CRISC - Exam Study Guide

(Certified in Risk and Information Systems Control)

Aligned with CRISC Review Manual - 7th Edition (2021)

Hemang Doshi

To my mother, Jyoti Doshi, and to the memory of my father, Hasmukh Doshi, for their sacrifices and for exemplifying the power of determination.

To my wife, Namrata Doshi, for being my loving partner throughout our life journey together, and to my 7 year-old daughter, Jia Doshi, for allowing me to write this book.

To my sister, Pooja Shah, my brother-in-law, Hiren Shah, and my nephew, Phenil Shah, for their love, support, and inspiration.

To my in-laws, Chandrakant Shah, Bharti Shah, and Ravish Shah, for their love and motivation.

To my mentor and guide, Dipak Mazumder, for showing me how talent and creativity evolve.

– Hemang Doshi

About the author

Hemang Doshi has more than 15 years' experience in the field of IS auditing/risk-based auditing/compliance auditing/vendor risk management/due diligence/system risk and control. He is the founder of www.cisaexamstudy.com and www.criscexamstudy.com, dedicated platforms for CISA and CRISC study, respectively.

Preface

Certified in Risk and Information Systems Control (**CRISC**) is one of the most sought-after courses in the field of risk management, auditing, control, and information security. CRISC is a globally recognized certification that validates your expertise and gives you the leverage you need in order to advance in your career. CRISC certification is key to a successful career in IT risk management. CRISC certification can showcase your expertise and assert your ability to apply a risk-based approach to planning, executing, and reporting on projects and engagements.

It helps to gain instant credibility as regards your interactions with internal stakeholders, regulators, external auditors, and customers.

As per ISACA's official website (www.isaca.org), the average salary of a CRISC holder is USD 117,000 +.

Who this book is for

If you are a passionate risk practitioner, IT professional, auditor or security professional and are planning to enhance your career by obtaining a CRISC certificate, this book is for you.

To get the most out of this book

This book is aligned with ISACA's 7th CRISC Review Manual - 7th Edition (2021) and CRISC Question, Answer and Explanation - 6th Edition (2021) and covers all the topics that a CRISC aspirant needs to understand in order to pass the CRISC exam successfully. The key aspect of this book is its use of simple language, which makes this book ideal for candidates with non-technical backgrounds. At the end of each topic, key pointers from the CRISC exam perspective are presented in table format. This is the unique feature of this book. It also contains exam-oriented practice questions. The questions are designed as per methodology used in an actual CRISC exam. This will help any CRISC aspirant to face the CRISC exam with increased confidence. For more practice questions along these lines, please refer to www.criscexamstudy.com

Recorded Lectures

This book is also available in video lecture format along with 600 plus exam-oriented practice questions in Udemy. Buyer of this book is entitled to 30% off on Hemang Doshi's recorded lectures. For discount coupon, please write at career@infosec-career.com/hemangdoshi99@yahoo.co.in

Get in touch

Feedback from our readers is always welcome. If you have feedback about any aspect of this book, mention the book title in the subject of your message and email us at career@infosec-career.com/hemangdoshi99@yahoo.co.in

Table of Content

ISACA's Thinking Hat

As you all are aware that ISACA's examinations are recognized throughout the globe and hence people across the world enrol for their examinations. It is of utmost importance for the ISACA to use jargons and terminologies in their study materials and examinations that is globally accepted and not restricted to particular country or continent. It is equally important for all of us to understand these jargons and terminologies in the same way as ISACA. For this, we need to let go our local perception and wear the ISACA's thinking hat.

Let us understand some important terminologies from the perspective of ISACA's examination.

Risk

Please do not apply any of the definition that you might be knowing about 'risk' for ISACA's exam. For ISACA 'risk' is a simple term consisting of two elements i.e., probability and impact. Risk is the probability of occurrence of an event which can have impact on the objective of the organization.

Whenever you see the word 'risk', remember two elements i.e., probability and impact.

Probability

ISACA sometimes interchange the word 'probability' with 'possibility' and 'chances'

Impact

Impact is also sometimes referred as 'consequences' and 'losses.'

Risk Management

Risk management indicates combination of following processes:

- Risk Assessment
    - Risk identification
    - Risk analysis
    - Risk evaluation

- Risk Response
- Risk Monitoring

Risk Assessment

Risk Assessment indicates combination of following three processes:

- Risk Identification
- Risk Analysis
- Risk Evaluation

Risk assessment is a process used to identify, analyse and evaluate the risk. Results of risk assessment is used to prioritize the risk and decide appropriate risk response option.

Risk Analysis

Risk analysis is the process to determine the level of risk. Level of risk can be either quantified (i.e., numerical, percentage, dollar amount etc.) or qualified (i.e., low risk, medium risk or high risk etc.)

Risk Evaluation

Risk evaluation is process of comparing the level of risk (as arrived from risk analysis) with acceptable risk level (i.e., risk appetite).

Risk Response

Risk response is also referred as risk treatment.

