaningful.

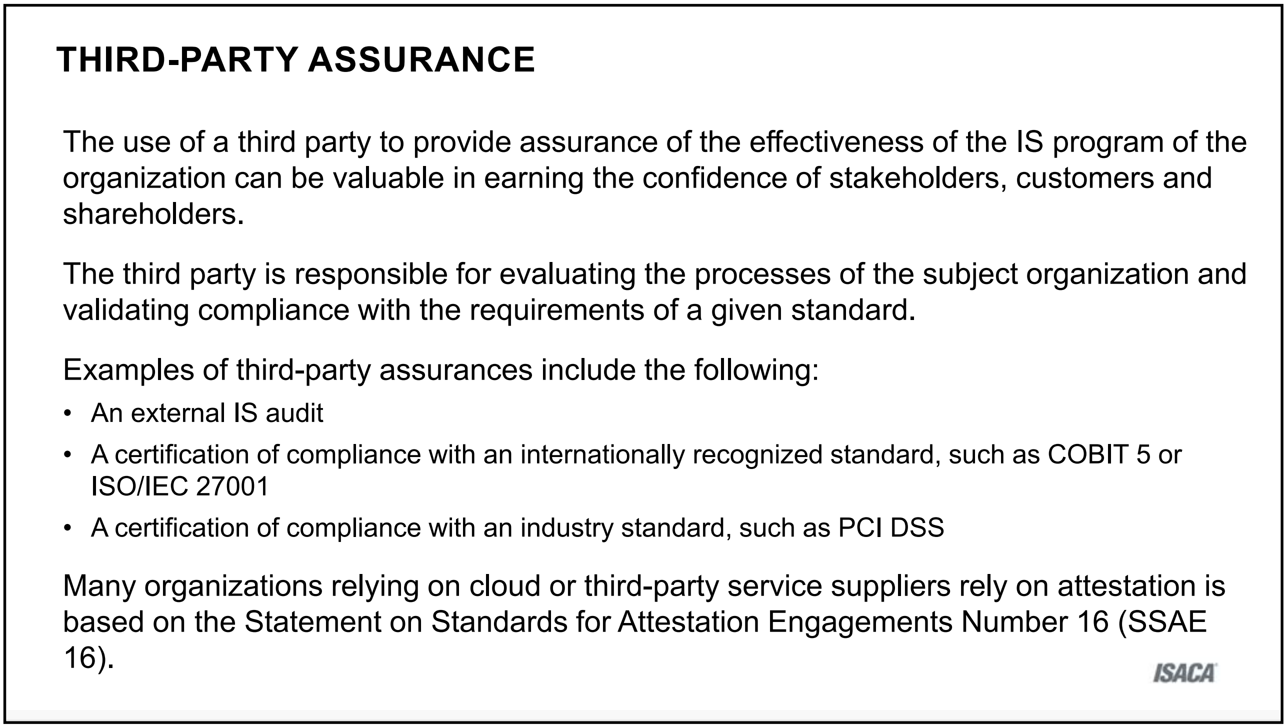


THE PENETRATION TEST (CONT'D)

The penetration test may pose a risk to the organization because the tools may result in system failure or compromise.

In view of this risk, it is very important that penetration tests are conducted only with the following guidelines in place:

- Management approval must be secured in advance.
- The test must be performed using a defined methodology.
- The testing process must be properly overseen.
- The results of the penetration test should be provided to management for follow-up and review.



THIRD-PARTY ASSURANCE

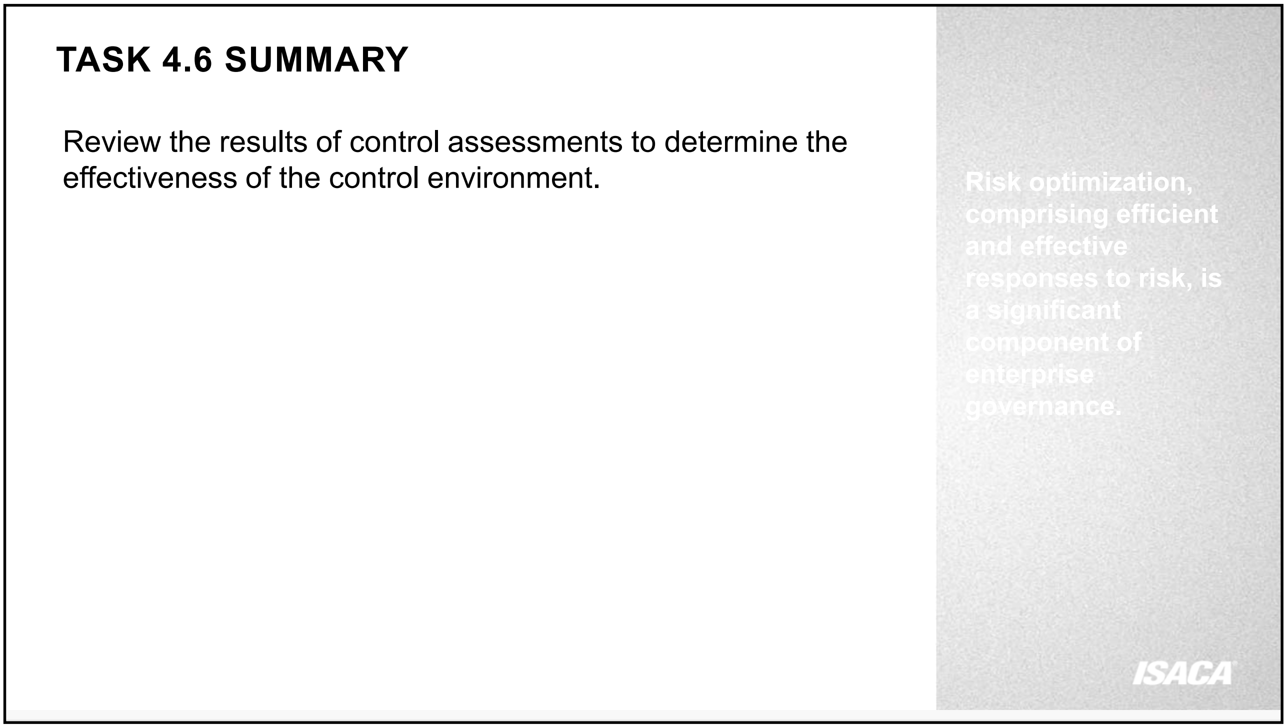
The use of a third party to provide assurance of the effectiveness of the IS program of the organization can be valuable in earning the confidence of stakeholders, customers and shareholders.

The third party is responsible for evaluating the processes of the subject organization and validating compliance with the requirements of a given standard.

Examples of third-party assurances include the following:

- An external IS audit
- A certification of compliance with an internationally recognized standard, such as COBIT 5 or ISO/IEC 27001
- A certification of compliance with an industry standard, such as PCI DSS

Many organizations relying on cloud or third-party service suppliers rely on attestation is based on the Statement on Standards for Attestation Engagements Number 16 (SSAE 16).

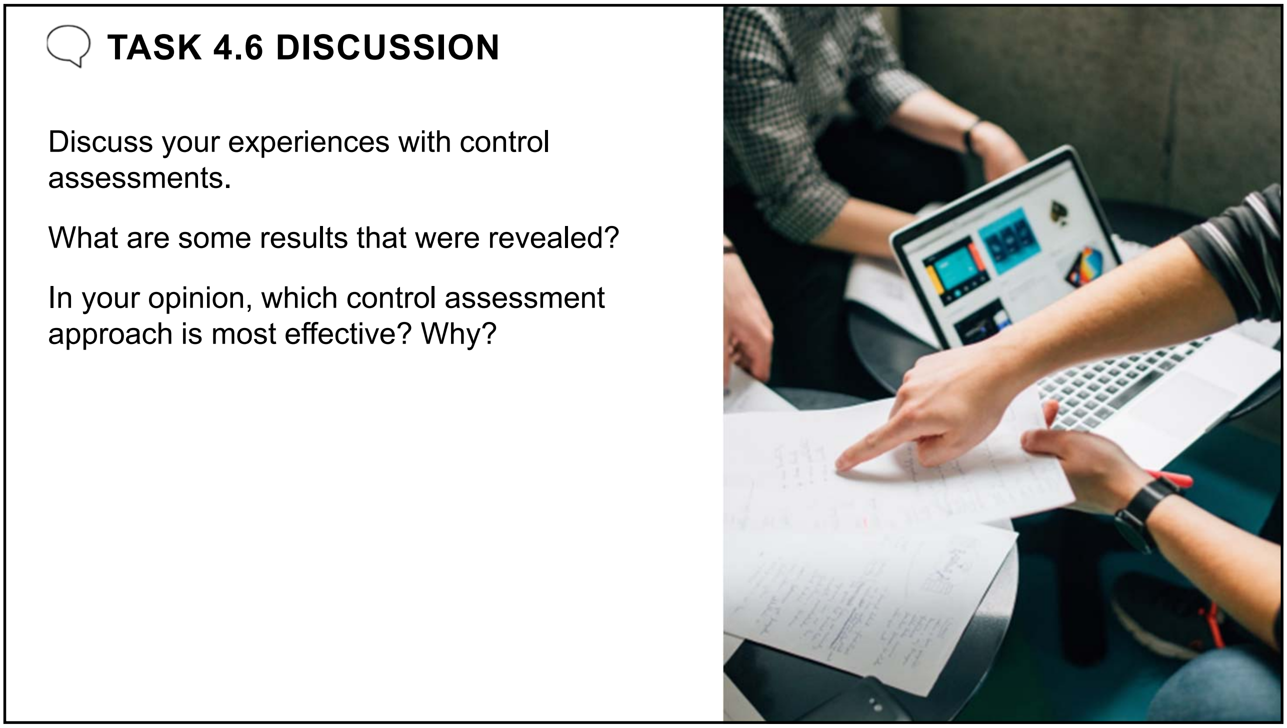


TASK 4.6 SUMMARY

Review the results of control assessments to determine the effectiveness of the control environment.

Risk optimization, comprising efficient and effective responses to risk, is a significant component of enterprise governance.

ISACA



TASK 4.6 DISCUSSION

Discuss your experiences with control assessments.

What are some results that were revealed?

In your opinion, which control assessment approach is most effective? Why?

DISCUSSION QUESTION

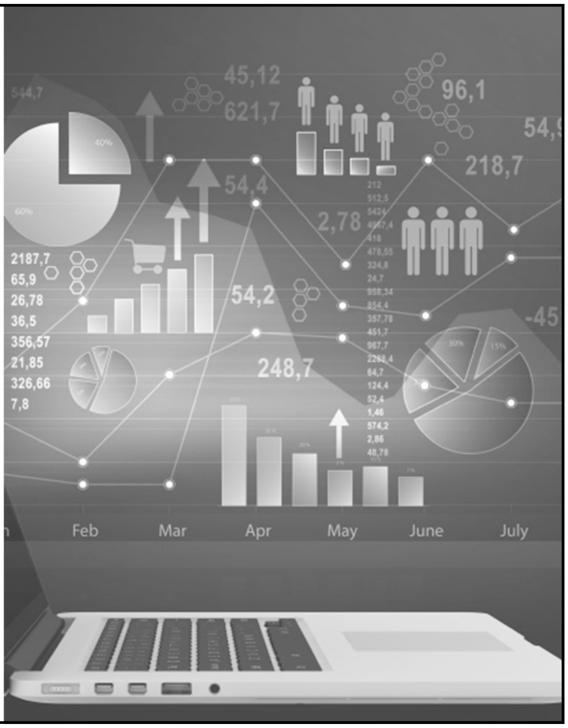
Which of the following MOST effectively ensures that service provider controls are within the guidelines set forth in the organization's information security policy?

A. Service level monitoring

B. Penetration testing

C. Security awareness training

D. Periodic auditing



DISCUSSION QUESTION

What role does the risk professional have in regard to the IS control monitoring process? The risk professional:

A. maintains and operates IS controls.

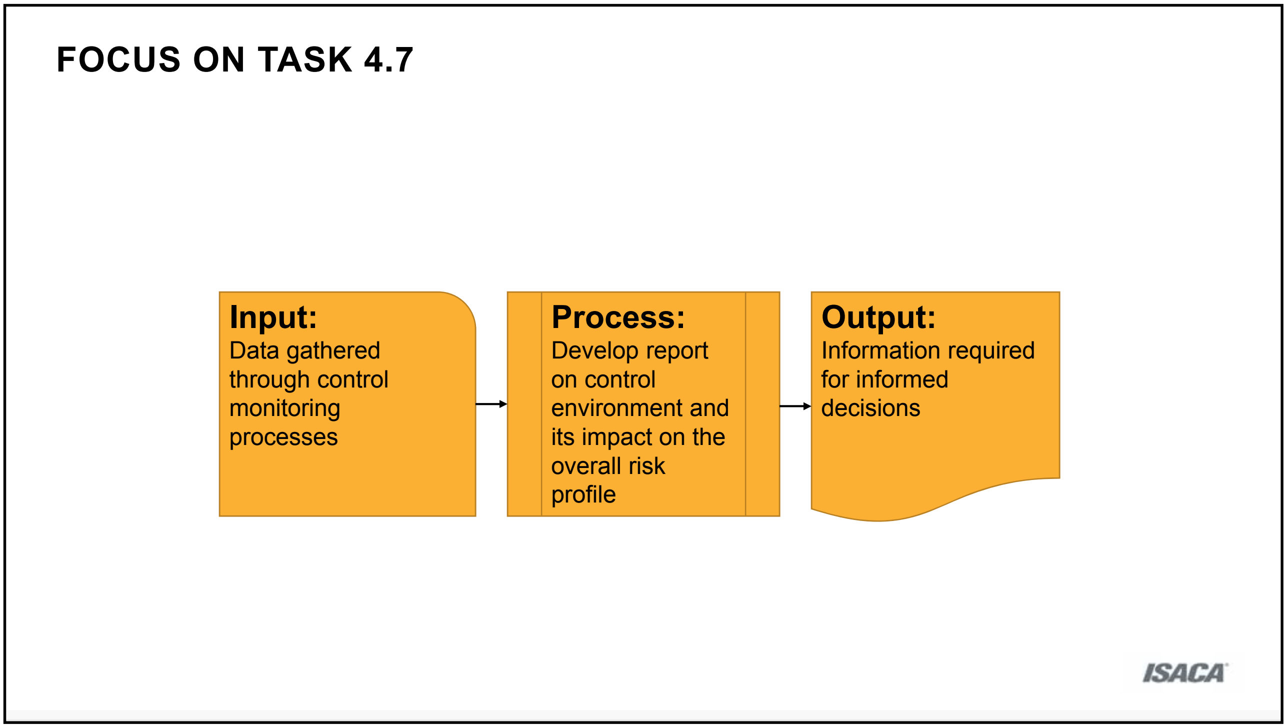
B. approves the policies for IS control monitoring.

C. determines the frequency of control testing by internal audit.

D. assists in planning, reporting and scheduling tests of IS controls.

TASK 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.



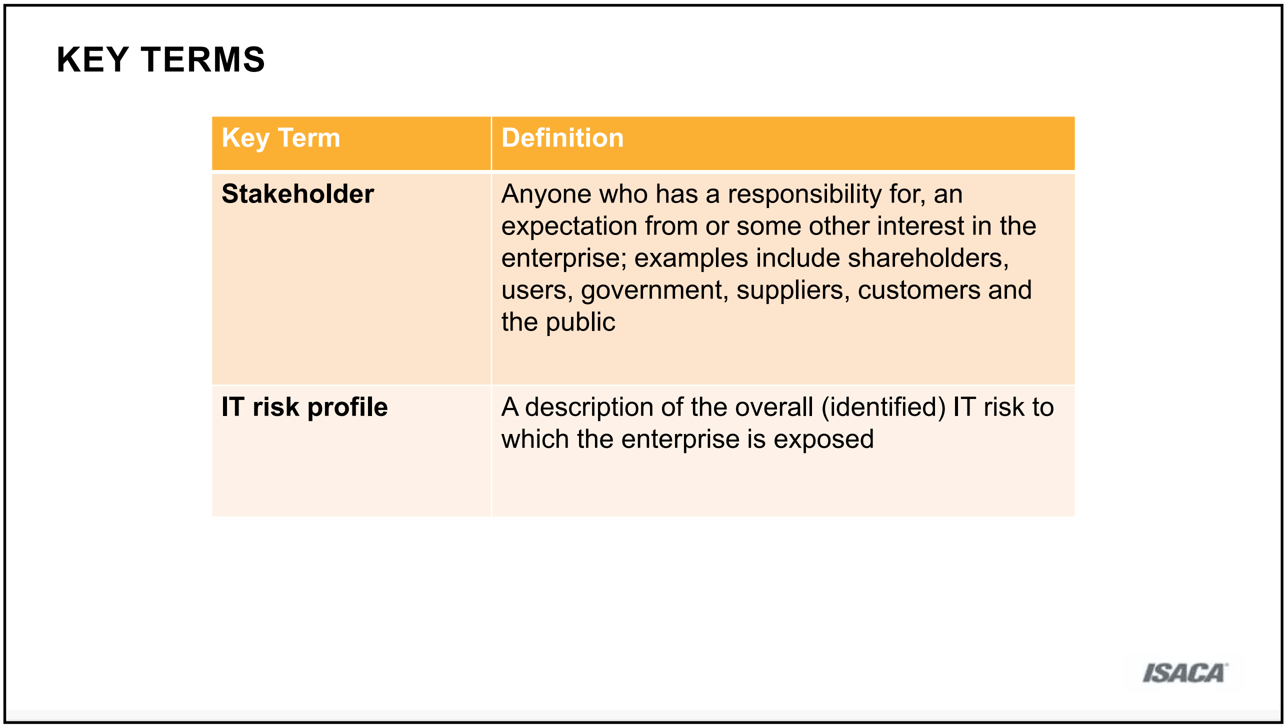
FOCUS ON TASK 4.7

Input:
Data gathered through control monitoring processes

Process:
Develop report on control environment and its impact on the overall risk profile

Output:
Information required for informed decisions

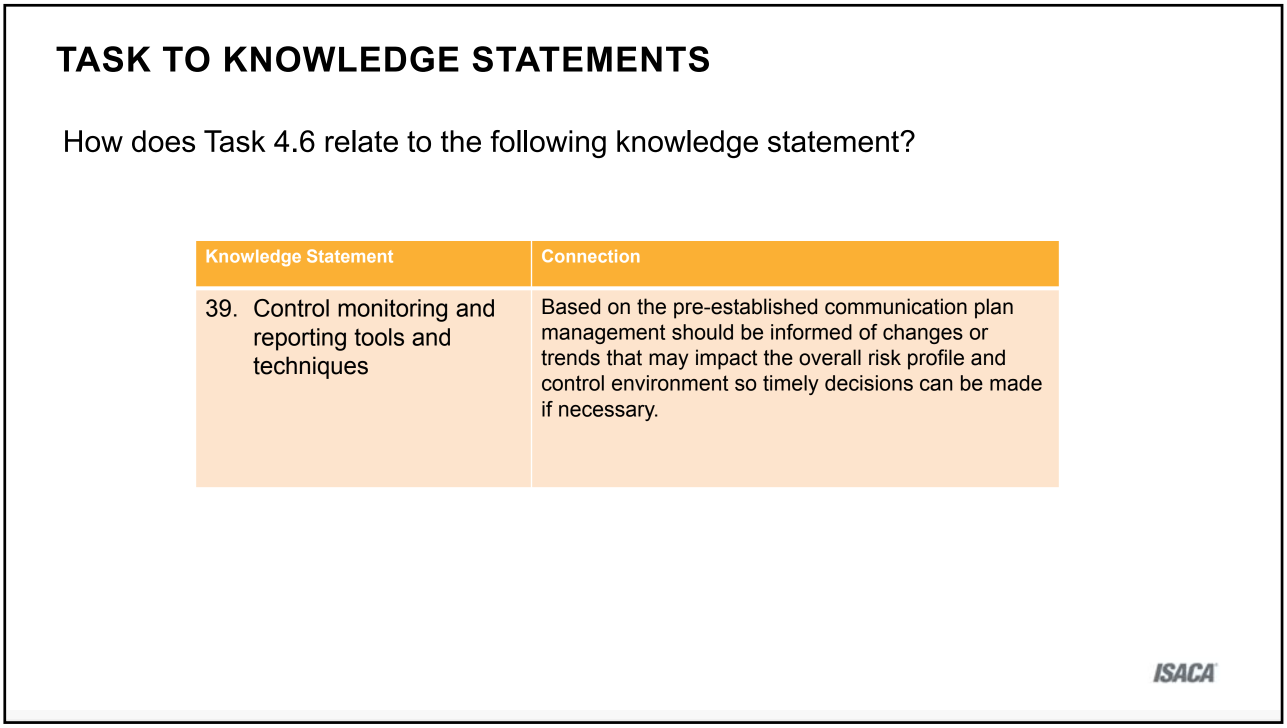
ISACA



KEY TERMS

Key Term	Definition
Stakeholder	Anyone who has a responsibility for, an expectation from or some other interest in the enterprise; examples include shareholders, users, government, suppliers, customers and the public
IT risk profile	A description of the overall (identified) IT risk to which the enterprise is exposed

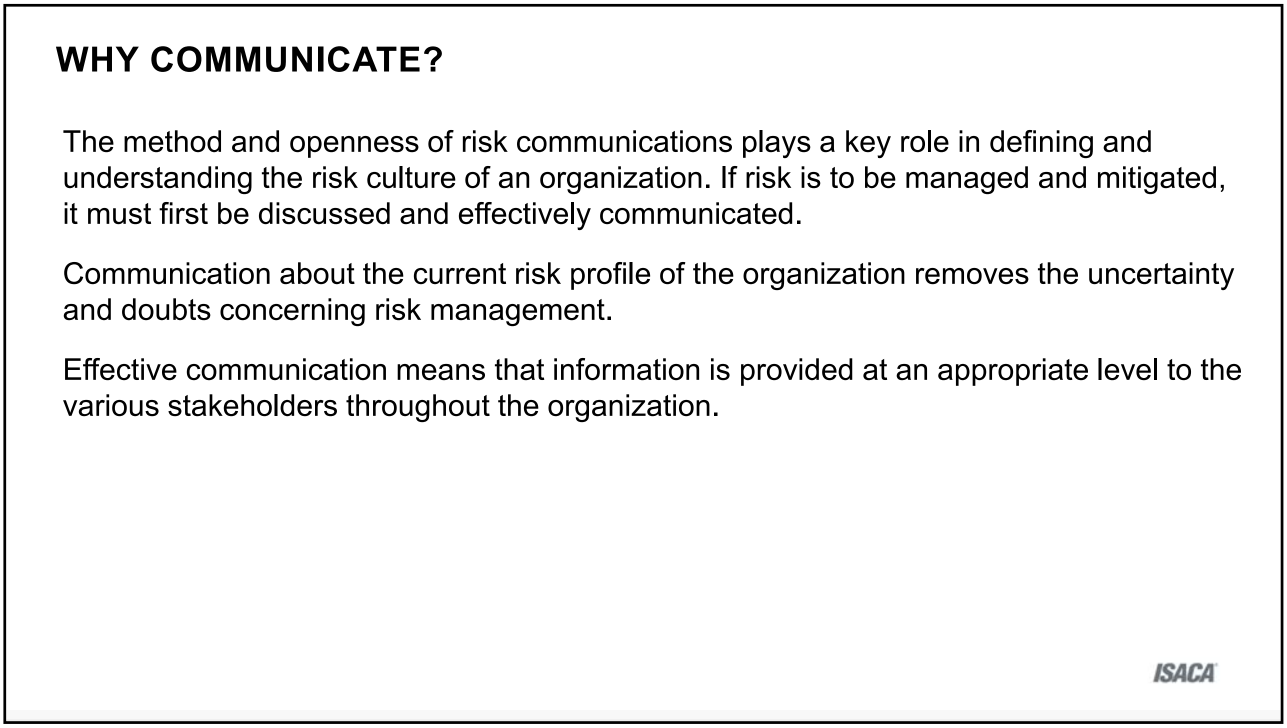
ISACA



TASK TO KNOWLEDGE STATEMENTS

How does Task 4.6 relate to the following knowledge statement?