Risk Response / Risk Treatment

Risk response / risk treatment includes four options:

- Risk mitigation
- Risk acceptance
- Risk avoidance
- Risk transfer

Risk Appetite

Risk appetite indicates organization's willingness to take risk. It is also sometimes referred as acceptable risk.

Risk Tolerance

Risk tolerance means minor deviation from risk appetite.

Risk Capacity

Risk capacity is the maximum amount of risk an organization can tolerate. After this level, existence of the organization is questionable.

Threat & Vulnerability

Threat indicates any factor that can cause harm to the assets of the organization. Vulnerability indicates weakness in the process or system.

Key Performance Indicator

KPI is an indicator to measure the performance of the business target

Key Risk Indicator

KRI is an indicator to measure the level of risk

Key Control Indicator

KCI is an indicator to measure the effectiveness of the control

Threshold

Threshold indicates minimum requirements or maximum limit within which KPI, KRI and KCI is expected to operate.

Chapter 1 – Governance

Chapter 1 consists of topics related to governance and management of IT. Chapter 1 represents 26% of total questions in CRISC exams. In this chapter, we will discuss following topics:

This chapter covers following topics:

1.1 Risk Management Concepts
1.2 Organizational Goals, Objectives and Strategy
1.3 IT Risk Strategy
1.4 Organization Structure, Roles and Responsibilities
1.5 Organization Culture
1.6 Policies and Standards
1.7 Business Process Review
1.8 Organizational Assets
1.9 Enterprise Risk Management & Risk Management Framework
1.10 Three lines of Defence
1.11 Risk Profile
1.12 Risk Appetite, Tolerance and Capacity
1.13 Legal, Regulatory and Contractual Requirements
1.14 Professional Ethics for Risk Management

1.1 Risk Management Concepts

A CRISC aspirants should have basic understanding of risk and risk related concepts. Let us discuss each element of risk management in detail.

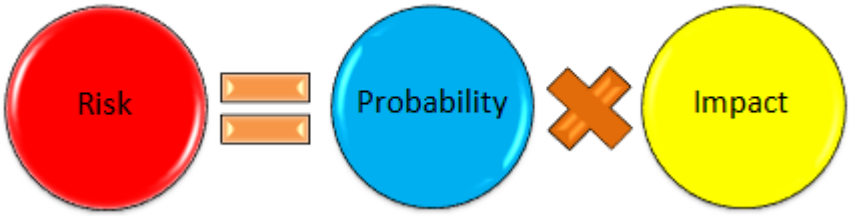
What is Risk?

Let us look into some of the widely accepted definitions of Risk.

Source	Risk defined as	Key Words
ERM-COSO	potential events that may impact the entity.	probability/impact
Oxford Dictionary	the probability of something happening multiplied by resulting cost or benefit if it does.	probability /cost/benefit
Business Dictionary	A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities and that may be avoided through preventive action.	probability/damage
ISO 31000	effect of uncertainty on objectives.	uncertainty/effect
Dictionary	a situation involving exposure to danger.	exposure
ISO/IEC 73	combination of an event and its consequences.	event/consequences

From a CRISC exam perspective, you need not worry about any of the above definitions. If you observe, almost every definition speaks directly or indirectly about two terms: **Probability** & **Impact**. In simplest form, Risk is the product of Probability & Impact.

i.e. Risk= P * I



(Probability is also known as likelihood, possibility, chances etc.)

Both the terms are equally important while determining risk. Let us understand with an example. Probability of damage of a product is very high, let say 1, however that product hardly costs anything and hence Impact is Nil i.e. zero even if the product is damaged. So, risk of rain on articles will be:

Risk = P * I

i.e. Risk = 1 * 0 = 0

CIA Principle

CIA stands for Confidentiality-Integrity-Availability. Risk practitioners are required to have a strong understanding of CIA and the interrelationship between the three principles and a fourth - nonrepudiation.

They are inversely related. To increase one of them results in decreasing at least one of the others or substantially increasing cost. For example: increasing confidentiality increases processing time, which reduces availability.

Confidentiality

Confidentiality refers to privacy of data. Principle of confidentiality requires that data should be available to only authorized users. Confidentiality can be ensured by following principles:

- Access on the basis of need to know
- Access on the basis of least privilege

Integrity

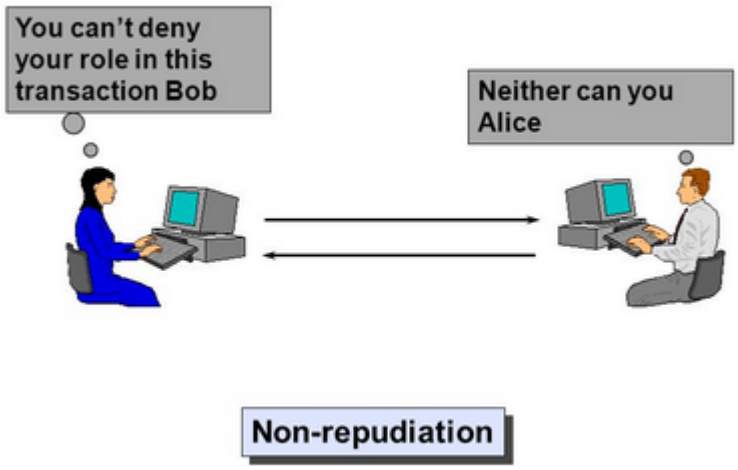
Integrity refers to correctness, completeness and accuracy of data. Principle of integrity requires guarding of data against improper modification, exclusion or destruction of information. Risk practitioners need to have technical expertise to verify integrity controls. Risk practitioners must carefully determine and evaluate risk related to data integrity.