Knowledge Statement	Connection
39. Control monitoring and reporting tools and techniques	Based on the pre-established communication plan management should be informed of changes or trends that may impact the overall risk profile and control environment so timely decisions can be made if necessary.

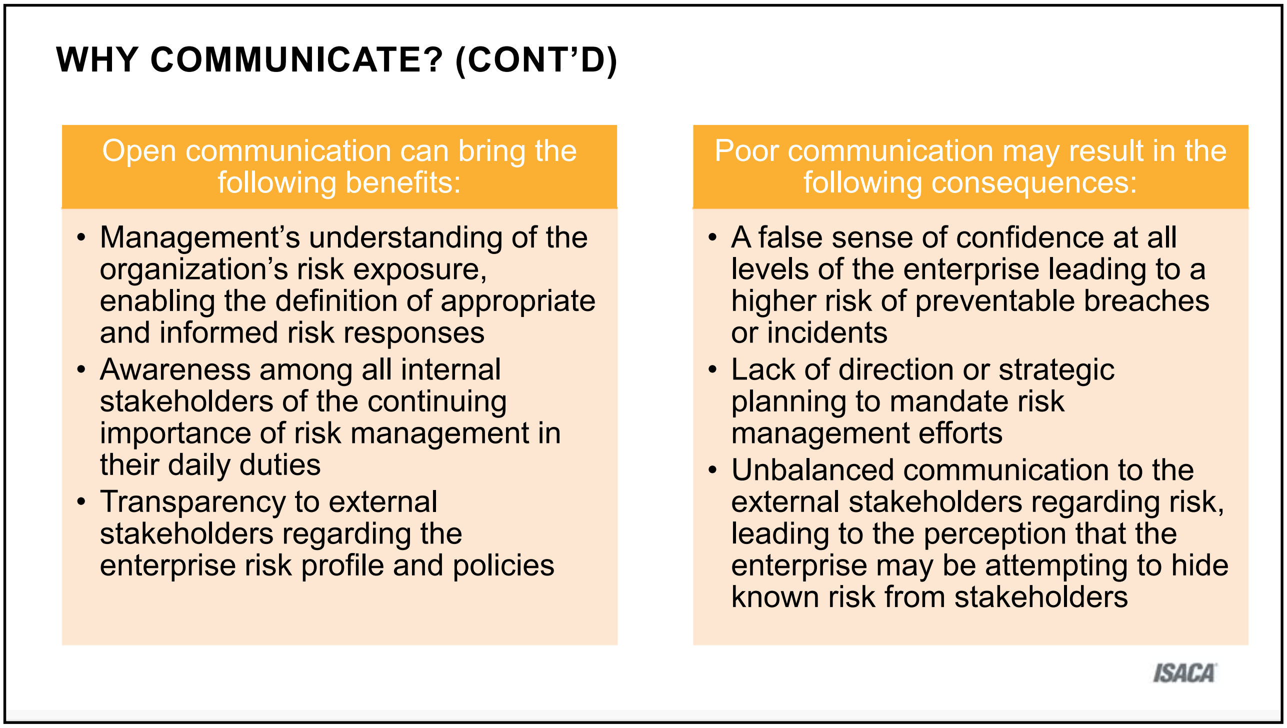


WHY COMMUNICATE?

The method and openness of risk communications plays a key role in defining and understanding the risk culture of an organization. If risk is to be managed and mitigated, it must first be discussed and effectively communicated.

Communication about the current risk profile of the organization removes the uncertainty and doubts concerning risk management.

Effective communication means that information is provided at an appropriate level to the various stakeholders throughout the organization.



WHY COMMUNICATE? (CONT'D)

Open communication can bring the following benefits:

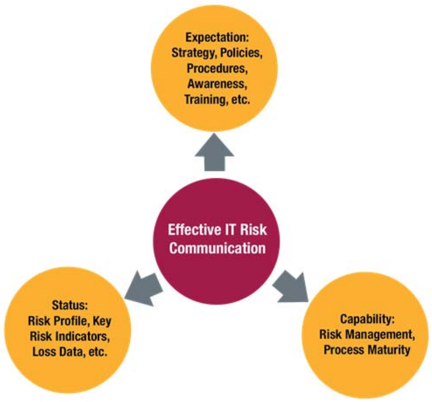
- Management's understanding of the organization's risk exposure, enabling the definition of appropriate and informed risk responses
- Awareness among all internal stakeholders of the continuing importance of risk management in their daily duties
- Transparency to external stakeholders regarding the enterprise risk profile and policies

Poor communication may result in the following consequences:

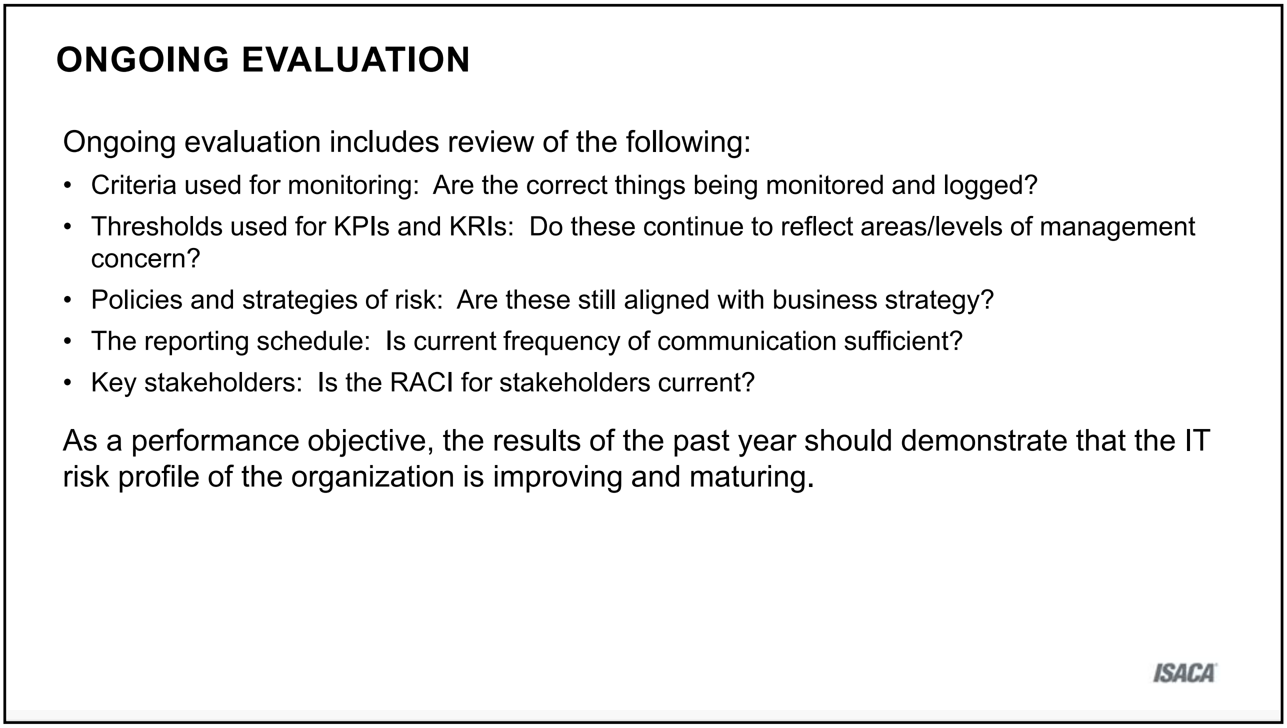
- A false sense of confidence at all levels of the enterprise leading to a higher risk of preventable breaches or incidents
- Lack of direction or strategic planning to mandate risk management efforts
- Unbalanced communication to the external stakeholders regarding risk, leading to the perception that the enterprise may be attempting to hide known risk from stakeholders

EFFECTIVE COMMUNICATION

Effective risk communication depends on the sharing of information regarding several aspects of the risk environment, as shown here:



Source: ISACA, *The Risk IT Framework,* USA, 2009, Figure 9

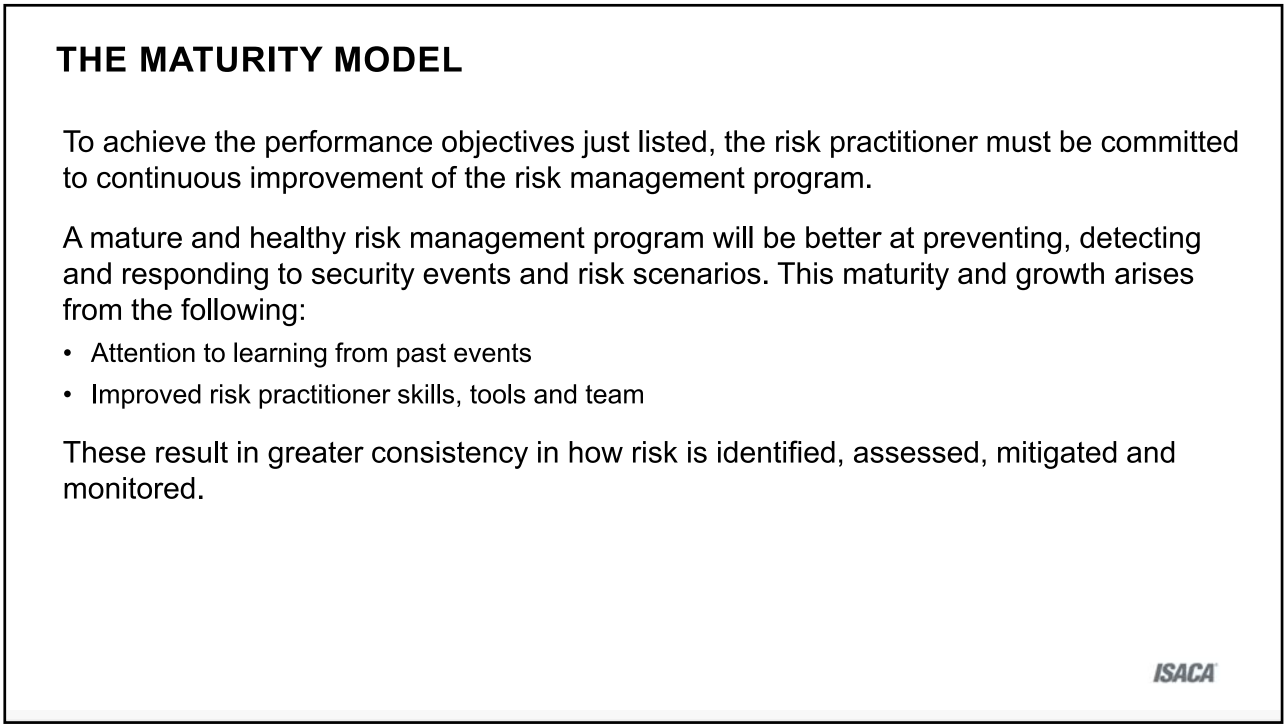


ONGOING EVALUATION

Ongoing evaluation includes review of the following:

- Criteria used for monitoring: Are the correct things being monitored and logged?
- Thresholds used for KPIs and KRIs: Do these continue to reflect areas/levels of management concern?
- Policies and strategies of risk: Are these still aligned with business strategy?
- The reporting schedule: Is current frequency of communication sufficient?
- Key stakeholders: Is the RACI for stakeholders current?

As a performance objective, the results of the past year should demonstrate that the IT risk profile of the organization is improving and maturing.



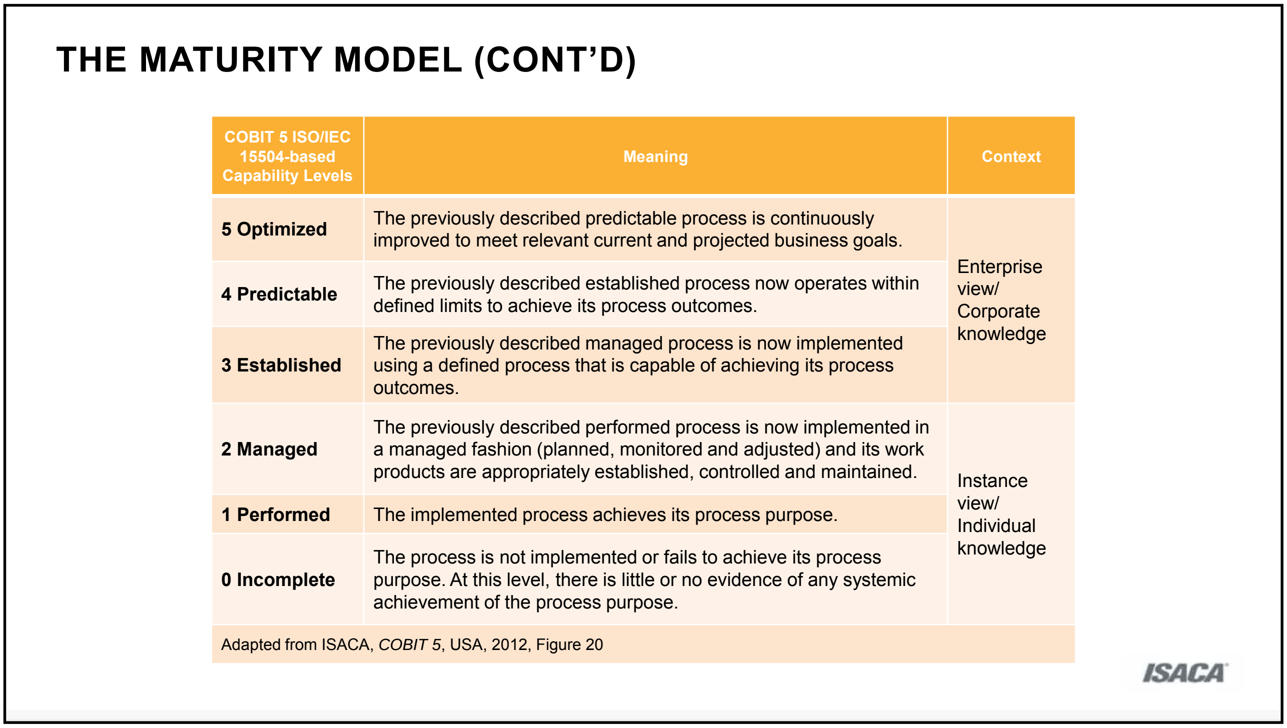
THE MATURITY MODEL

To achieve the performance objectives just listed, the risk practitioner must be committed to continuous improvement of the risk management program.

A mature and healthy risk management program will be better at preventing, detecting and responding to security events and risk scenarios. This maturity and growth arises from the following:

- Attention to learning from past events
- Improved risk practitioner skills, tools and team

These result in greater consistency in how risk is identified, assessed, mitigated and monitored.



THE MATURITY MODEL (CONT’D)

COBIT 5 ISO/IEC 15504-based Capability Levels	Meaning	Context
5 Optimized	The previously described predictable process is continuously improved to meet relevant current and projected business goals.	Enterprise view/ Corporate knowledge
4 Predictable	The previously described established process now operates within defined limits to achieve its process outcomes.	
3 Established	The previously described managed process is now implemented using a defined process that is capable of achieving its process outcomes.	
2 Managed	The previously described performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.	Instance view/ Individual knowledge
1 Performed	The implemented process achieves its process purpose.	
0 Incomplete	The process is not implemented or fails to achieve its process purpose. At this level, there is little or no evidence of any systemic achievement of the process purpose.	

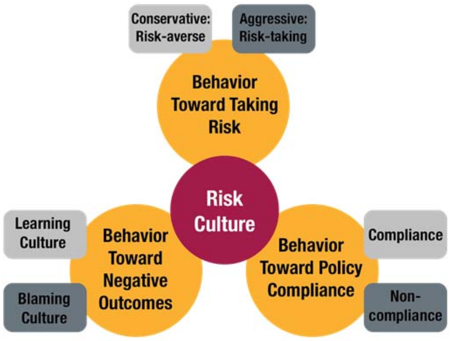
Adapted from ISACA, *COBIT 5*, USA, 2012, Figure 20

RISK CULTURE

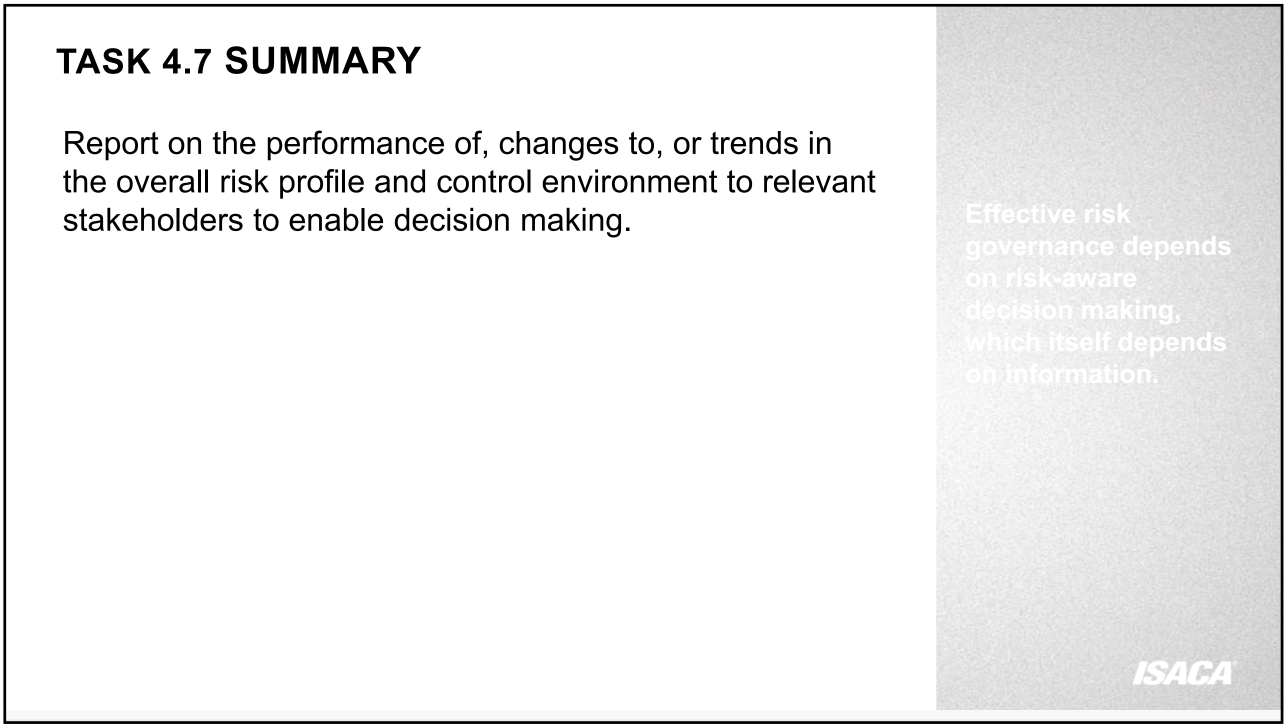
Senior management either consciously or unconsciously develops an attitude toward risk that indicates their willingness to embrace, cautiously accept or avoid risk.

This is referred to the risk culture.

Mature IT-risk management and open communication aids in improving the enterprise risk culture and has as its goal the improvement of behavior in each of the areas shown.


Conservative: Risk-averse
Aggressive: Risk-taking
Behavior Toward Taking Risk
Risk Culture
Learning Culture
Blaming Culture
Behavior Toward Negative Outcomes
Behavior Toward Policy Compliance
Compliance
Non-compliance

Source: ISACA, *The Risk IT Framework*, USA, 2009, figure 11



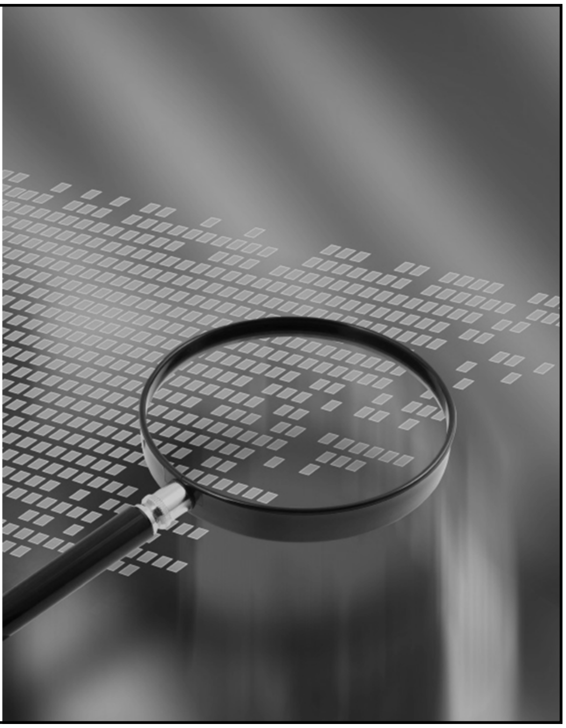
TASK 4.7 SUMMARY

Report on the performance of, changes to, or trends in the overall risk profile and control environment to relevant stakeholders to enable decision making.

Effective risk governance depends on risk-aware decision making, which itself depends on information.

TASK 4.7 ACTIVITY

Now that you have completed the risk registry and other exercises, develop a high level executive summary about the current status of risks and controls.



DISCUSSION QUESTION

When a significant vulnerability is discovered in the security of a critical web server, immediate notification should be made to the:

A. development team to remediate.

B. data owners to mitigate damage.

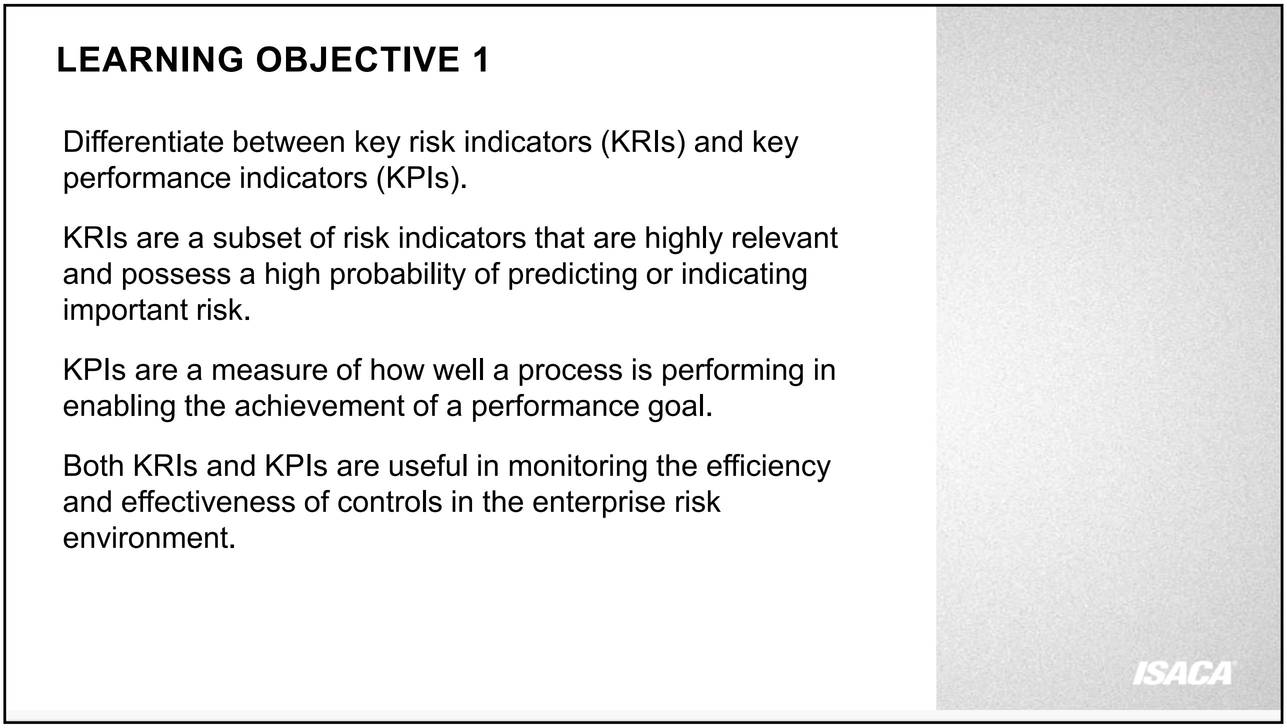
C. system owner to take corrective action.

D. incident response team to investigate.

DISCUSSION QUESTION

Which of the following MOST enables risk-aware business decisions?

A. Robust information security policies
B. An exchange of accurate and timely information
C. Skilled risk management personnel
D. Effective process controls



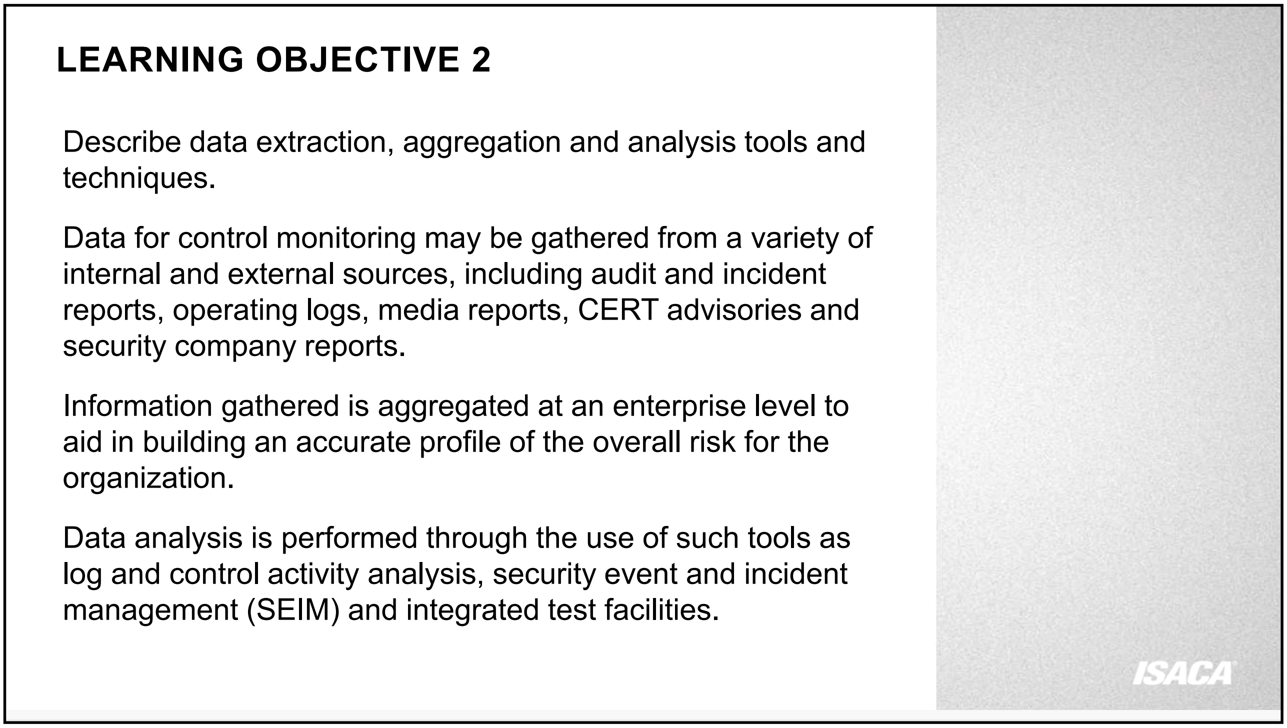
LEARNING OBJECTIVE 1

Differentiate between key risk indicators (KRIs) and key performance indicators (KPIs).

KRIs are a subset of risk indicators that are highly relevant and possess a high probability of predicting or indicating important risk.

KPIs are a measure of how well a process is performing in enabling the achievement of a performance goal.

Both KRIs and KPIs are useful in monitoring the efficiency and effectiveness of controls in the enterprise risk environment.



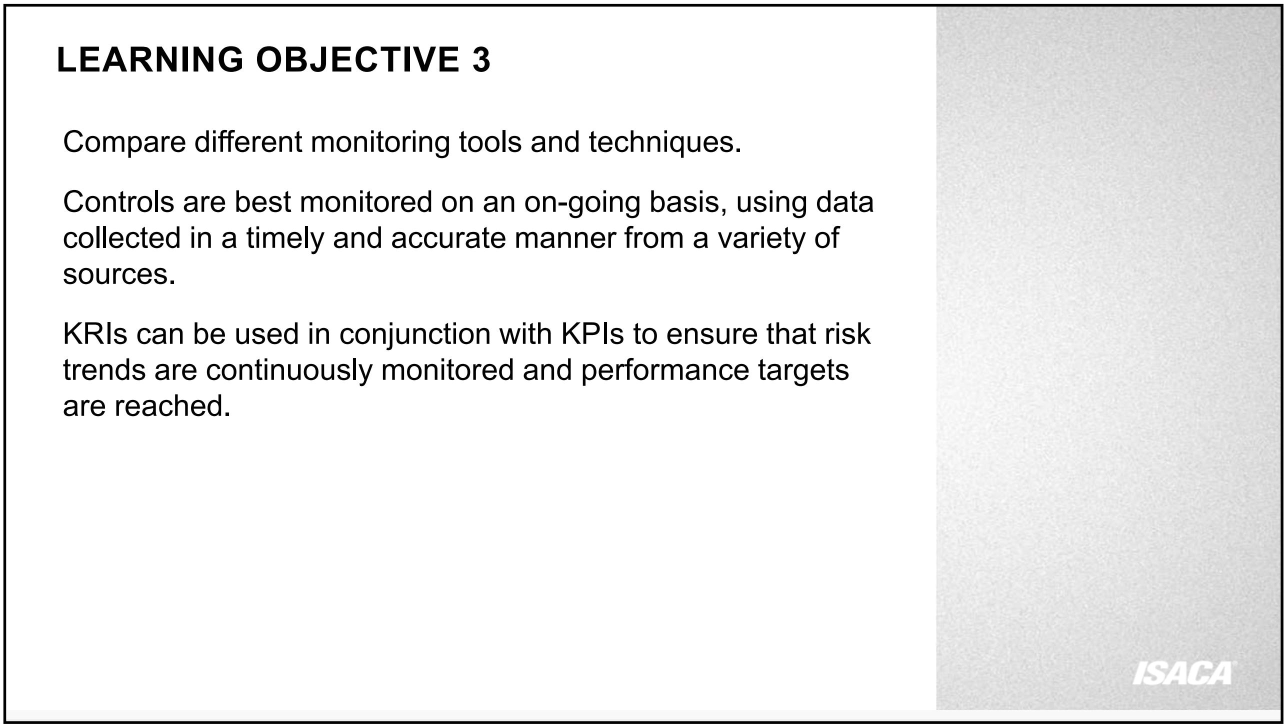
LEARNING OBJECTIVE 2

Describe data extraction, aggregation and analysis tools and techniques.

Data for control monitoring may be gathered from a variety of internal and external sources, including audit and incident reports, operating logs, media reports, CERT advisories and security company reports.

Information gathered is aggregated at an enterprise level to aid in building an accurate profile of the overall risk for the organization.

Data analysis is performed through the use of such tools as log and control activity analysis, security event and incident management (SEIM) and integrated test facilities.

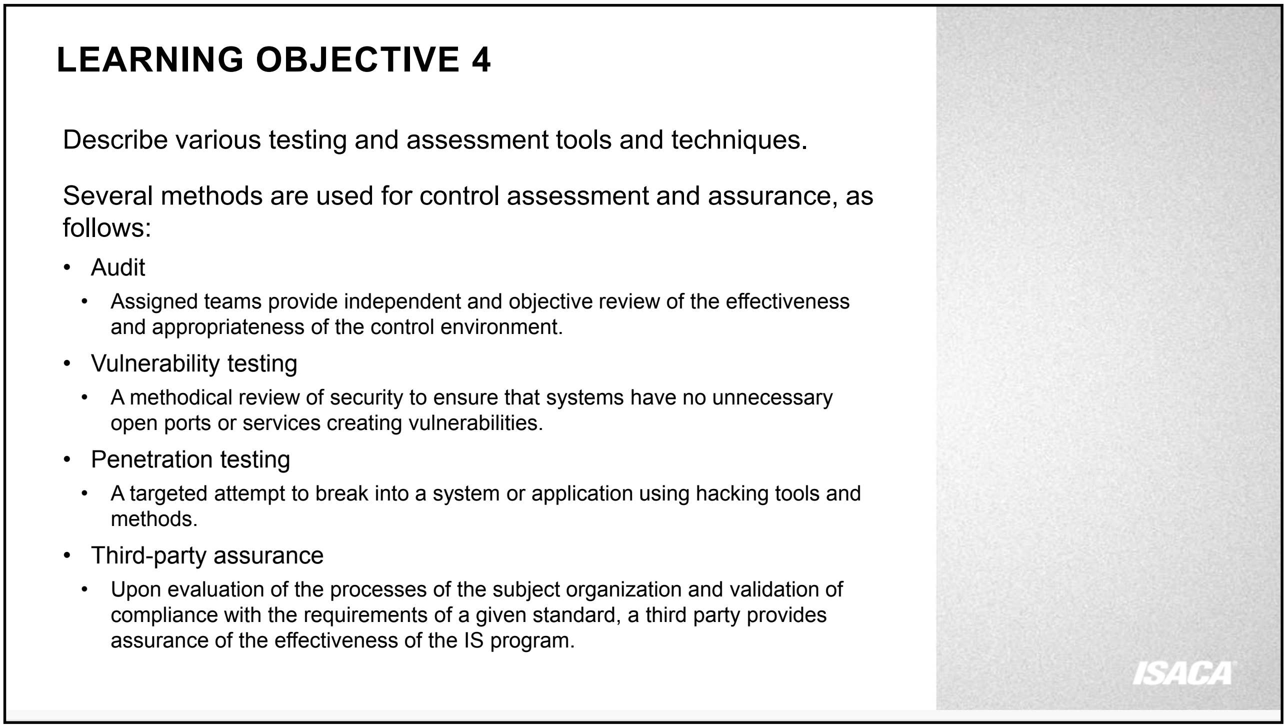


LEARNING OBJECTIVE 3

Compare different monitoring tools and techniques.

Controls are best monitored on an on-going basis, using data collected in a timely and accurate manner from a variety of sources.

KRIs can be used in conjunction with KPIs to ensure that risk trends are continuously monitored and performance targets are reached.

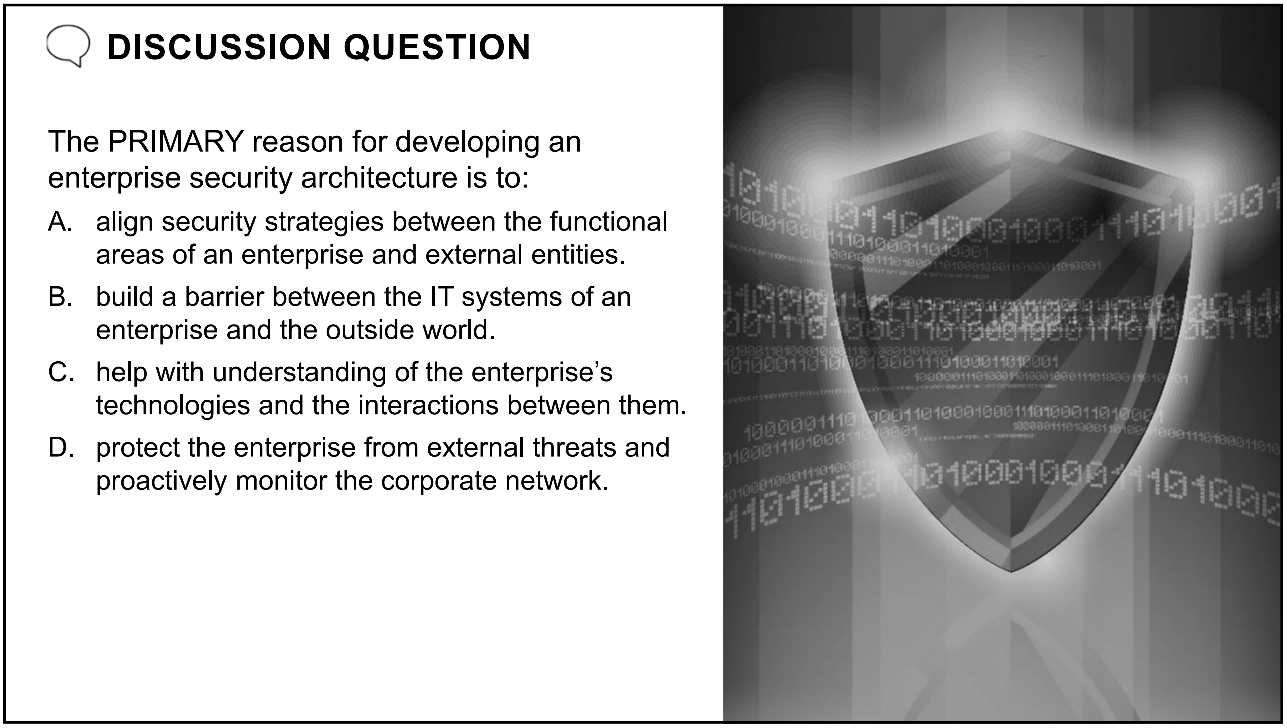


LEARNING OBJECTIVE 4

Describe various testing and assessment tools and techniques.

Several methods are used for control assessment and assurance, as follows:

- Audit
  - Assigned teams provide independent and objective review of the effectiveness and appropriateness of the control environment.
- Vulnerability testing
  - A methodical review of security to ensure that systems have no unnecessary open ports or services creating vulnerabilities.
- Penetration testing
  - A targeted attempt to break into a system or application using hacking tools and methods.
- Third-party assurance
  - Upon evaluation of the processes of the subject organization and validation of compliance with the requirements of a given standard, a third party provides assurance of the effectiveness of the IS program.



DISCUSSION QUESTION

The PRIMARY reason for developing an enterprise security architecture is to:

A. align security strategies between the functional areas of an enterprise and external entities.

B. build a barrier between the IT systems of an enterprise and the outside world.

C. help with understanding of the enterprise’s technologies and the interactions between them.

D. protect the enterprise from external threats and proactively monitor the corporate network.

DISCUSSION QUESTION

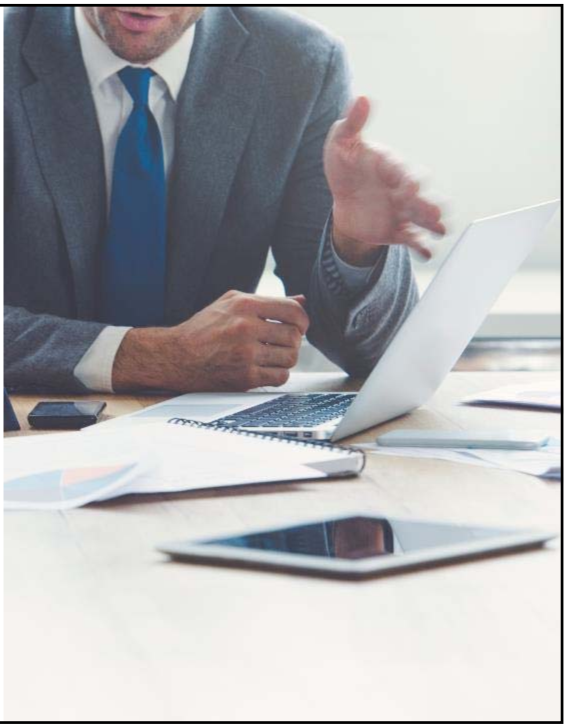
The BEST reason to implement a maturity model for risk management is to:

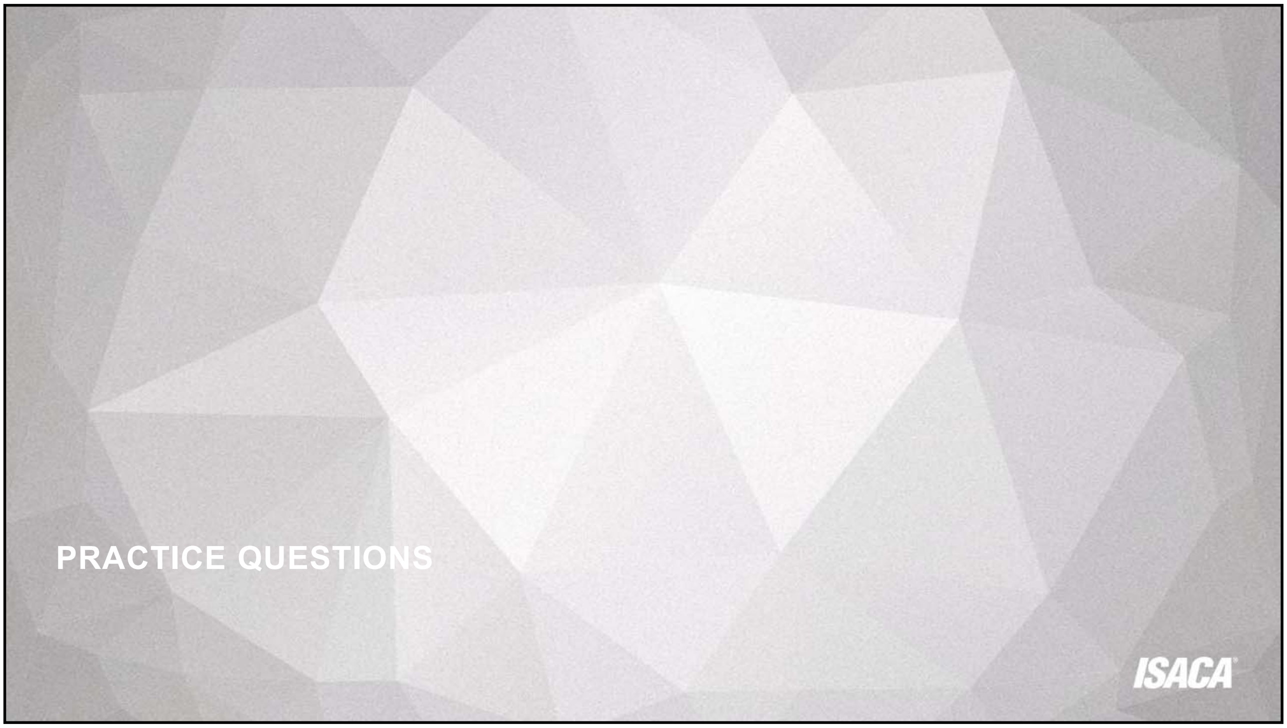
A. permit alignment with business objectives.