Availability

Availability refers to timely access to information and data. In some cases, near-real-time availability may be needed for safety and system operations. It is very important that the business determines the level of availability requirement for smooth business functioning. Gap between required level and current level of availability indicates availability risks.

To be prepared for a natural disaster, it is appropriate to assume the worst-case scenario. This helps the organization to strengthen its ability to recover.

Non - repudiation



- Nonrepudiation refers to a positive guarantee that a given action was carried out by a given individual or process.
- Nonrepudiation requires tracing of responsibility and enforcing accountability.
- Nonrepudiation can be implemented through digital signatures and certificate-based authentication in a public key infrastructure (PKI).
- Risk practitioners should ensure nonrepudiation is implemented for critical processes such as deletion of records or modification of data.
- Public key infrastructure (PKI) allows senders to provide authentication, integrity validation and nonrepudiation.
- Most important aspect to establish non-repudiation is the use of individual and unique ID. It is difficult to establish whether the non-repudiation is shared or generic IDs are used as there can be multiple users.

Key aspects from CRISC exam perspective

CRISC Question	Possible Answer
What is the greatest concern for users of generic/shared accounts?	• Accountability cannot be established • Non - repudiation cannot be implemented

What is the objective of non-repudiation?	For enforcing responsibility and accountability
How non - repudiation can be implemented?	Nonrepudiation can be implemented through digital signatures and certificate-based authentication in a public key infrastructure (PKI).
Method to provides message integrity, sender authentication and non - repudiation	Public Key Infrastructure
Best method to protect the confidentiality of data being transmitted over a network	• Data encapsulation • Data encryption
Most effective control against insider threats to confidential information	Role based access controls (RBAC)
Once likelihood has been determined, the next step is	To determine the magnitude of impact
Which method is used to provide message integrity, sender authentication and non - repudiation?	• Impact Analysis • Risk Ranking
Confidentiality can be ensured by following principles of:	• Access on the basis of need to know • Access on the basis of least privilege

Practice Questions

1. Risk practitioner noticed that a generic account is used by two or more staff members. Which of the following is the main concern?

A. Repudiation

B. Segregation of duties

C. Password Confidentiality

D. Capturing of audit logs

Answer: A. Repudiation

Explanation: In case of generic ID, the username and password are the same for more than one user. This will impact the non-repudiation of information as it will be difficult to establish which user logged in and performed the transaction. Repudiation is the denial of a transaction by the user. None of the users can be held accountable because each user can deny accountability for transactions performed under the generic account.

2. To ensure message integrity and non-repudiation, which of the following techniques is best?

A. MD 5 Hash

B. Symmetric Encryption

C. Authentication Code

D. Public Key Encryption

Answer: D. Public Key Encryption

Explanation: Public key infrastructure (PKI) allows senders to provide authentication, integrity validation and nonrepudiation. Other options do not serve the objective. Symmetric encryption provides confidentiality. Hashing can provide integrity and confidentiality. Authentication codes provide integrity.

3. While designing risk mitigation for unavailability of IT services during natural disaster, which of the following is the first step?

A. Ensure availability of updated call tree.

B. Arrangement for low cost alternate sites.

C. Employees to be made aware of natural disasters.

D. Worst case scenario analysis.

Answer: D. Worst case scenario analysis.

Explanation: Best strategy would be to consider the worst-case scenario and derive the expected impact. On the basis of expected impact further mitigation action can be planned out. Adequate investment should be made based on an impact analysis.

4. A Risk practitioner noticed that copy of printed documents is saved on the built-in hard disk of the printer. Which of the following is the best course of action?

A. Printer should be configured to automatically wipe all the data on disks after each print job.

B. Risk assessment should be conducted considering the risk of disclosure of data.

C. Printer to be replaced with other printers without any built-in hard disk.

D. Employees to be instructed to delete the data immediately.

Answer: B. Risk assessment should be conducted considering the risk of disclosure of data.

Explanation: Risk assessment will help to determine the level of risk and appetite. On the basis of risk assessment, appropriate risk mitigation techniques can be planned and implemented. Implementing other options are not appropriate without a prior risk assessment because the data may be useful for forensic investigation and may impact performance of the printer.