B. help improve governance and compliance.

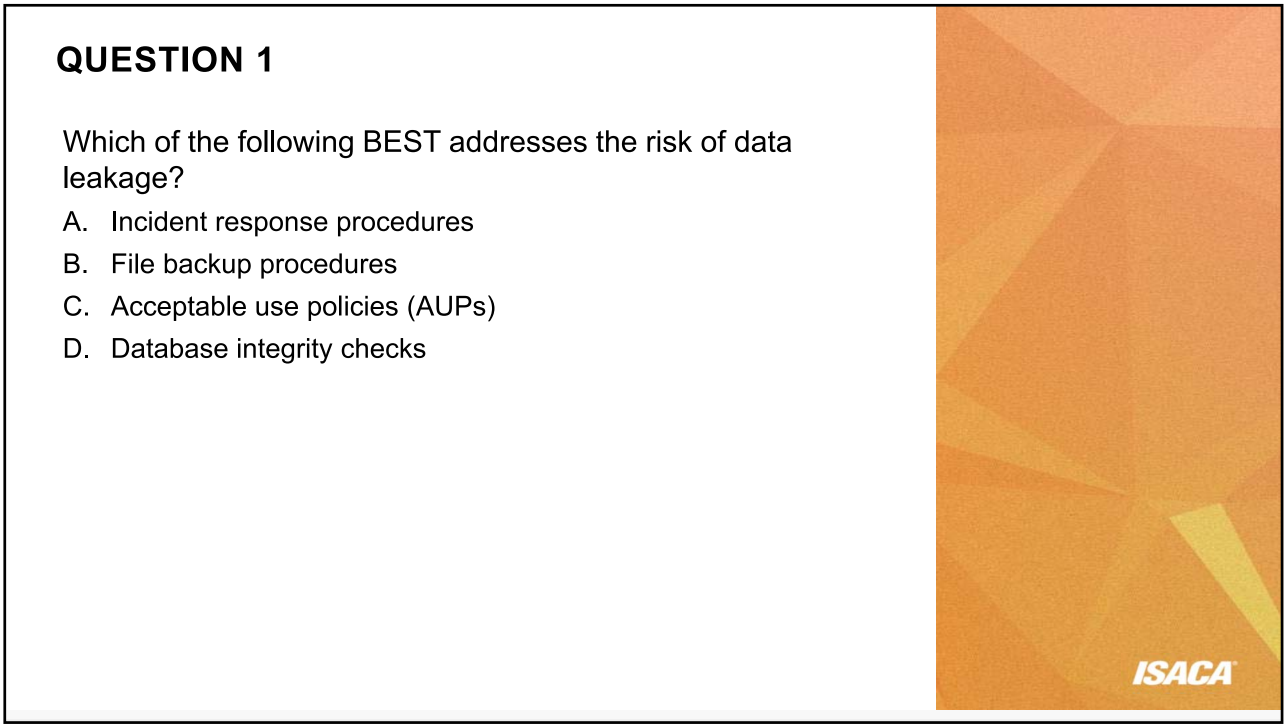
C. ensure that security controls are effective.

D. enable continuous improvement.





PRACTICE QUESTIONS



QUESTION 1

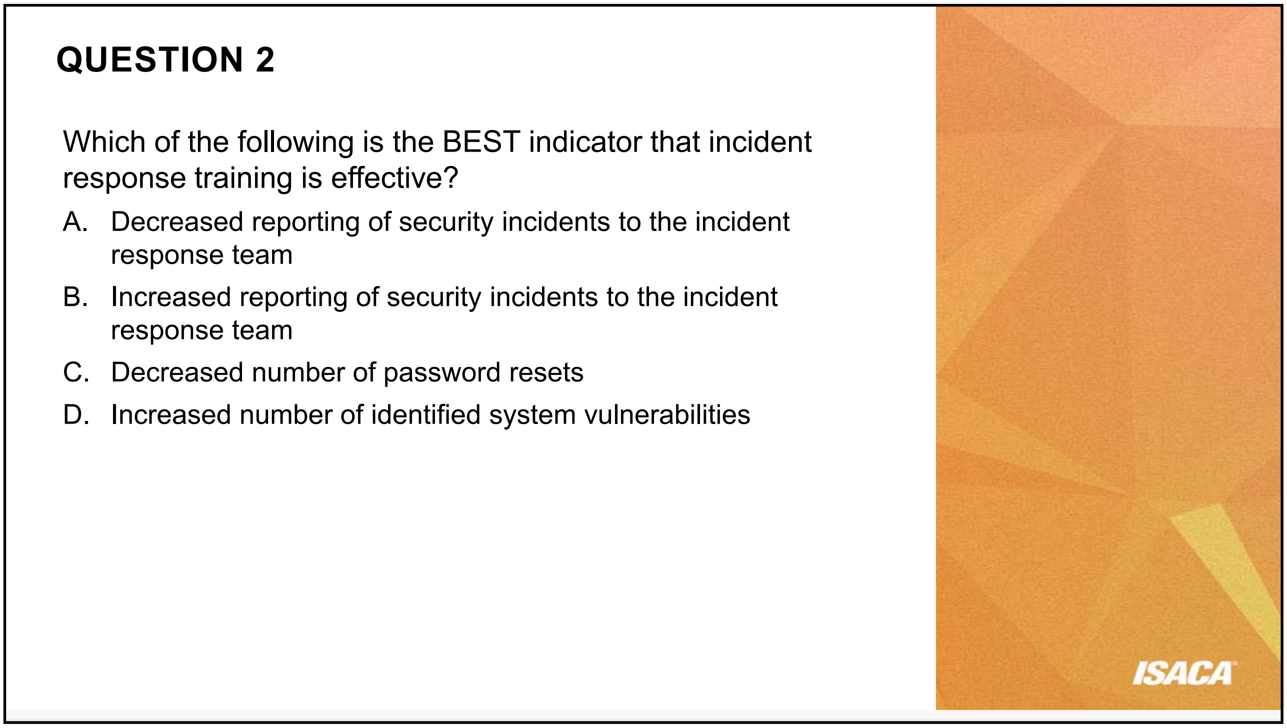
Which of the following BEST addresses the risk of data leakage?

A. Incident response procedures

B. File backup procedures

C. Acceptable use policies (AUPs)

D. Database integrity checks



QUESTION 2

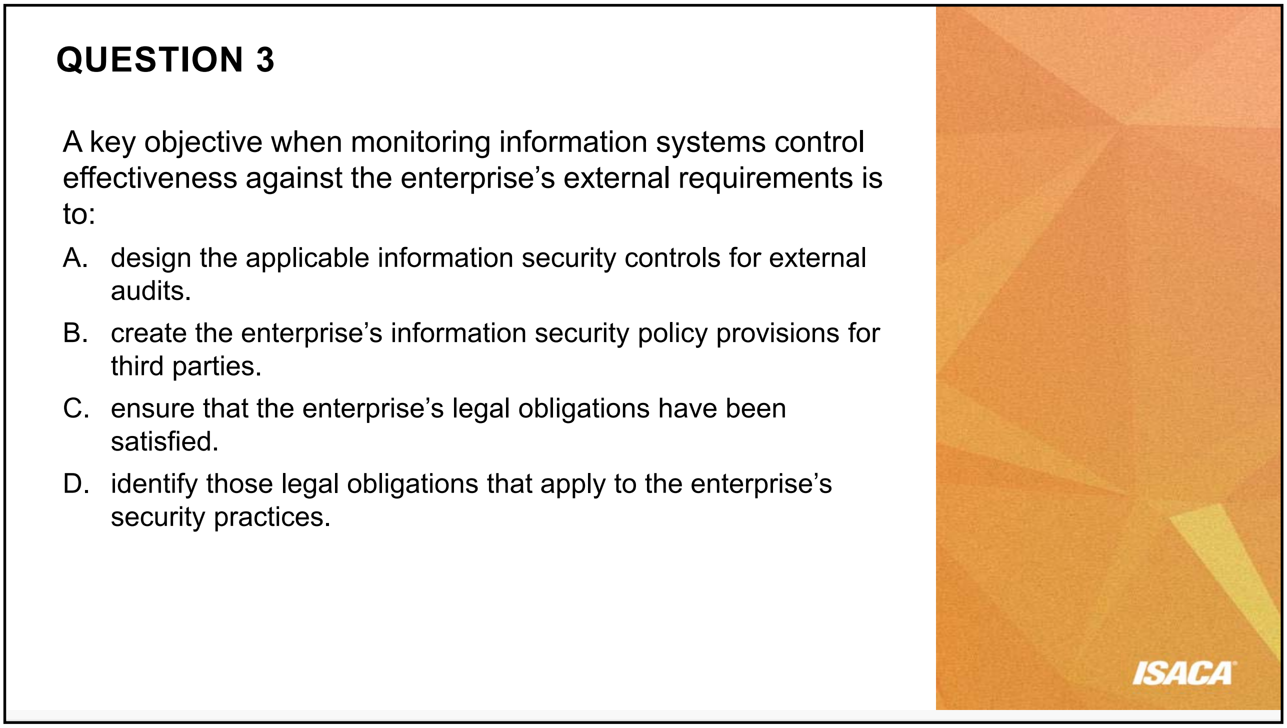
Which of the following is the BEST indicator that incident response training is effective?

A. Decreased reporting of security incidents to the incident response team

B. Increased reporting of security incidents to the incident response team

C. Decreased number of password resets

D. Increased number of identified system vulnerabilities



QUESTION 3

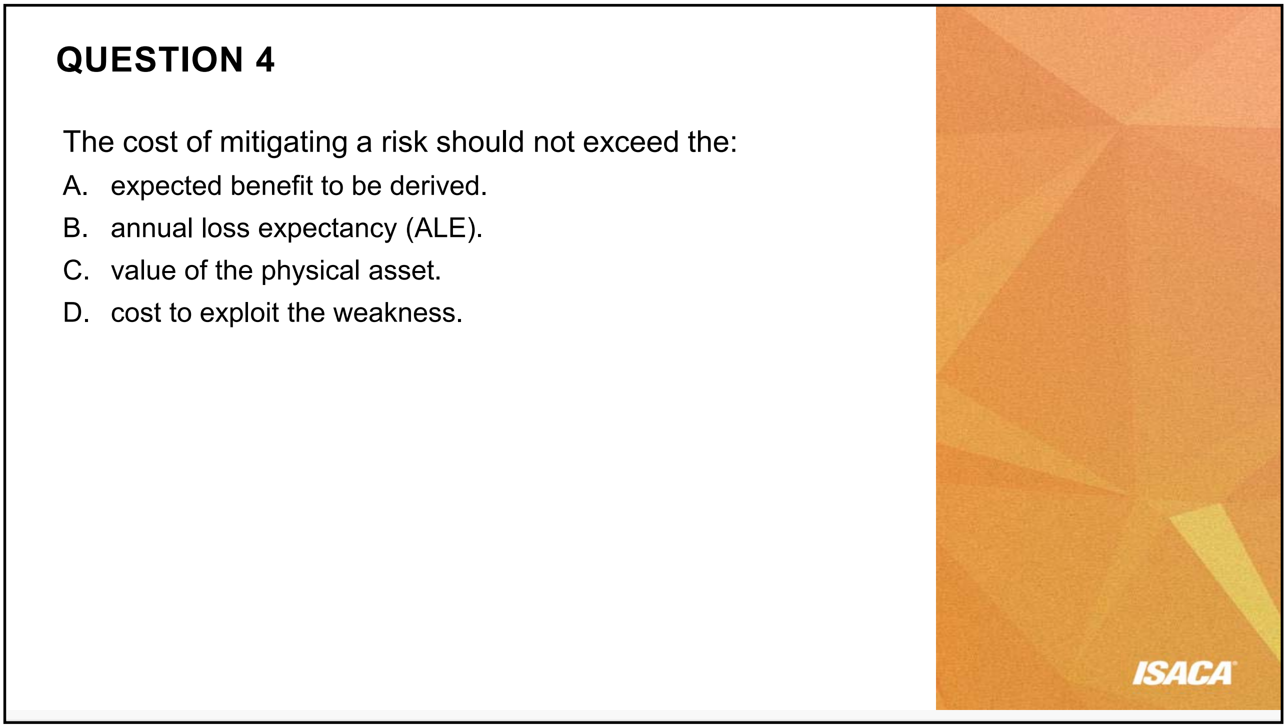
A key objective when monitoring information systems control effectiveness against the enterprise's external requirements is to:

A. design the applicable information security controls for external audits.

B. create the enterprise's information security policy provisions for third parties.

C. ensure that the enterprise's legal obligations have been satisfied.

D. identify those legal obligations that apply to the enterprise's security practices.



QUESTION 4

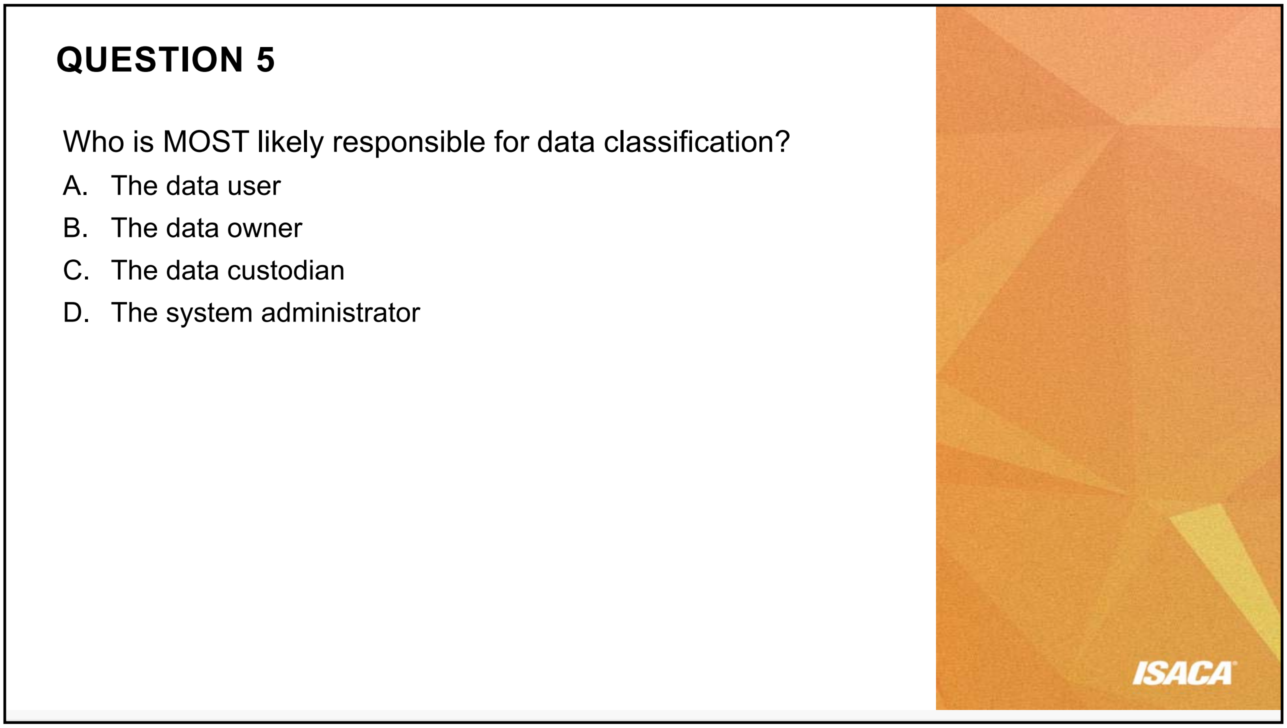
The cost of mitigating a risk should not exceed the:

A. expected benefit to be derived.

B. annual loss expectancy (ALE).

C. value of the physical asset.

D. cost to exploit the weakness.



QUESTION 5

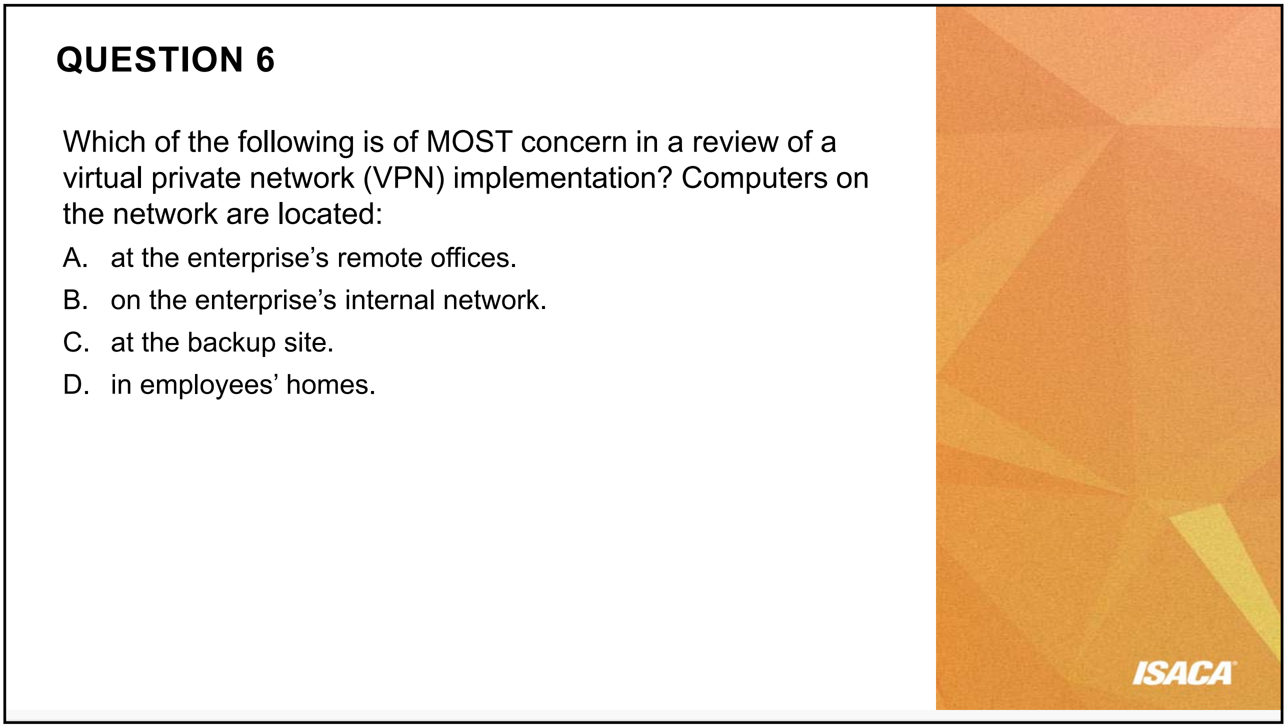
Who is MOST likely responsible for data classification?

A. The data user

B. The data owner

C. The data custodian

D. The system administrator



QUESTION 6

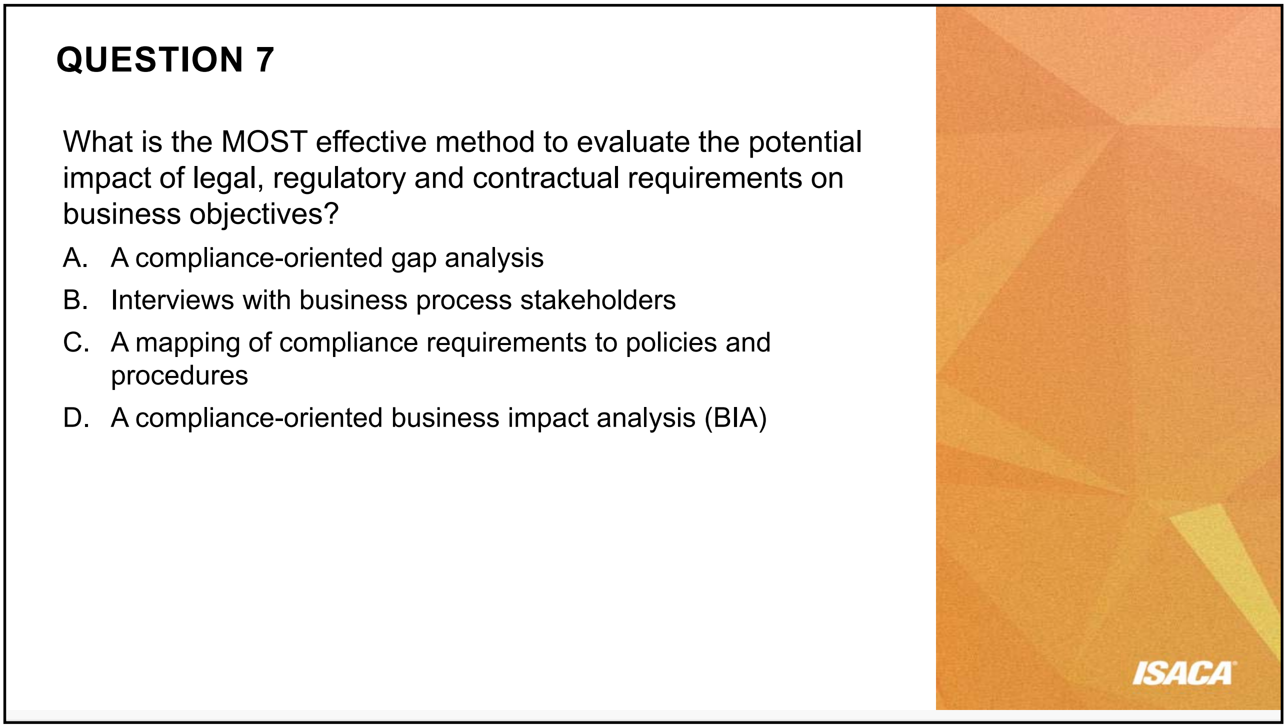
Which of the following is of MOST concern in a review of a virtual private network (VPN) implementation? Computers on the network are located:

A. at the enterprise's remote offices.

B. on the enterprise's internal network.

C. at the backup site.

D. in employees' homes.



QUESTION 7

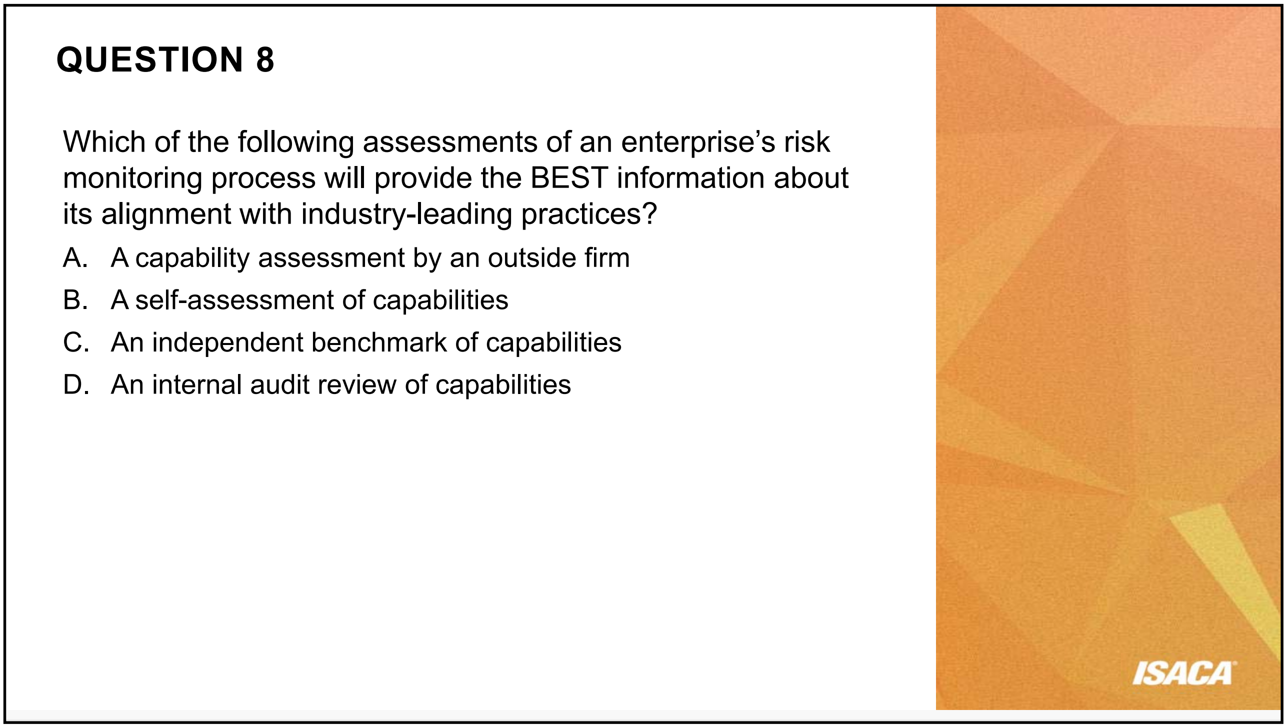
What is the MOST effective method to evaluate the potential impact of legal, regulatory and contractual requirements on business objectives?

A. A compliance-oriented gap analysis

B. Interviews with business process stakeholders

C. A mapping of compliance requirements to policies and procedures

D. A compliance-oriented business impact analysis (BIA)



QUESTION 8

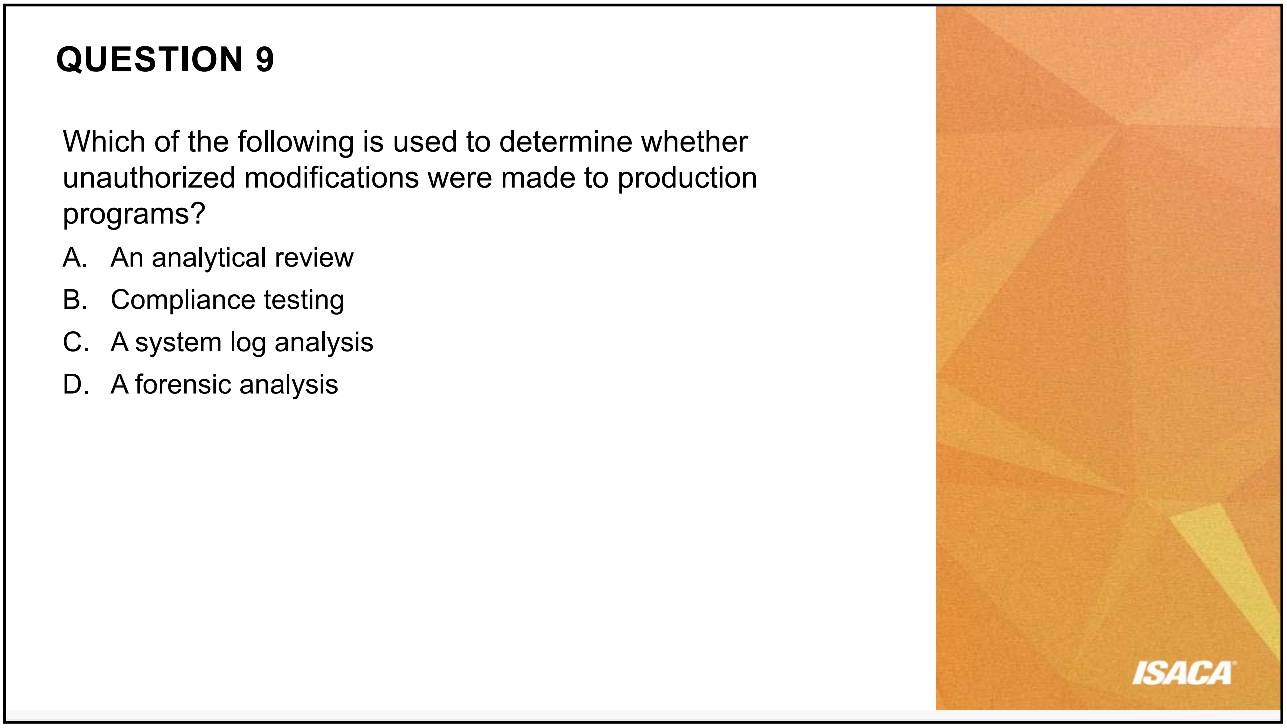
Which of the following assessments of an enterprise's risk monitoring process will provide the BEST information about its alignment with industry-leading practices?

A. A capability assessment by an outside firm

B. A self-assessment of capabilities

C. An independent benchmark of capabilities

D. An internal audit review of capabilities



QUESTION 9

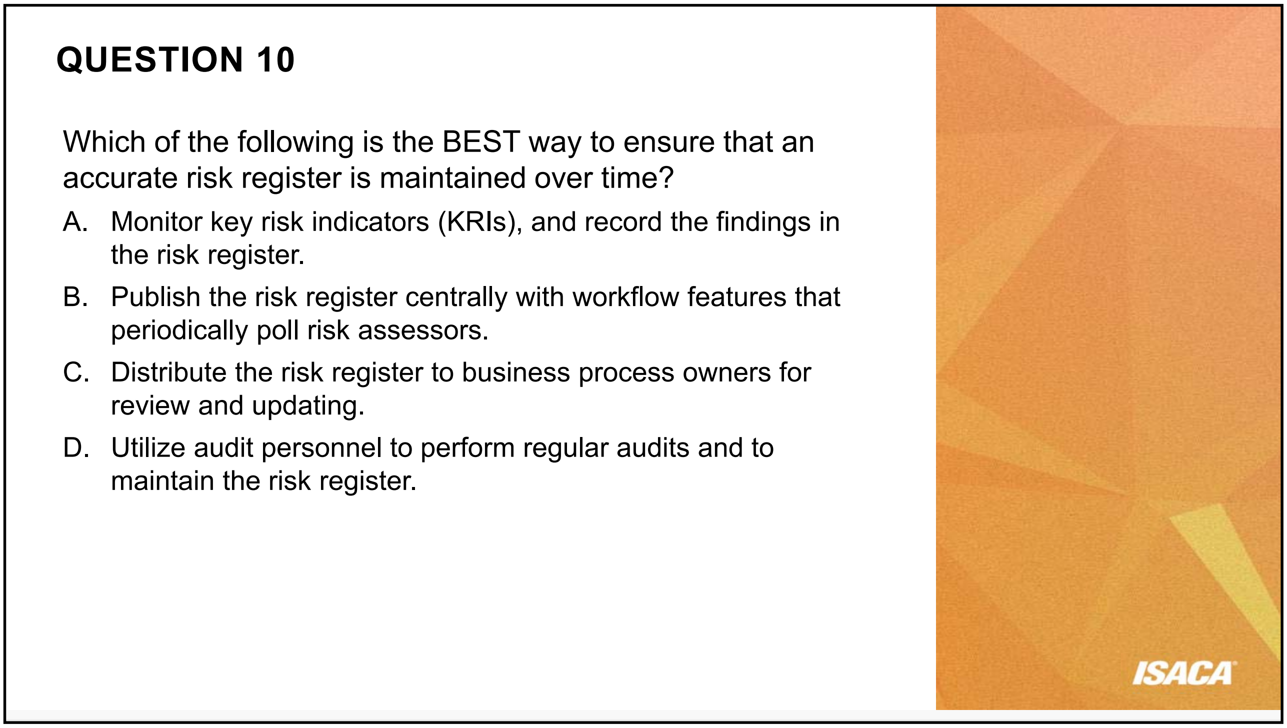
Which of the following is used to determine whether unauthorized modifications were made to production programs?

A. An analytical review

B. Compliance testing

C. A system log analysis

D. A forensic analysis



QUESTION 10

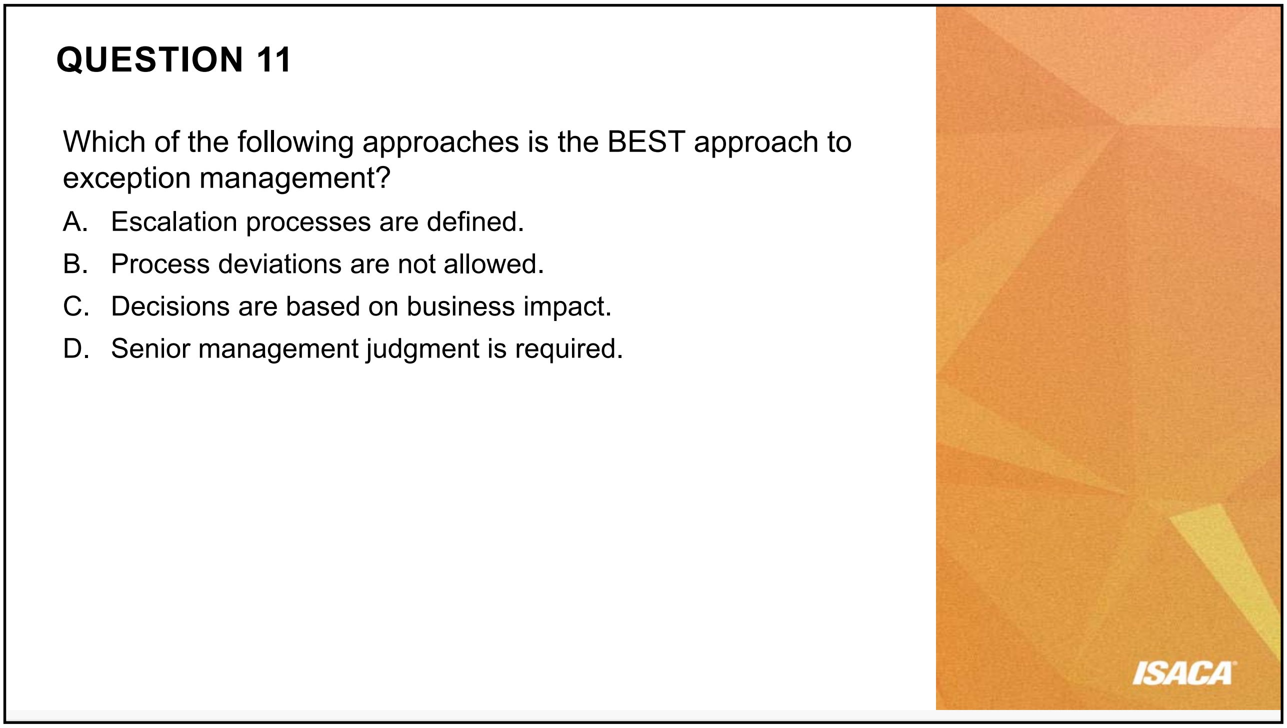
Which of the following is the BEST way to ensure that an accurate risk register is maintained over time?

A. Monitor key risk indicators (KRIs), and record the findings in the risk register.

B. Publish the risk register centrally with workflow features that periodically poll risk assessors.

C. Distribute the risk register to business process owners for review and updating.

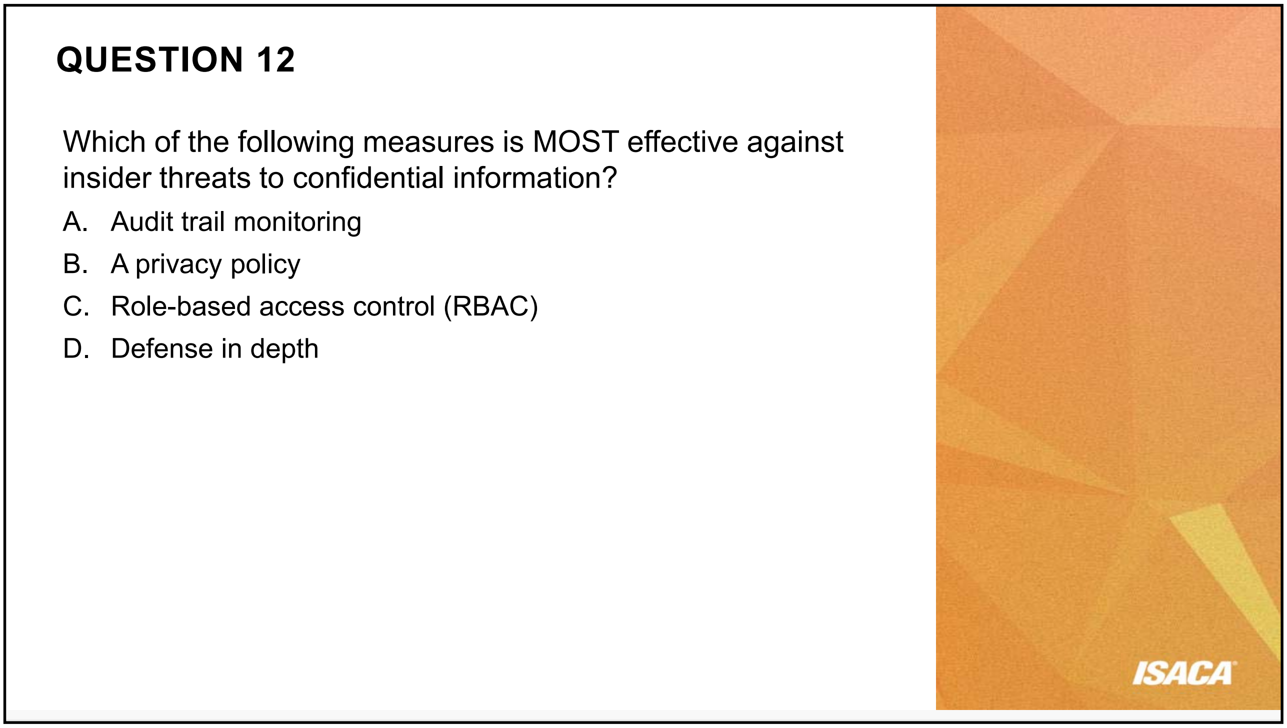
D. Utilize audit personnel to perform regular audits and to maintain the risk register.



QUESTION 11

Which of the following approaches is the BEST approach to exception management?

A. Escalation processes are defined.
B. Process deviations are not allowed.
C. Decisions are based on business impact.
D. Senior management judgment is required.



QUESTION 12

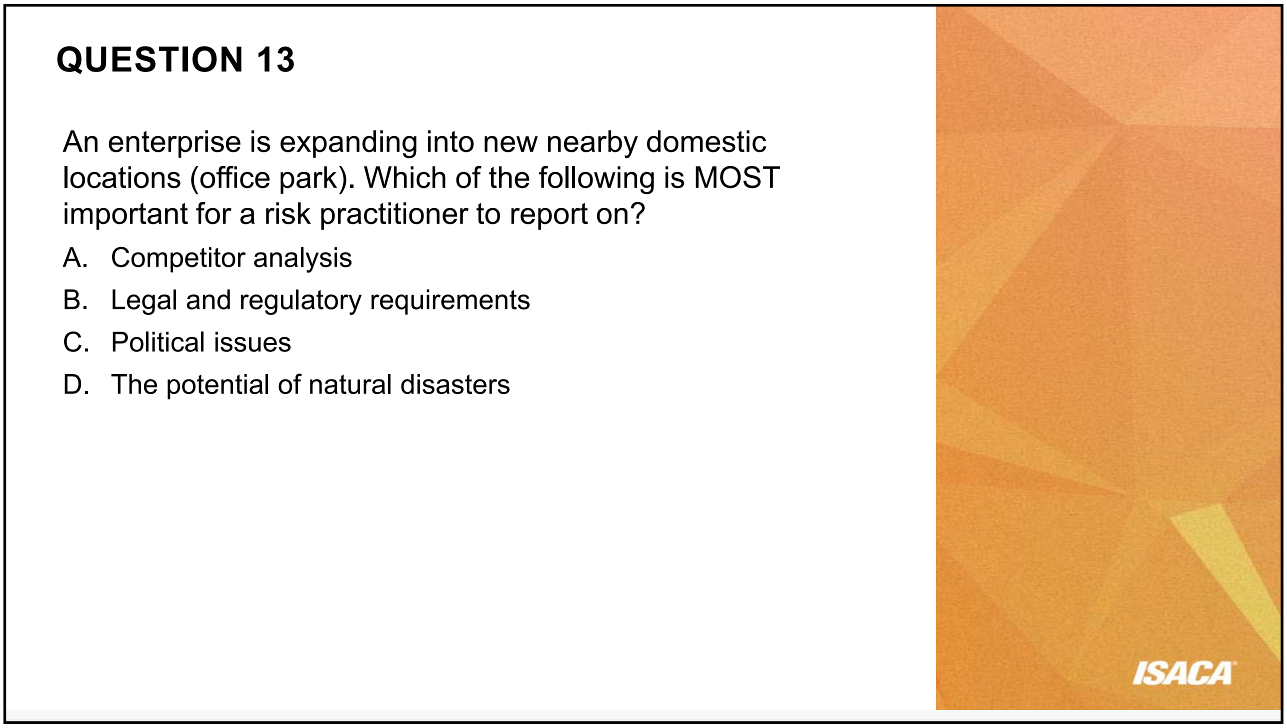
Which of the following measures is MOST effective against insider threats to confidential information?

A. Audit trail monitoring

B. A privacy policy

C. Role-based access control (RBAC)

D. Defense in depth



QUESTION 13

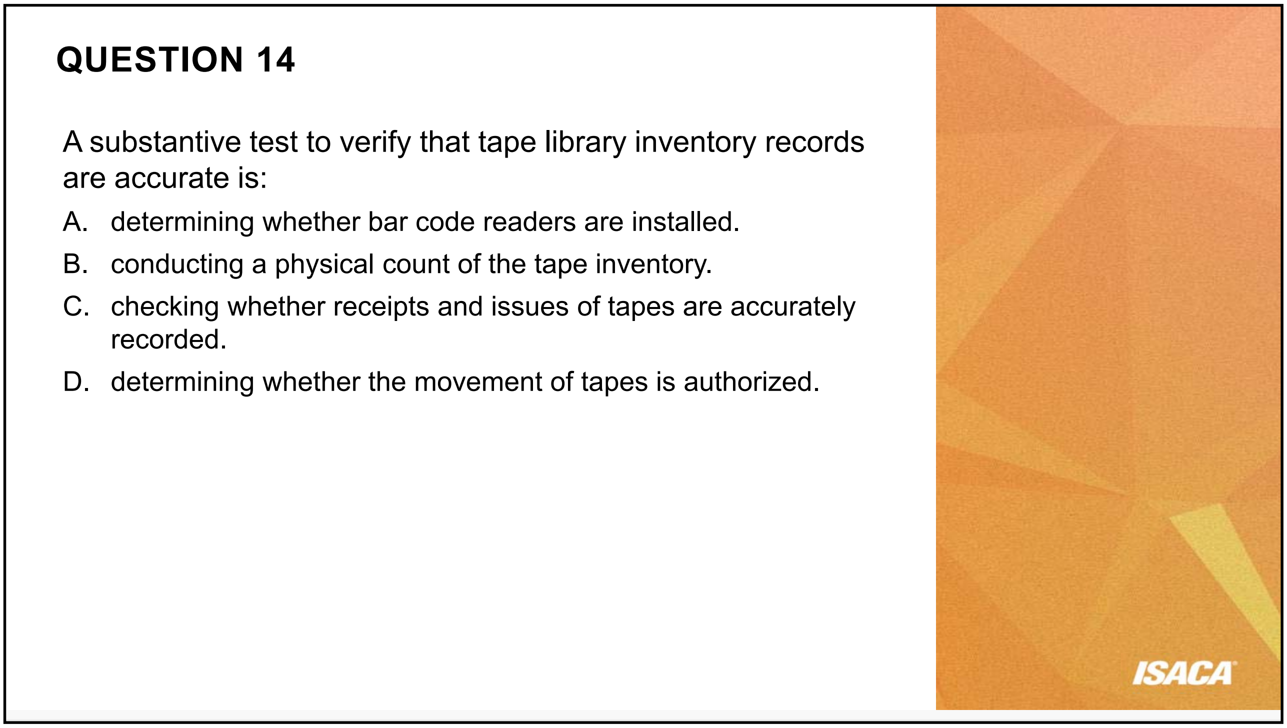
An enterprise is expanding into new nearby domestic locations (office park). Which of the following is MOST important for a risk practitioner to report on?