5. Which of the following is the most effective measure to protect confidential information against insider threats?

A. Log monitoring

B. Information Security Policy

C. Need to know basis access control

D. Network Defense

Answer: C. Need to know basis access control

Explanation: Need to know access control provides access according to business needs; therefore, it reduces unnecessary access rights and enforces accountability. Others are important controls but most effective will be option C.

For more CRISC practice questions visit: https://www.udemy.com/course/crisc-with-hemang-doshi/?referralCode=D9EE73CB3445E8BB1302

1.2 Organizational Goals, Objectives and Strategy

IT governance is also known as enterprise governance of IT (EGIT). IT governance is a process used to monitor and control IT activities. IT governance ensures that information technology provides added value to business processes and also that IT risks are appropriately addressed. It ensures that IT activities are aligned with business objectives. The alignment of IT and business leads to the attainment of business value

The **Board of Directors** is primarily responsible for EGIT. Governance is implemented through leadership, organizational structures, policies that are set out, and performance monitoring to ensure that business objectives are achieved.

CRISC aspirants should be aware of the following aspect of organizational goals, objectives and strategy:

- Business and IT processes should be aligned to achieve the organization's overall objectives.
- It is important that the Board of Directors and senior officials are involved in IT governance.

- Enhanced control over outsourced IT activities.
- Performance monitoring vis-à-vis generally accepted standards and benchmarking with peers.
- A structured approach to monitoring compliance with legal, regulatory, and contractual requirements.

IT governance – success factors

CRISC aspirants should remember the factors mentioned in this section for the successful implementation of EGIT:

- IT governance is primarily the responsibility of directors and senior management. IT governance is designed to ensure the optimal use of IT resources to support business objectives.
- The effectiveness of an IT governance implementation can be determined most effectively by ensuring the involvement of all stakeholders.

- It is very important to define the accountability of each critical function.

- The risk practitioner is required to review the organization's chart to understand the roles, responsibilities, and authority of various functionaries.

- IT can add value to the business only if IT strategies are aligned with the business strategy. The Risk practitioner should determine whether IT and business requirements are integrated and heading in the same direction. A strategic IT plan must contain a clear statement regarding the vision and mission of IT.

- The participation of senior officials is very important to ensure that the information security policy is in accordance with business objectives. Mediation between senior officials in terms of business and technology needs is the best option when it comes to improving strategic alignment.

- To achieve an organization's objective, the IT department should have long- and short-term plans. Plans should be consistent with the organization's business objectives.

- To ensure that IT is continuously supporting the business requirements, it is important to design an internal control framework. Internal control system should be able to detect any mismatch between IT and business alignment and correct the same in timely manner.

Strategic IT Risk

It is very important for a risk practitioner to have thorough understanding of strategic level risk. First step is to understand the business strategy and goals of the organization. This can be best done by discussing with senior executives. Senior executive provides their view about expectations and dependencies from IT. This helps in understanding the potential risks.

Key aspects from CRISC exam perspective

CRISC Question	Possible Answer
How to determine whether IT adds value to the organization?	Alignment of the IT strategy with the organizational strategy
Who has the final responsibility for IT governance?	Board of Directors
What is the main objective of IT governance?	Optimal use of technology resources
What is the best way to gain commitment and support of senior management for information security investment?	To align security risk to enterprise business objectives.
What is the prime purpose of corporate governance?	Provide strategic direction
Risk Management Strategies are primarily based on:	Business objectives and operations
What is main objective of security architecture?	To align the security strategy between the different functional areas of the organization and external parties
What is the primary consideration when selecting a risk response technique?	Enterprise goals and objectives.

Practice Questions

1. Most important aspect to be considered at the time of developing risk management strategy for the organization is:

A. criteria for assessing the risk

B. complexity of technology architecture

C. disaster recovery strategy

D. business objectives and operations

Answer: D. business objectives and operations

Explanation: Main objective of a strategy is to support the business objectives and operations. At the time of development of risk management strategies, the risk practitioner should consider the organization's goals and objectives and tolerance for risk and design risk management framework. Few organizations would like to accept the known risk while other organization implement controls to reduce the risk. Other options are secondary aspects.

2. What is the most effective method to ensure that IT is effective in addressing the business requirements?

A. An internal control system or framework

B. conducting cost benefit analysis

C. analyzing return on investment

D. benchmarking industry processes

Answer: A. An internal control system or framework

Explanation: To ensure effectiveness of IT in addressing the business requirements, organization should design internal control system that monitors whether IT is aligned with the business requirements. To ensure that IT is continuously supporting the business requirements, it is important to design an internal control framework. Internal control system should be able to detect any mismatch between IT and business alignment and correct the same in timely manner. Other options are secondary aspects.