A. Competitor analysis

B. Legal and regulatory requirements

C. Political issues

D. The potential of natural disasters



QUESTION 14

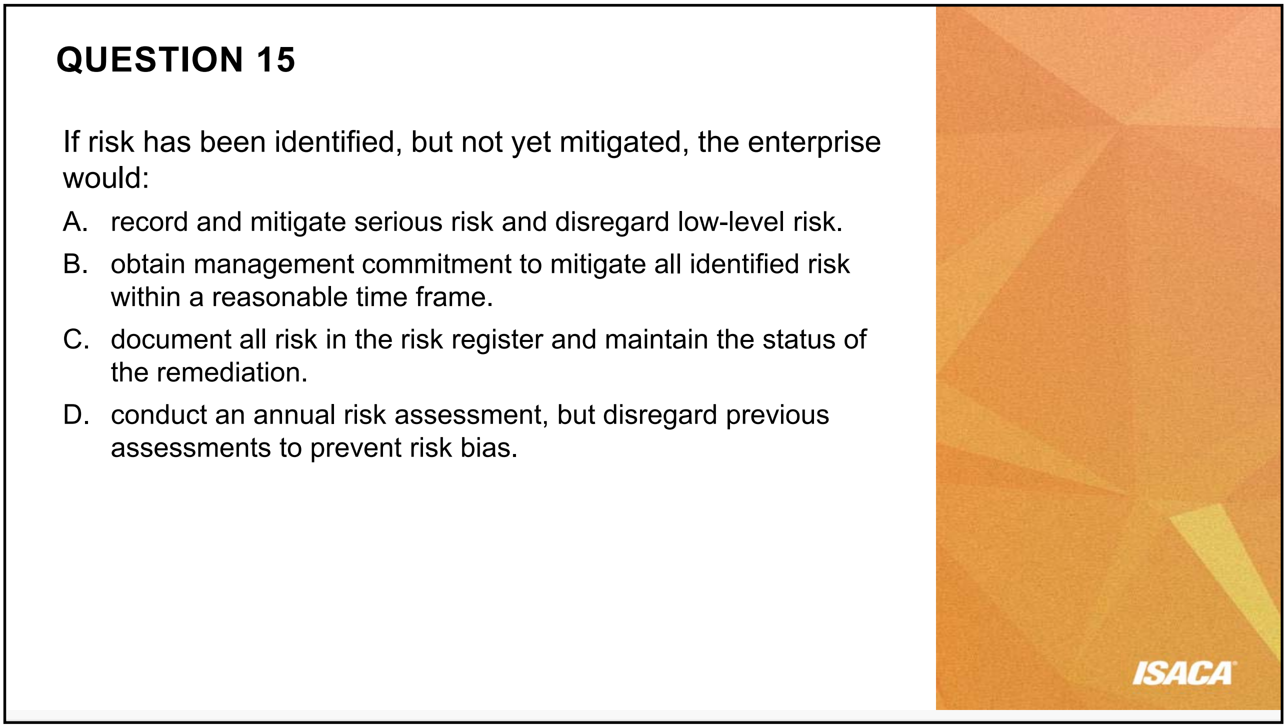
A substantive test to verify that tape library inventory records are accurate is:

A. determining whether bar code readers are installed.

B. conducting a physical count of the tape inventory.

C. checking whether receipts and issues of tapes are accurately recorded.

D. determining whether the movement of tapes is authorized.



QUESTION 15

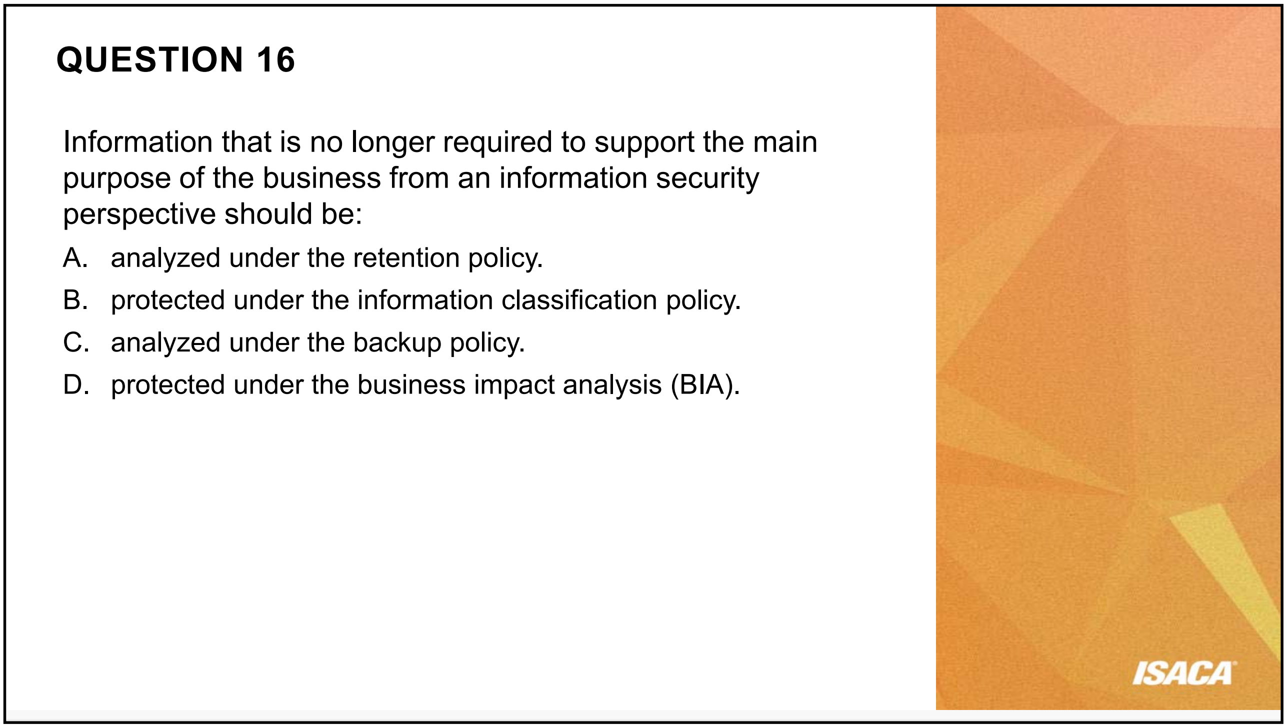
If risk has been identified, but not yet mitigated, the enterprise would:

A. record and mitigate serious risk and disregard low-level risk.

B. obtain management commitment to mitigate all identified risk within a reasonable time frame.

C. document all risk in the risk register and maintain the status of the remediation.

D. conduct an annual risk assessment, but disregard previous assessments to prevent risk bias.



QUESTION 16

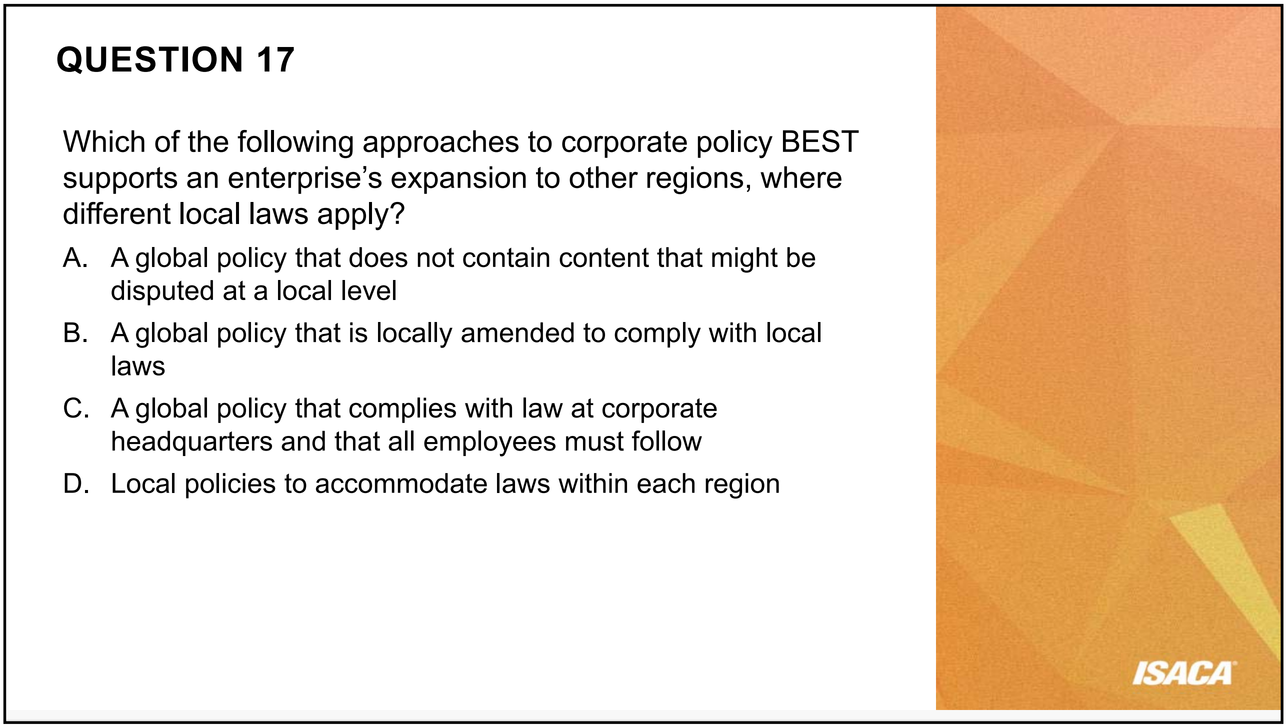
Information that is no longer required to support the main purpose of the business from an information security perspective should be:

A. analyzed under the retention policy.

B. protected under the information classification policy.

C. analyzed under the backup policy.

D. protected under the business impact analysis (BIA).



QUESTION 17

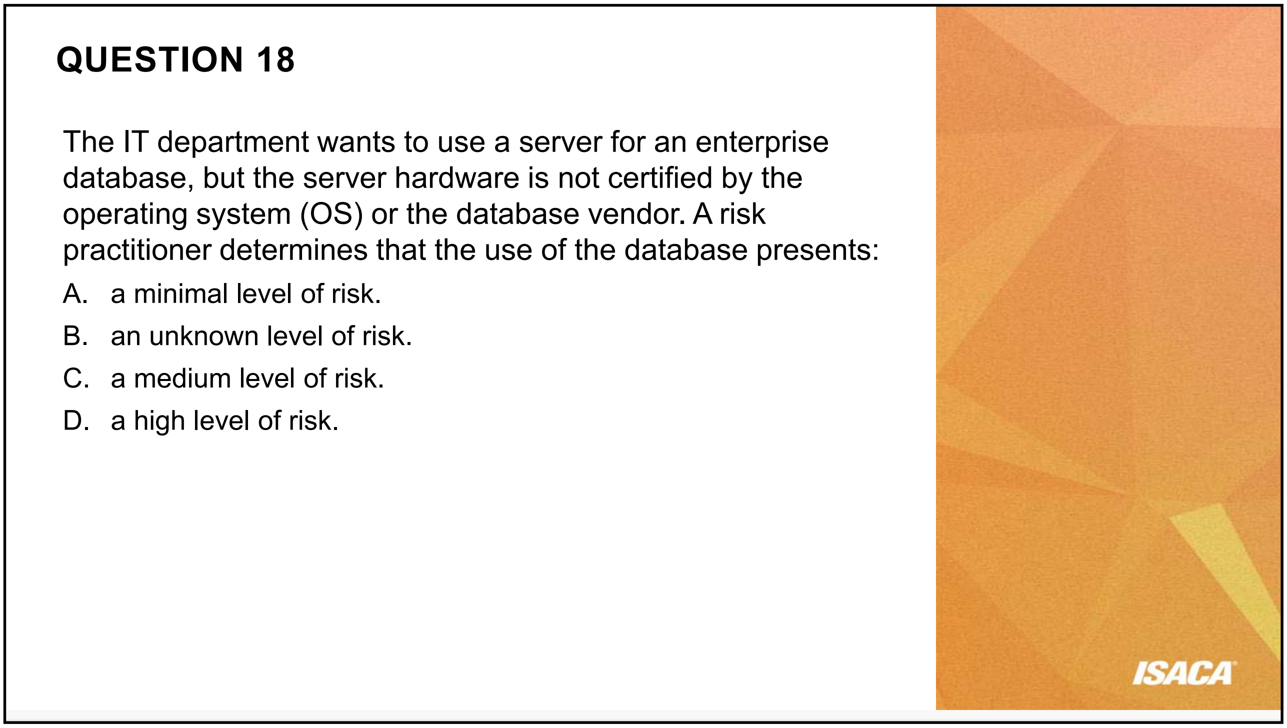
Which of the following approaches to corporate policy BEST supports an enterprise’s expansion to other regions, where different local laws apply?

A. A global policy that does not contain content that might be disputed at a local level

B. A global policy that is locally amended to comply with local laws

C. A global policy that complies with law at corporate headquarters and that all employees must follow

D. Local policies to accommodate laws within each region



QUESTION 18

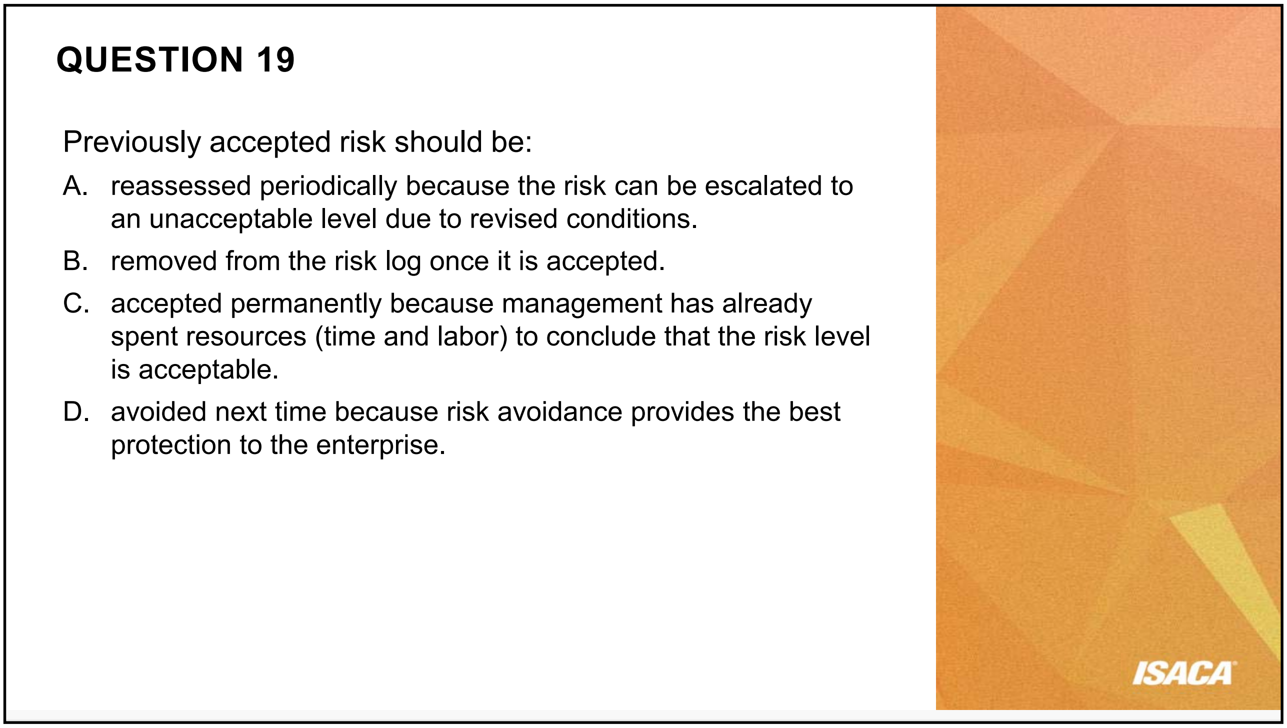
The IT department wants to use a server for an enterprise database, but the server hardware is not certified by the operating system (OS) or the database vendor. A risk practitioner determines that the use of the database presents:

A. a minimal level of risk.

B. an unknown level of risk.

C. a medium level of risk.

D. a high level of risk.



QUESTION 19

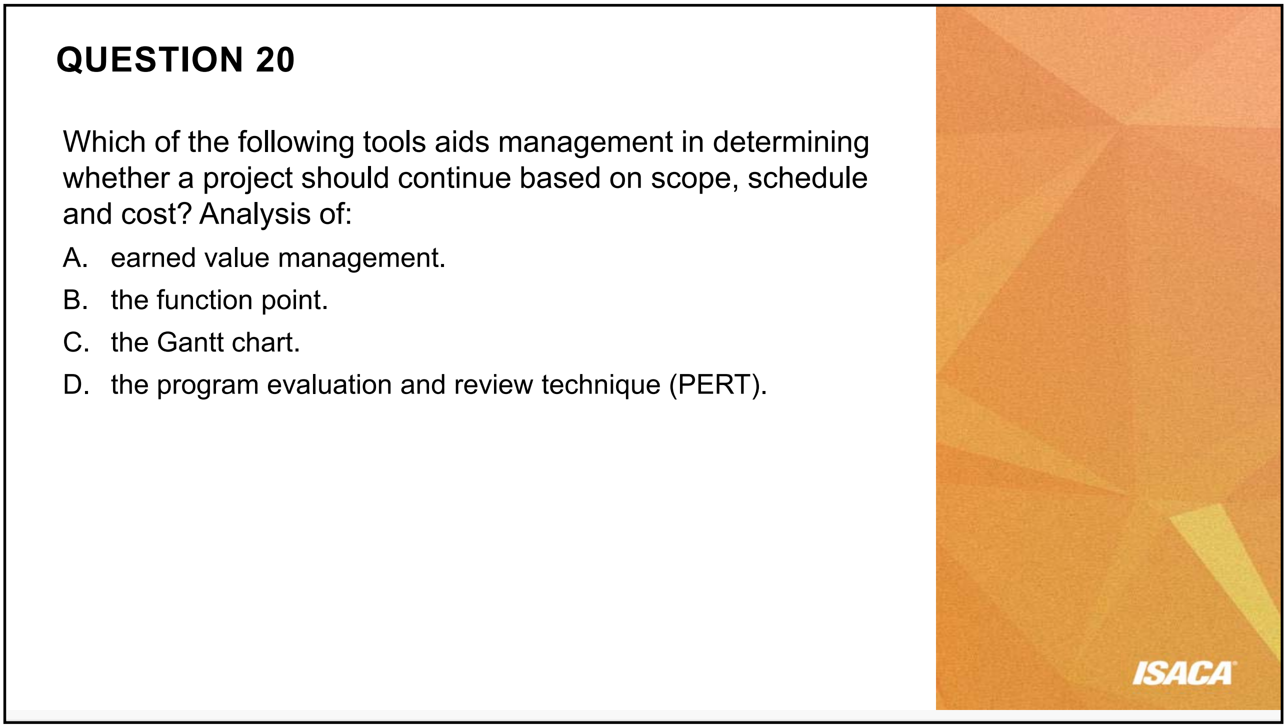
Previously accepted risk should be:

A. reassessed periodically because the risk can be escalated to an unacceptable level due to revised conditions.

B. removed from the risk log once it is accepted.

C. accepted permanently because management has already spent resources (time and labor) to conclude that the risk level is acceptable.

D. avoided next time because risk avoidance provides the best protection to the enterprise.



QUESTION 20

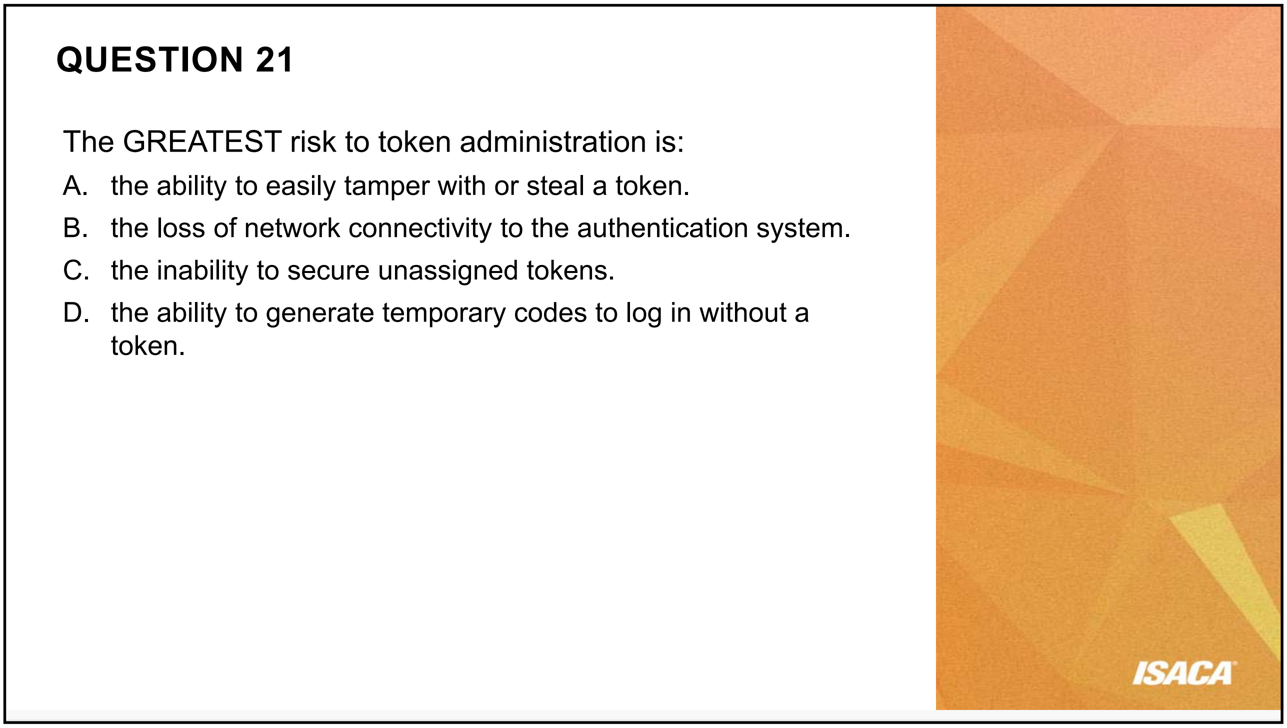
Which of the following tools aids management in determining whether a project should continue based on scope, schedule and cost? Analysis of:

A. earned value management.

B. the function point.

C. the Gantt chart.

D. the program evaluation and review technique (PERT).



QUESTION 21

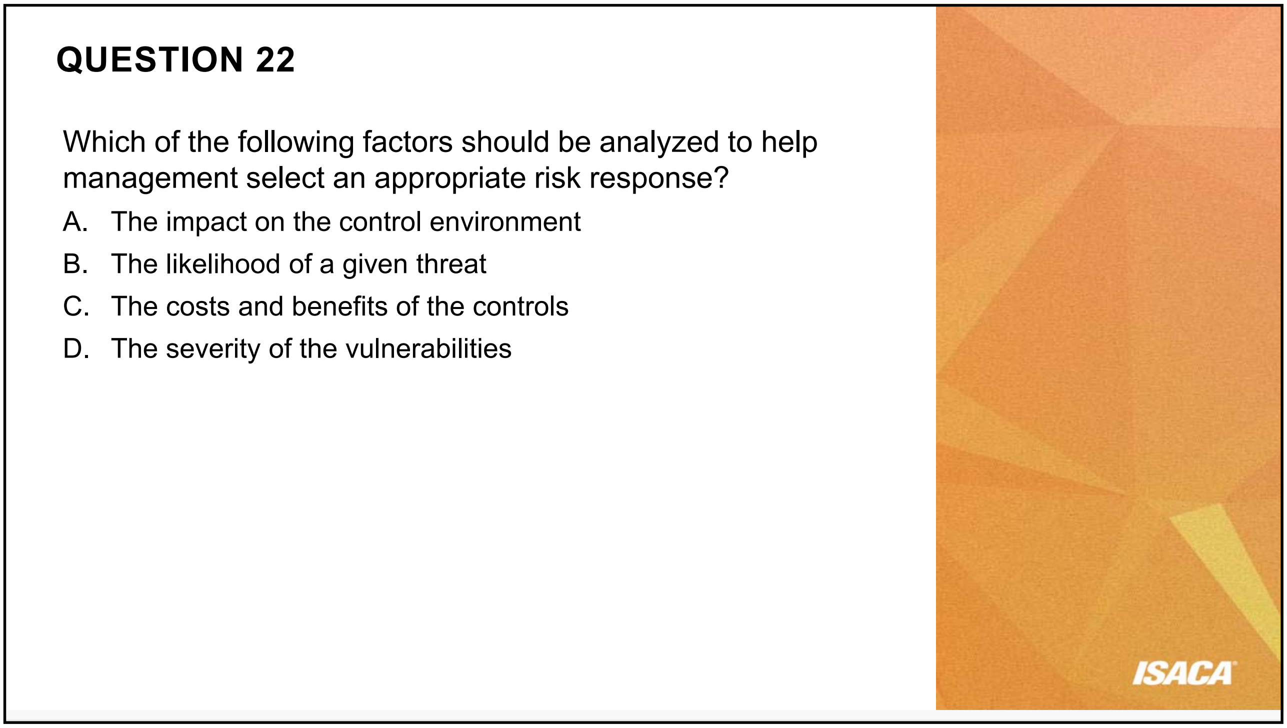
The GREATEST risk to token administration is:

A. the ability to easily tamper with or steal a token.

B. the loss of network connectivity to the authentication system.

C. the inability to secure unassigned tokens.

D. the ability to generate temporary codes to log in without a token.



QUESTION 22

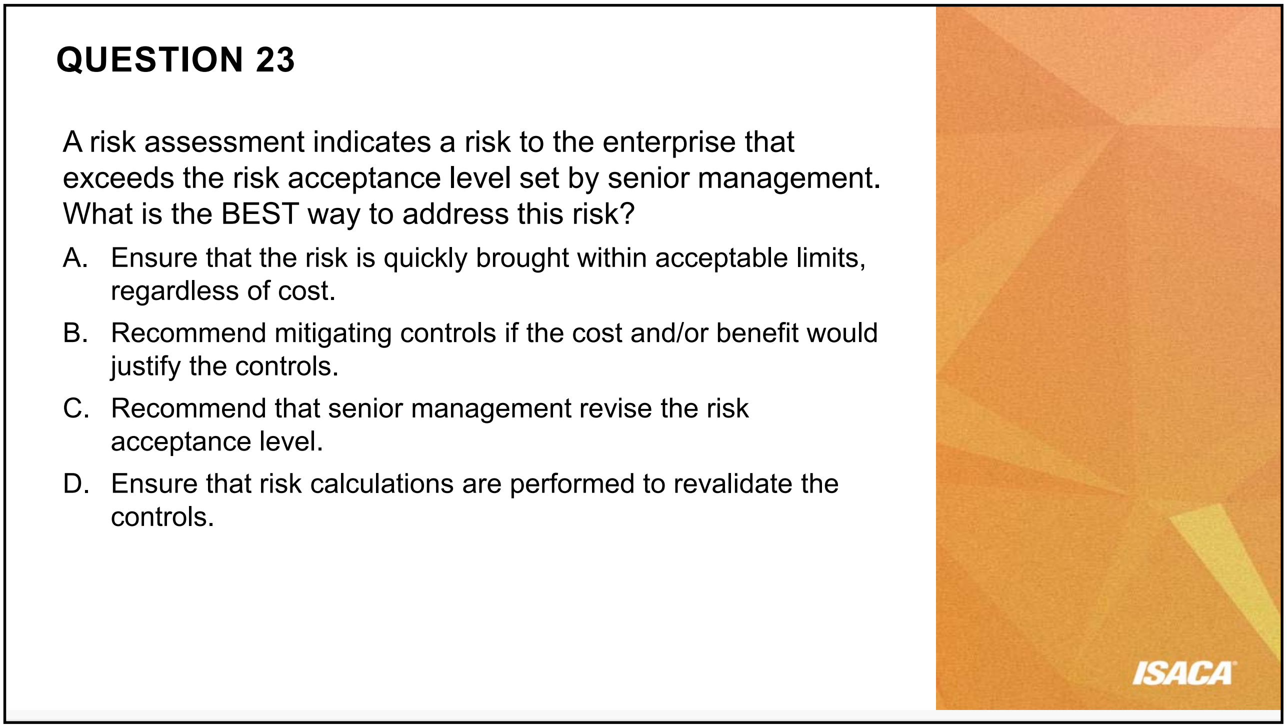
Which of the following factors should be analyzed to help management select an appropriate risk response?

A. The impact on the control environment

B. The likelihood of a given threat

C. The costs and benefits of the controls

D. The severity of the vulnerabilities



QUESTION 23

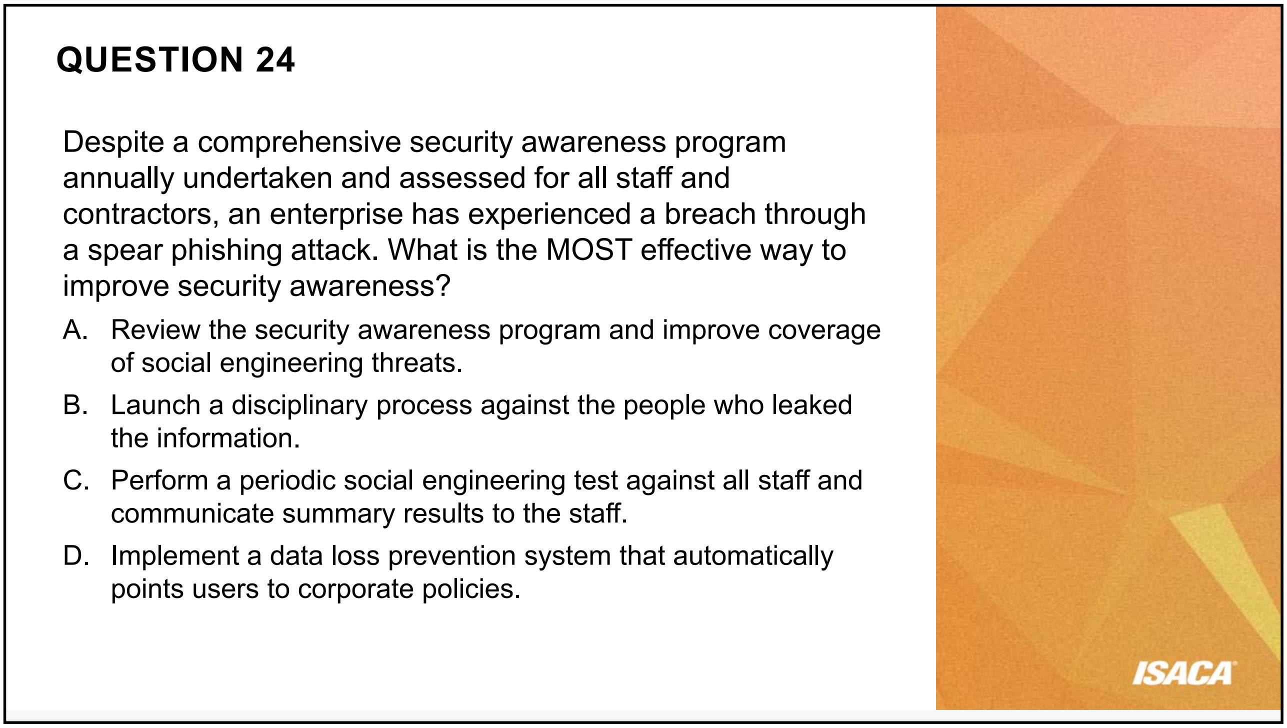
A risk assessment indicates a risk to the enterprise that exceeds the risk acceptance level set by senior management. What is the BEST way to address this risk?

A. Ensure that the risk is quickly brought within acceptable limits, regardless of cost.

B. Recommend mitigating controls if the cost and/or benefit would justify the controls.

C. Recommend that senior management revise the risk acceptance level.

D. Ensure that risk calculations are performed to revalidate the controls.



QUESTION 24

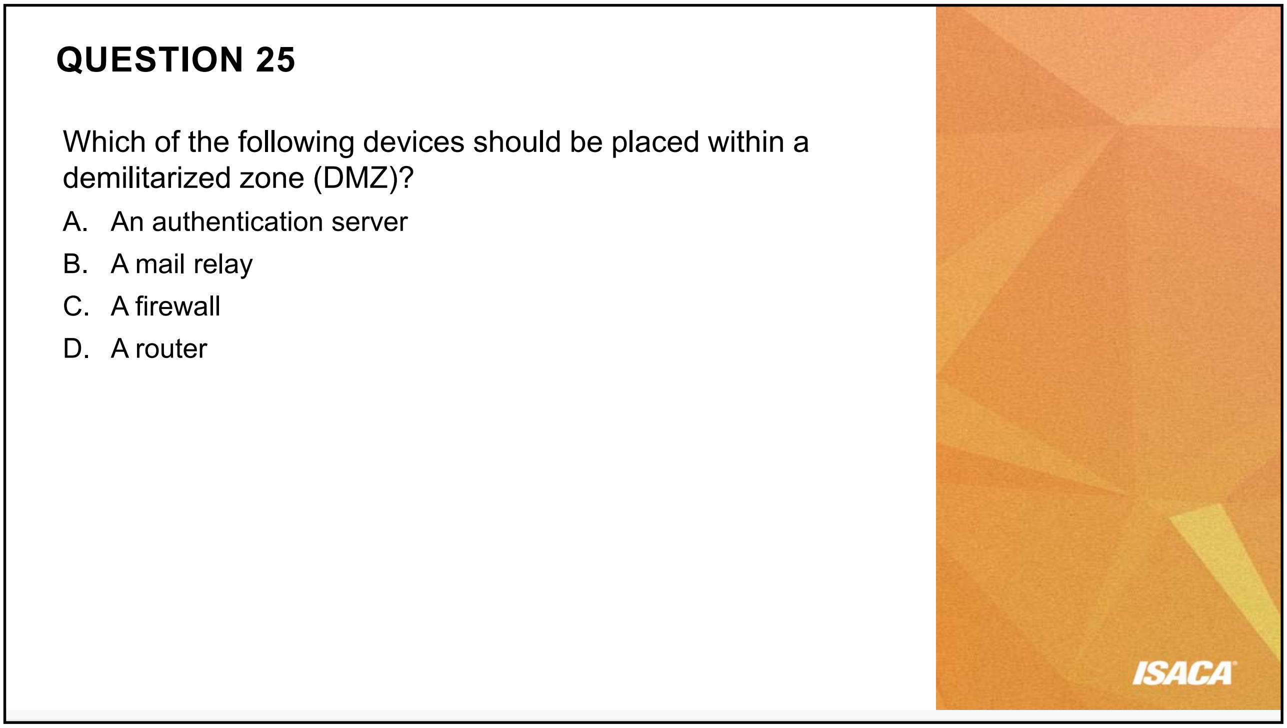
Despite a comprehensive security awareness program annually undertaken and assessed for all staff and contractors, an enterprise has experienced a breach through a spear phishing attack. What is the MOST effective way to improve security awareness?

A. Review the security awareness program and improve coverage of social engineering threats.

B. Launch a disciplinary process against the people who leaked the information.

C. Perform a periodic social engineering test against all staff and communicate summary results to the staff.

D. Implement a data loss prevention system that automatically points users to corporate policies.



QUESTION 25

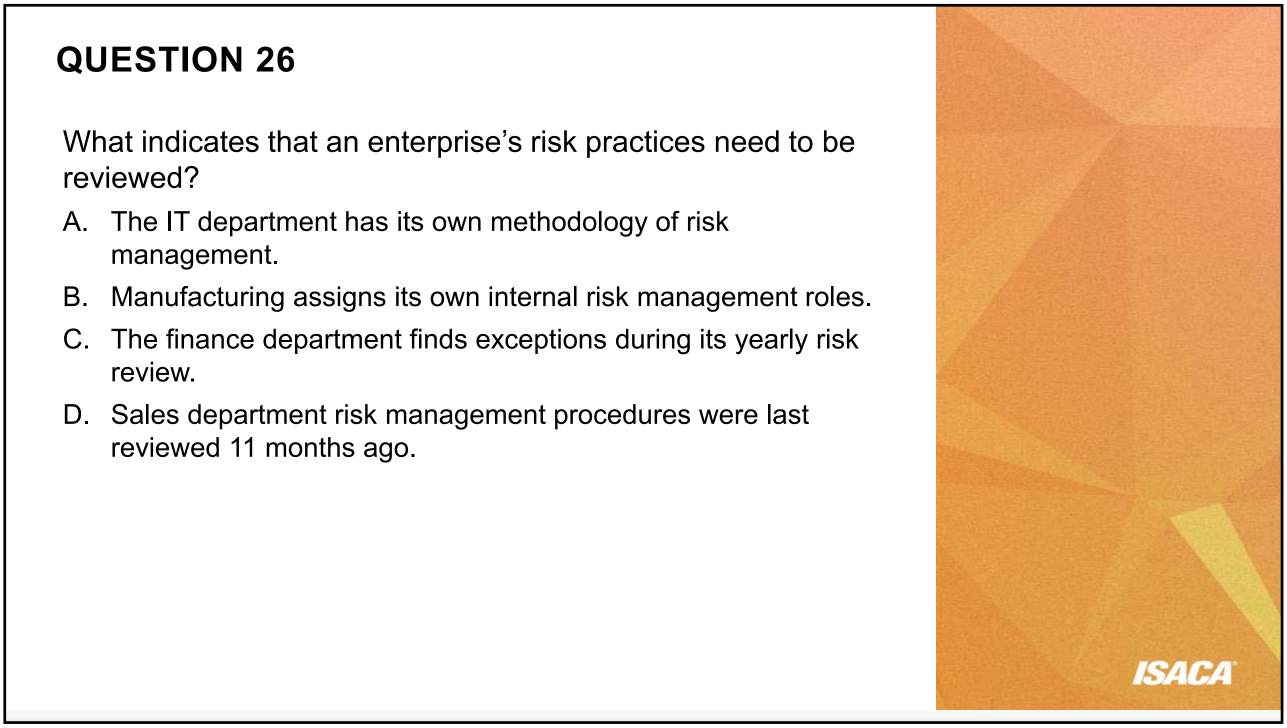
Which of the following devices should be placed within a demilitarized zone (DMZ)?

A. An authentication server

B. A mail relay

C. A firewall

D. A router



QUESTION 26

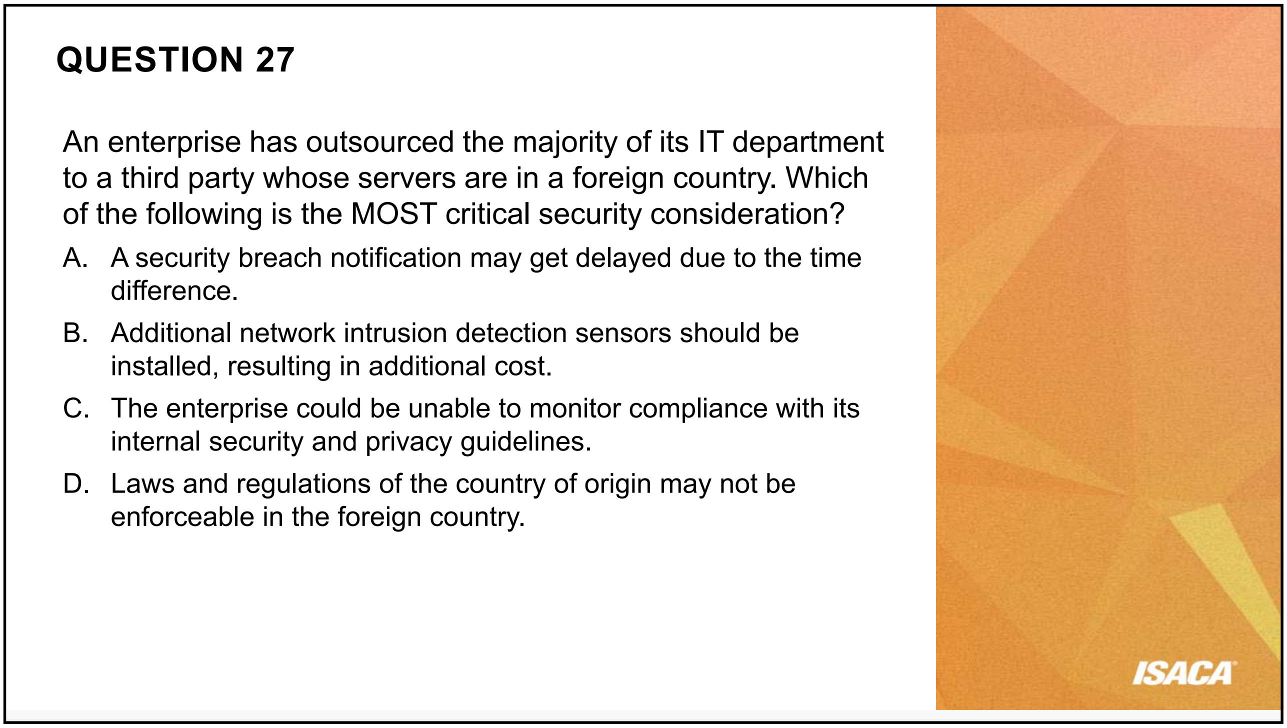
What indicates that an enterprise’s risk practices need to be reviewed?

A. The IT department has its own methodology of risk management.

B. Manufacturing assigns its own internal risk management roles.

C. The finance department finds exceptions during its yearly risk review.

D. Sales department risk management procedures were last reviewed 11 months ago.



QUESTION 27

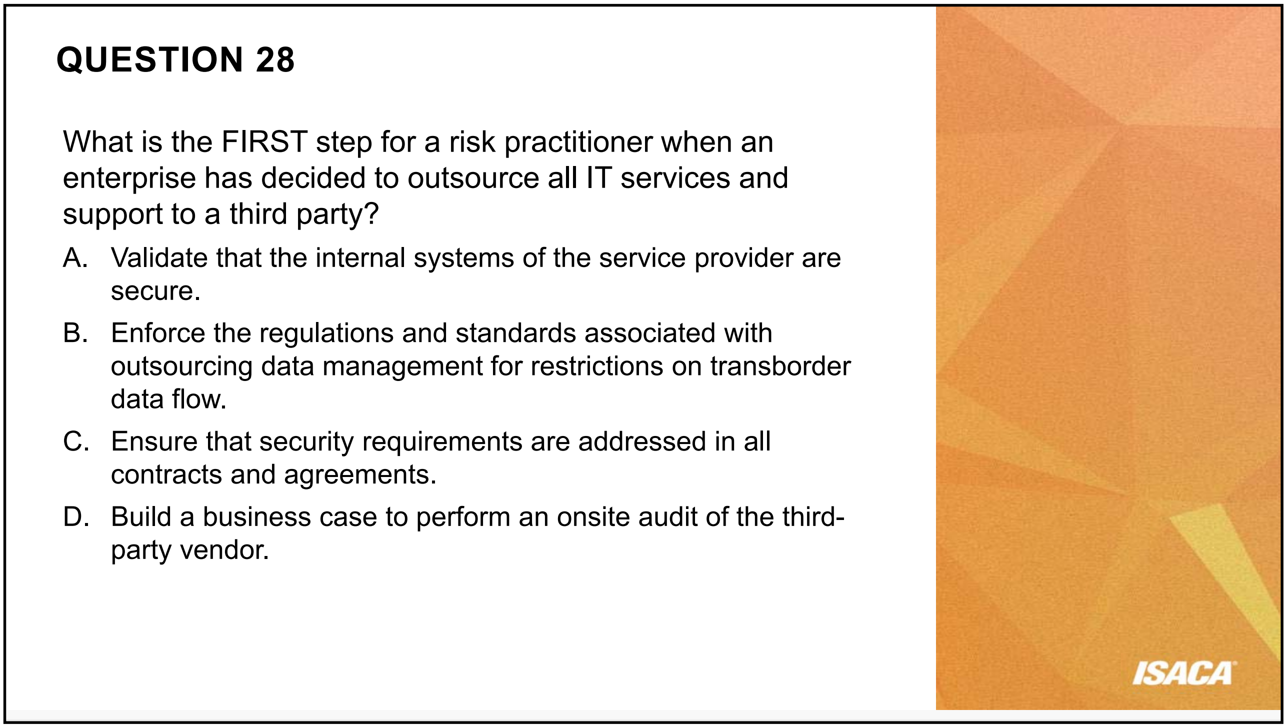
An enterprise has outsourced the majority of its IT department to a third party whose servers are in a foreign country. Which of the following is the MOST critical security consideration?