3. Most relevant risk assessment outputs to justify an organization' s information security program is:

A. A list of risk that may impact the organization

B. A list of threat applicable to the organization

C. Evaluation of the impact

D.A list of appropriate controls for addressing risk

Answer: D.A list of appropriate controls for addressing risk

Explanation: Without implemented controls, information security program will have no value. Implementing control is most important aspect of information security program. Risk assessment outputs includes the details of necessary control to reduce the risk. Controls are the prime element for any information security program and justifies the existence of information security program. List of risk is not sufficient as it does not cover how the risk will be addressed. List of threat is not sufficient as it does not address how the risk will be reduced. Evaluation of the impact is not sufficient as it does not cover how to reduce the impact by implementing the control

4. What should be reviewed to determine that whether a risk has been mitigated to an acceptable level?

A. IT requirements

B. Information security requirements

C. Requirements of international standards

D. Organizational requirement

Answer: D. Organizational requirement

Explanation: Organizational requirement are derived from goals and objectives of the organization. When determining the acceptable level of risk, organization requirements are the prime determination. Other options do not consider critical factor of organizational goals and objectives. Other options are not the prime determination.

5. To obtain support from senior management, business case should include:

A. details of the technical risk

B. details of accepted industry practices

C. details of successful attack against competitor

D. details of security risk impacting business objective

Answer: D. details of security risk impacting business objective

Explanation: Senior management is more interested in achieving the goals and objectives of the organization. Tying security risk to key business objectives is the best way to gain support from senior management. Senior management will not be interested in knowing the technical risks or accepted industry practices or successful attack against competitor. They will be more keen to protect their business objectives.

6. What is the main objective of developing enterprise security architecture?

A. to align security strategies among the functional areas of the organization and external entities

B. to ensure that external traffic do not directly communicate with internal network

C. to facilitate the understanding of the organization's technologies and their interactions.

D. to monitor the organization's internal network from external threat

Answer: A. to align security strategies among the functional areas of the organization and external entities

Explanation: The enterprise security architecture should align strategies and objectives of different functional areas within the organization and facilitates structured communication with external partners, customers and

suppliers. strategy. There should be co-ordinated efforts for effective information security. Other options are secondary aspects.

7. Which of the following indicates that risk practitioner needs to review the organization' s risk practices?

A. risk assessment findings are often challenged by business process owners

B. sales department appoints its own risk officer

C. head of the manufacturing department has approved few exceptions for manufacturing processes

D. finance department conduct review of their risk management processes on yearly basis

Answer: A. risk assessment findings are often challenged by business process owners

Explanation: Business process owner are generally the risk owner. They have thorough understanding of business processes and related risk. If they do not agree with risk assessment findings, then it suggests that risk practices area not aligned with business strategies. Other options are normal risk management practices and not the area of major concern.

8. IT plan should be primarily driven by:

A. business strategy and requirements

B. available technology

C. operational procedures

D. laws and regulations

Answer: A. business strategy and requirements

Explanation: Main objective of IT is to support the business strategy and objectives. IT plan should be aligned with business objectives. Other options are secondary aspects.

9. Most significant impact due to lack of strategic planning is:

A. high instances of licensing violations

B. use of obsolete systems

C. improper oversight of IT investment

D. improper incident management process

Answer: C. improper oversight of IT investment

Explanation: Major risk of lack of strategic plan is improper oversight of IT investment. In absence of strategic plan, IT investment may not be aligned with business goals and objectives. Other options are secondary aspects.

10. What is the first step in understanding the strategic IT risk?

A. review IT project risk.

B. understanding organization's strategy from senior executives.

C. develop enterprise architecture strategy.

D. review past IT incident reports

Answer: B. understanding organization's strategy from senior executives.

Explanation: First step is to understand the business strategy and goals of the organization. This can be best done by discussing with senior executives. Senior executive provides their view about expectations and dependencies from IT. This helps in understanding the potential risks. Other options are subsequent steps.

11. What is the main consideration at the time of selecting a risk response technique?

A. responding to all identified risks

B. availability of the resources

C. whether risk response supports the organizational goals and objectives

D. whether risk response is line with industry good practices

Answer: C. whether risk response supports the organizational goals and objectives

Explanation: First and most important consideration is that whether risk response supports the goals and objectives of the organization. Risks that impact the organization's goals and objective should be prioritized and responded first. It is not required to respond to all the risks. Availability of the resource is not the prime consideration. Industry good practice is not the prime consideration.

12.The effectiveness of an IT governance implementation can be most effectively determined by:

A. Ensuring that the objectives are defined

B. Ensuring the involvement of stakeholders

C. The identification of emerging risks

D. Ensuring that relevant enablers are determined

Answer: B. Ensuring the involvement of stakeholders

Explanation: The effectiveness of IT governance implementation can be determined most effectively by involving stakeholders and addressing their requirements. Considering the stakeholder's needs and involving them in the project drives its success.

13. The Risk practitioner noted that roles and responsibilities in terms of IT governance and management are not properly documented and defined. What is the most appropriate recommendation?

A. To review the alignment of IT with business objectives

B. To define the accountability for each critical function

C. To conduct an IS audit on an ongoing basis

D. To create the role of CRO in the organization

Answer: B. To define accountability for each critical function.

Explanation: The IS auditor should recommend defining accountability for each critical function of the organization. Undefined responsibilities constitute a major risk in attaining business objectives. Other options will not add value if accountability and responsibility are not defined.

14.The primary reason for reviewing the organizational chart is as follows:

A. To understand the structure of the organization

B. To understand various communication channels

C. To understand the roles and responsibilities of individuals

D. To understand the network and system architecture

Answer: C. To understand the roles and responsibilities of individuals. Explanation: The primary reason for reviewing the organizational chart is to understand the roles, responsibilities, and authority of the individual. This helps in determining whether there is proper segregation of functions. Options B and D can be determined with the use of a network diagram.

15. Which of the following is the prime consideration in determining whether IT adds value to the business?

A. The alignment of the IT strategy with the organizational strategy

B. Defining organizational accountability

C. Empowering IT with the latest technology

D. Designing a risk management process for the IT department

Answer: A. Alignment of IT strategy with the organization's strategy. Explanation: IT can add value to the business only if IT strategies are aligned with business strategies. The other options are not as important as option A.

16. A major risk associated with a lack of top management support in terms of IT strategic planning is the following:

A. The absence of technical advancement

B. The absence of IT processes, policies, and guidelines

C. A lack of alignment between the technology and business objectives

D. A lack of qualified IT staff

Answer: C. A lack of alignment between technology and business objectives.
Explanation: A major risk arising from the lack of involvement of senior management in supporting IT-related strategic planning is that IT activities are not aligned with business objectives. Investment in IT will be of no value if IT does not support the business objectives.

17. The greatest concern with respect to an organization's governance model is the following:

A. Senior management does not review information security policy

B. The patch management policy is not documented

C. An IS audit is only conducted once every 2 years

D. The IT risk management program only covers critical functions

Answer: A. Senior management does not review information security policy.
Explanation: Participation by top management is critical in ensuring that information security policy complies with business requirements. The information security policy should be reviewed at least once a year to address new and emerging risks. An IT risk management program need not necessarily cover all the functions of the organization. Options B and C are not as critical as option A.

18. For sound IT governance, the IT plan should be consistent with the following:

A. The organization's business plan

B. The organization's business continuity plan

C. The organization's investment plan

D. The organization's information security plan

Answer: A. An organization's business plan.
Explanation: For effective and sound IT governance, IT and business plans should be aligned and should be moving in the same direction. IT should add value to the business.

19. Who among the following is responsible for IT governance?

A. Directors

B. Steering committee

C. CEO

D. CIO

Answer: A. Directors.
Explanation: IT governance is primarily the obligation of the Board of Directors. The Board of Directors is required to ensure that IT activities are moving in the desired direction and that IT is adding value to the business.

20. To achieve the organization's objective, the most important consideration for an IT department is to have which of the following:

A. A budget-oriented philosophy

B. Long- and short-term strategies

C. The latest technology

D. Documented IT processes and guidelines

Answer: B. Long- and short-term strategies.
Explanation: To achieve an organization's objectives, the most important consideration for an IT department is to have long- and short-term plans. An organization's business objective and IT plan should correspond. This is most important consideration of all of the options.

For more CRISC practice questions visit: https://www.udemy.com/course/crisc-with-hemang-doshi/?referralCode=D9EE73CB3445E8BB1302

1.3 IT Risk Strategy

It is very important for a risk practitioner to understand a business's overall risk strategy to guide development of an IT risk strategy that aligns with organizational goals and priorities. IT risk must be measured not only by its impact on IT services but also by the impact of risk on business operations.

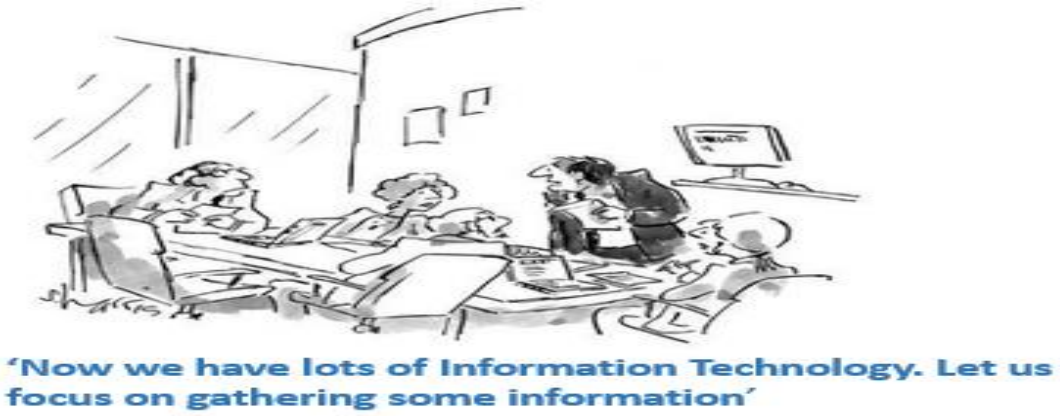
The strategic IT plan is the first policy to create when developing an enterprise's governance model. For a new entity, the first approach is to establish an IT strategy plan. Once the strategy plan is defined, policies and procedures can be designed to support the strategy plan.