A. A security breach notification may get delayed due to the time difference.

B. Additional network intrusion detection sensors should be installed, resulting in additional cost.

C. The enterprise could be unable to monitor compliance with its internal security and privacy guidelines.

D. Laws and regulations of the country of origin may not be enforceable in the foreign country.



QUESTION 28

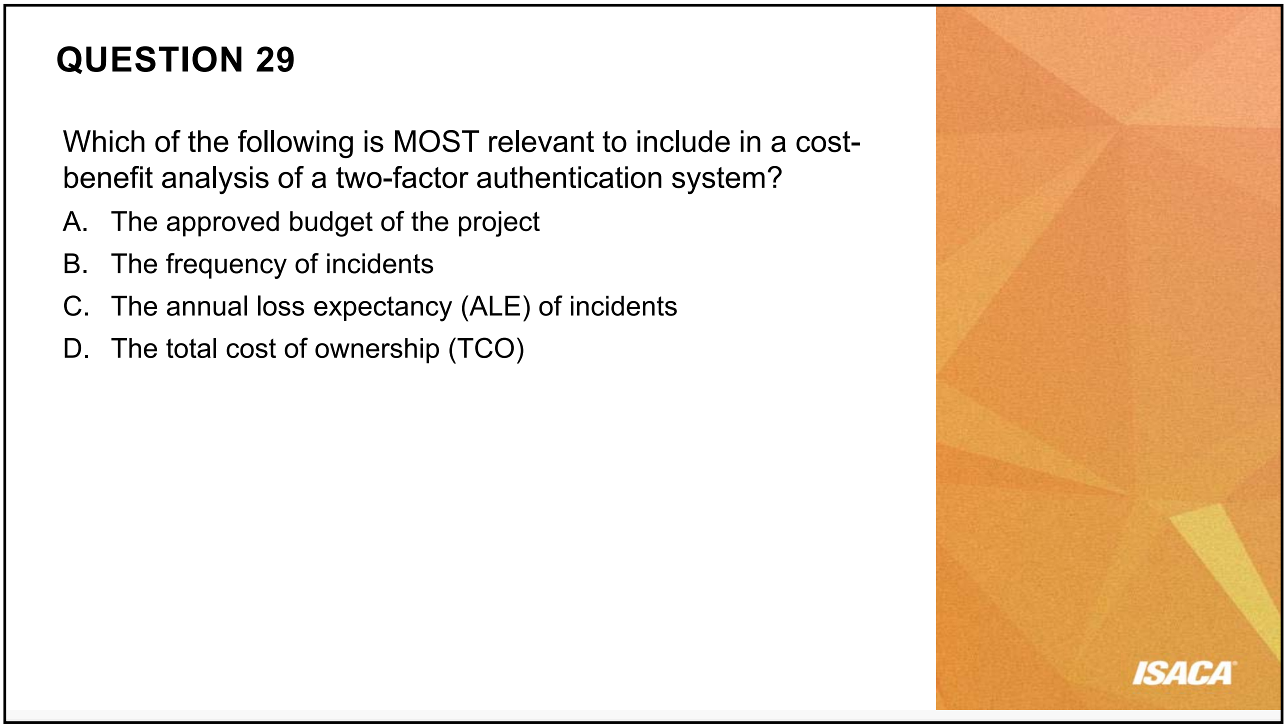
What is the FIRST step for a risk practitioner when an enterprise has decided to outsource all IT services and support to a third party?

A. Validate that the internal systems of the service provider are secure.

B. Enforce the regulations and standards associated with outsourcing data management for restrictions on transborder data flow.

C. Ensure that security requirements are addressed in all contracts and agreements.

D. Build a business case to perform an onsite audit of the third-party vendor.



QUESTION 29

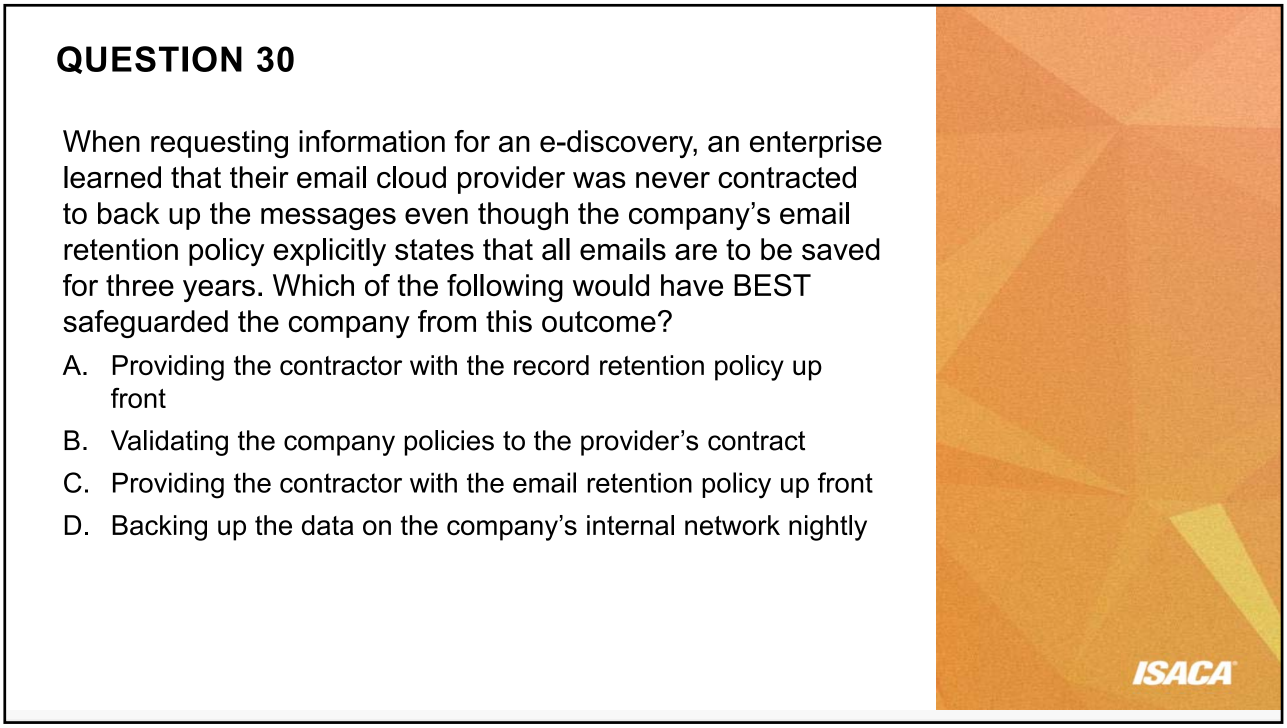
Which of the following is MOST relevant to include in a cost-benefit analysis of a two-factor authentication system?

A. The approved budget of the project

B. The frequency of incidents

C. The annual loss expectancy (ALE) of incidents

D. The total cost of ownership (TCO)



QUESTION 30

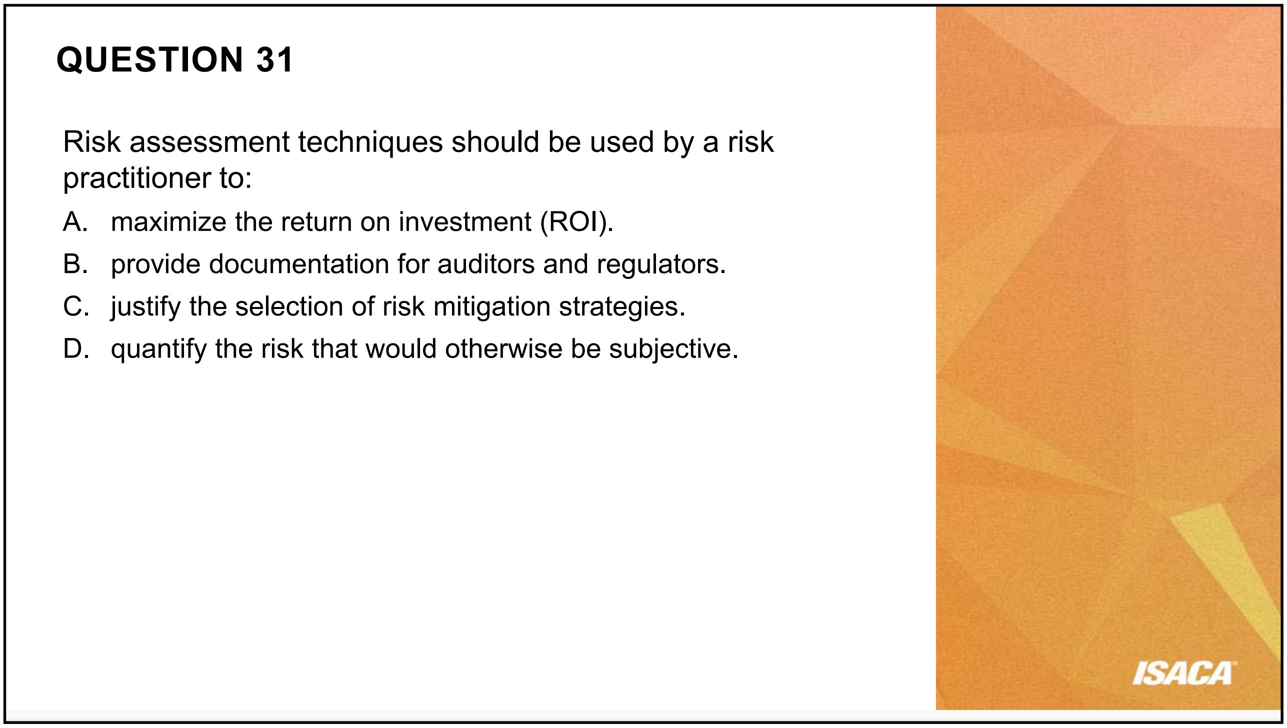
When requesting information for an e-discovery, an enterprise learned that their email cloud provider was never contracted to back up the messages even though the company's email retention policy explicitly states that all emails are to be saved for three years. Which of the following would have BEST safeguarded the company from this outcome?

A. Providing the contractor with the record retention policy up front

B. Validating the company policies to the provider's contract

C. Providing the contractor with the email retention policy up front

D. Backing up the data on the company's internal network nightly



QUESTION 31

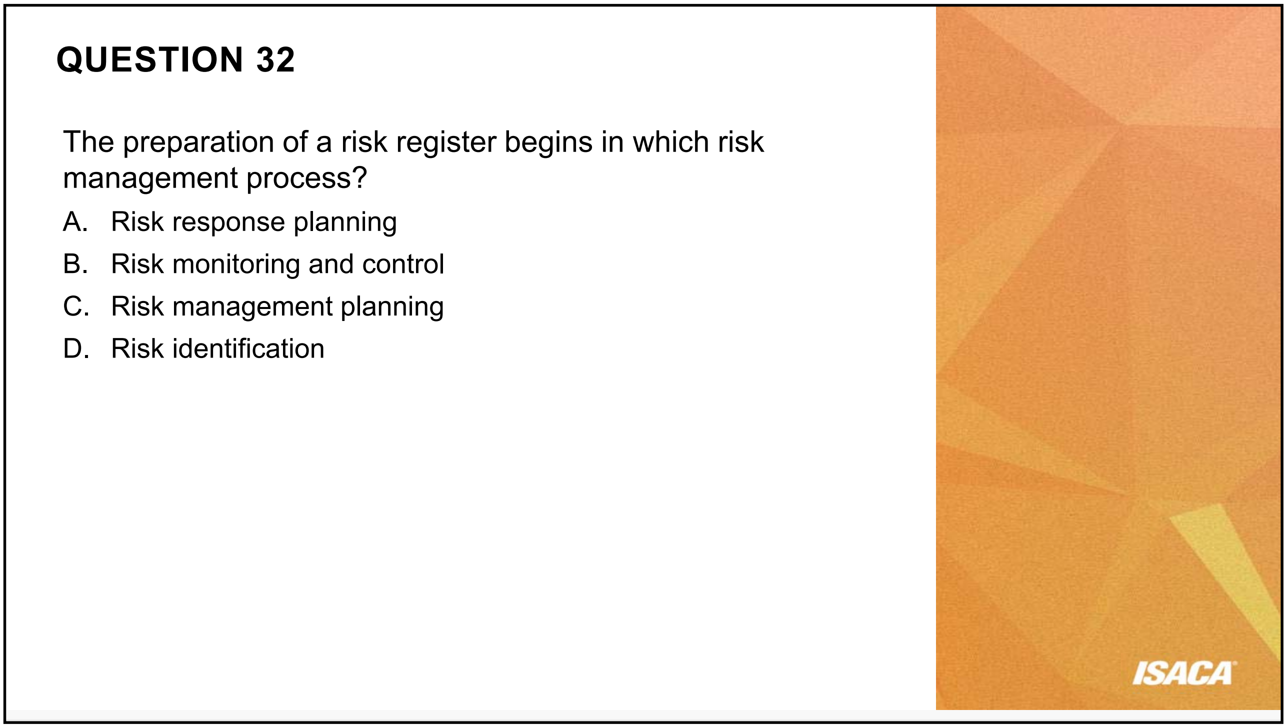
Risk assessment techniques should be used by a risk practitioner to:

A. maximize the return on investment (ROI).

B. provide documentation for auditors and regulators.

C. justify the selection of risk mitigation strategies.

D. quantify the risk that would otherwise be subjective.



QUESTION 32

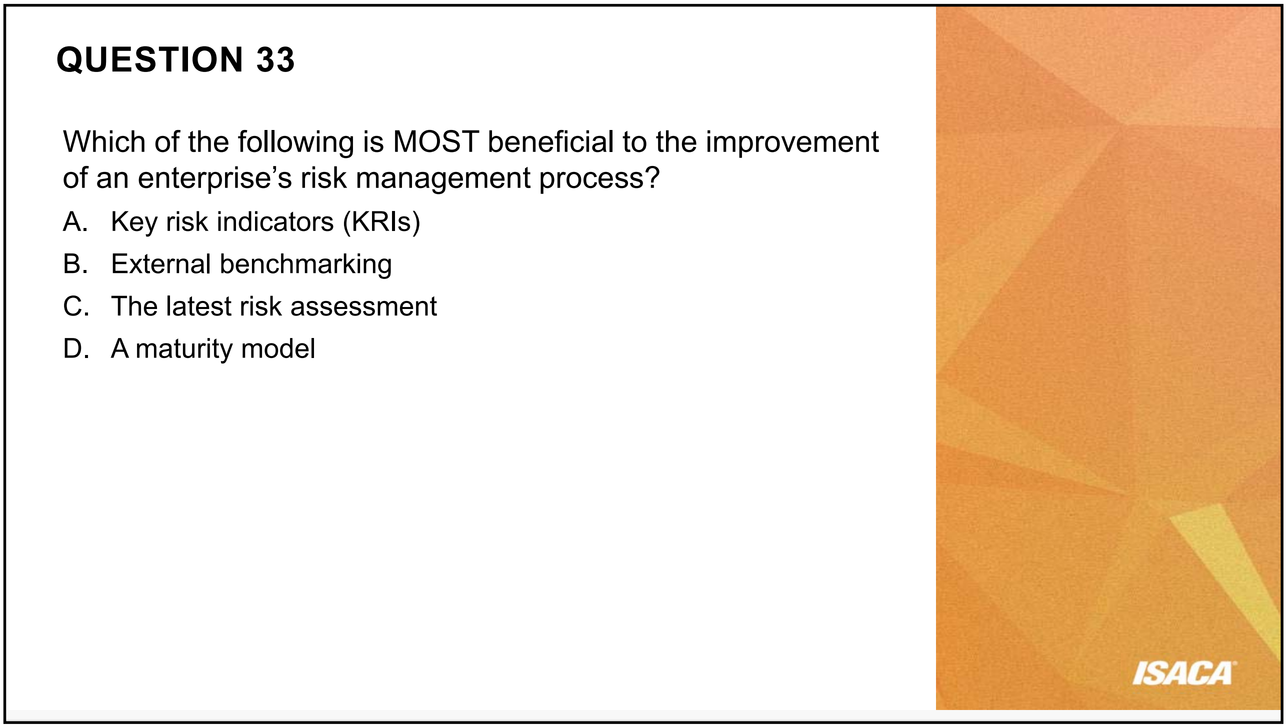
The preparation of a risk register begins in which risk management process?

A. Risk response planning

B. Risk monitoring and control

C. Risk management planning

D. Risk identification



QUESTION 33

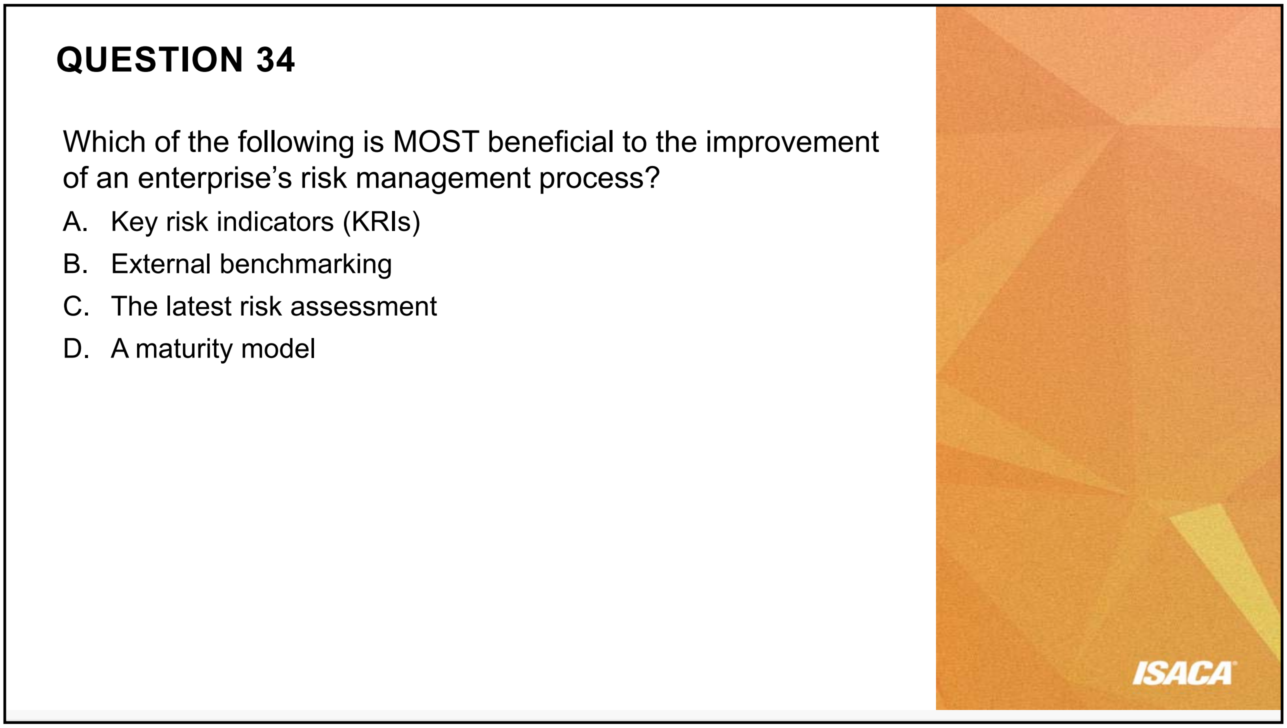
Which of the following is MOST beneficial to the improvement of an enterprise’s risk management process?

A. Key risk indicators (KRIs)

B. External benchmarking

C. The latest risk assessment

D. A maturity model



QUESTION 34

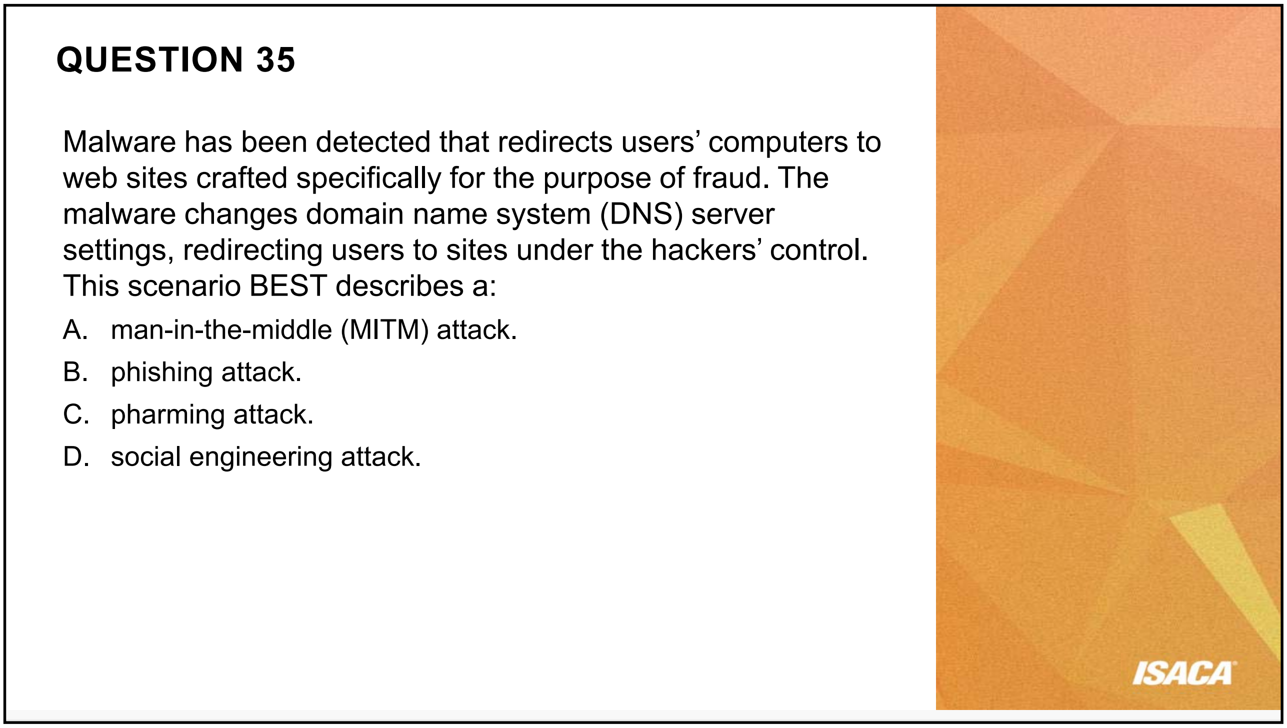
Which of the following is MOST beneficial to the improvement of an enterprise’s risk management process?

A. Key risk indicators (KRIs)

B. External benchmarking

C. The latest risk assessment

D. A maturity model



QUESTION 35

Malware has been detected that redirects users' computers to web sites crafted specifically for the purpose of fraud. The malware changes domain name system (DNS) server settings, redirecting users to sites under the hackers' control. This scenario BEST describes a:

A. man-in-the-middle (MITM) attack.

B. phishing attack.

C. pharming attack.

D. social engineering attack.

THANK YOU!