Types of IT-related Business Risk

It is expected from a CRISC aspirant to understand below risk:

Type	Description
Access Risk	Risk of unauthorized access resulting in loss of confidentiality.
Availability Risk	Risk that service/data is not accessible when needed.
Infrastructure Risk	Risk of inadequate IT infrastructure and systems to effectively support the needs of the business. Infrastructure includes hardware, networks, software, people and processes.
Integrity Risk	Risk of incomplete, incorrect or inaccurate data.
Investment or Expense Risk	The risk that the IT investment fails to provide value commensurate with its cost or is otherwise excessive or wasteful, including the overall IT investment portfolio.
Project Ownership Risk	Risk of IT projects failure due to lack of accountability and commitment.
Relevance Risk	Risk that the right information may not get to the right recipients at the right time to allow the right action to be taken.
Schedule Risk	Risk of IT projects not completing within expected timelines.

Senior Management Support



Support from senior management is utmost important for the success of the risk management process. Support from senior management ensures budget, authority, access to personnel and information, and legitimacy that will provide a successful result.

Senior management having a strategic view and knowledge of the performance metrics and indicators should be involved in the sign-off process of IT Risk Management.

Interaction with senior management is the best way to understand the goals and objectives of the organization. This gives risk practitioner insight into the potential & evolving risk universe of the organization.

Alignment of risk appetite with business goals and objectives

Risk appetite should be aligned with business objectives. This helps an enterprise to evaluate and deploy valuable resources toward high-risk areas which can impact business objectives.

RACI (Responsible, Accountable, Consulted, Informed)

Following are the four roles that are involved in the risk management process:

Role	Description
Responsible	They are responsible for performing the actual work to meet stated objectives.

Accountable	A single person who oversees and manages the person(s) responsible. He is liable and answerable for the project. For effective accountability, it should be assigned to a specific person.
Consulted	They provide support and assistance to the risk management effort. Consulted personnel may be from other departments or from external sources or from regulators.
Informed	They are not directly responsible for the work effort. The individuals who are informed of the risk management effort but may not necessarily be involved in its execution

The RACI model assists in understanding the relationships or interactions between the various stakeholders and the roles of each stakeholder in the successful completion of the risk management effort.

Organizational Culture, Ethics and Behaviour and the Impact on Risk

Ethics plays an important role in risk management. Organizations with poor ethical standards may be more prone to risk of fraud or theft. Ethics are related to an individual's view about what is right and what is wrong. Policy and processes should be clearly communicated to address the risk of a person violating the ethics. Processes should be visibly enforced and equally applicable for the employees.

Establishing an Enterprise Approach to Risk Management

It is ideal to have a standardized and structured risk management approach that can be applied to the entire enterprise without substantial modification or customization. Results of risk management in one process should be comparable to the results in another.

In absence of a structured approach, there can be a gap in risk measurement of different projects or systems. Risk identified on a system-by-system or project-by-project basis creates new risk of false assurance by having neither consistency nor interoperability among the risk solutions that are implemented.

A critical part of establishing the risk management process is availability of concise and coherent risk management policy.

Key aspects from CRISC exam perspective

CRISC Question	Possible Answer

What is the best approach for development of a corporate policy for an organization operating in multiple countries/regions?	Develop a global policy that can be locally amended to comply with local laws
What is the objective of aligning risk appetite with business objectives?	Resources are directed to areas/processes where risk tolerance is low
Who should provide a final sign-off on the IT risk management plan?	Senior Management
Accountability for the risk to an IT system resides with	Senior Management
Information security governance model depends on:	complexity of the organizational structure
Risk management methodology primarily depends on:	Risk culture of the organization
What is the most important consideration while outsourcing to a foreign country?	Laws and Regulations (privacy laws)
Most effective way to understand the potential impact of law and other contractual requirements on business objectives is:	Compliance oriented business impact analysis
Which should be the first documented to be created while developing IT policies and procedures?	IT strategic plan

Practice Questions

1. Which of the following is the most critical consideration while giving a project to a third-party service provider whose servers are in a foreign country?

A. delay in incident communication due to time difference

B. additional cost due to installation of network intrusion detection systems

C. laws and regulations of origin country may not be enforceable to foreign country

D. difficulty to monitor compliance due to geographical distance

Answer: C. laws and regulations of origin country may not be enforceable to foreign country.

Explanation: A potential violation of local laws applicable to the enterprise or the vendor may not be recognized by foreign countries and hence terms and conditions of SLA may not be enforced. Other options are not the major considerations.

2. What will be the best course of action by a risk practitioner, in case of enactment of a new law impacting security requirements of an organization?

A. to analysis which systems and processes will have impact because of new law.

B. to wait till next review cycle

C. to avail information for course of action initiated by competitors.

D. to notify the system custodians to implement changes.

Answer: A. to analysis which systems and processes will have impact because of new law.

Explanation: To analyze and assess what systems and technology-related processes may be impacted is the best course of action. The analysis must also determine whether existing controls already address the new requirements.

3. Which of the following is the best approach for organizations having operations in multiple countries?

A. Availability of a global corporate policy which excludes all disputed local level content.

B. Availability of a global policy that can be locally amended to comply with local laws.

C. Availability of a global policy that complies with law at corporate headquarters and that all employees must follow.

D. Availability of local policies to include laws within each region.

Answer: B. Availability of a global policy that can be locally amended to comply with local laws.

Explanation: Option B is the only way to minimize the effort and also be in line with local laws.

4. An enterprise which is operating in multiple countries has a single handbook in multiple languages applicable to all the employees. Which is the most important concern?

A. Translation error may remain undetected.

B. Handbook does not include new policies.

C. Expired policies are not removed from handbook.

D. Handbook may not comply with local laws and regulations.

Answer: D. Handbook may not comply with local laws and regulations.

Explanation: It is very important to acknowledge the compliance with all the laws and regulations. Customs and laws play a role in an enterprise's ability to effectively operate in a given location, it is important for the employee handbook to appropriately acknowledge all applicable laws and regulations.

5. To understand the potential impact of law and other contractual requirements on business objectives, which of the following is most effective?

A. Compliance audit

B. Gap analysis

C. Interview with senior management

D. Compliance oriented business impact analysis (BIA)

Answer: D. Compliance oriented business impact analysis (BIA)

Explanation: A compliance-oriented business impact analysis (BIA) will identify all of the compliance requirements to which the enterprise has to align and their impacts on business objectives and activities. Other methods will not provide potential impact of non-compliance.

For more CRISC practice questions visit: https://www.udemy.com/course/crisc-with-hemang-doshi/?referralCode=D9EE73CB3445E8BB1302

1.4 Organization Structure, Roles and Responsibilities

A CRISC candidate is expected to have an understanding of the organizational structure as well as the various roles and responsibilities of important IT functions.

The following table depicts the roles of IT-related functions:

Authority/committee	Description
Board of Directors	IT governance is mainly the responsibility of the Board of Directors.
Strategy committee	• Advises the board on IT initiatives.

	• This committee consists of members of the board and specialist members of the non-board.
Steering committee	• Ensures that the IS department is in line with the goals and priorities of the organization. • The committee must determine whether IS processes support business requirements in order to ensure this. • Monitors and encourages the implementation of IT services in support of business plans for specific projects.
Project steering committee	• This committee consists of a senior representative who will be affected by the new system for each feature. • Provides general feedback and monitors costs and timetables for the project. • Ultimately, the project steering committee is responsible for all project costs and schedules. • The steering committee's role is to ensure the project's progress. • If there are any issues that may impact the expected outcomes, these should be escalated by the steering committee.

Differences between the IT strategy committee and the IT steering committee

A CRISC aspirant should understand the functions of the IT strategy and IT steering committees. The following table outlines the differences between the two committees:

Strategy committee	Steering committee
Members include board members and specialist officers.	Members include the CEO, CIO, and other functionaries as required.
The strategy committee advises the board on IT strategies.	The steering committee focuses on the implementation and monitoring of IT projects.
Responsibilities include: • Aligning IT and business objectives • Identifying any exposure to IT risks	Responsibilities include: • Approving project plans and budgets • Setting priorities and milestones • Acquiring and assigning appropriate resources

• Providing direction to management regarding IT strategies	• Ensuring that the project meets business requirements and providing continuous monitoring • Ensuring the efficient use of IT resources
In a nutshell, the strategy committee sets out the IT roadmap.	In a nutshell, the steering committee drives IT-related projects.

Centralized vis-à-vis decentralized security processes

In a centralized process, information security activities are handled at a centralized place which is mostly head office of the organization. In a decentralized process, implementing and monitoring of security activities are delegated to local offices of the organization.

Following table differentiates between centralized and decentralized processes:

Centralized process	Decentralized process
More consistency in security process	Comparatively less consistency
Optimum utilization of information security resources	Comparatively more resource requirement
Comparatively less alignment with requirements of decentralized units	Better alignment with decentralized unit requirements
Centralized process will generally take more time for processing request due to more gap between IS department and end user.	Faster turnaround of request as compared centralized process

Centralization of information security management will result into greater uniformity and monitoring of the process. This in turn will help in better adherence to security policies

Key aspects from CRISC exam perspective

The following table covers important aspects from the perspective of the CRISC exam:

Questions	Possible answer
The IS steering committee is primarily responsible for:	• Approving and monitoring major projects, the status of IS plans, and budgets • Monitoring project milestones and aligning project and business requirements

	• Prioritizing IT projects as per business requirements
Overall responsibility for system development projects is assumed by:	The steering committee
Who should be member of IT steering committee?	key members from each department.
Who should assume the ownership of a project ?	User management
Who is accountable for ensuring relevant controls over IS resources?	The resource owner (data owner/system owner)
Who has responsibility for data classification?	Data owner
Which level of management is most effective in managing and executing an enterprise's risk program?	Mid-level management
Who must give final sign-off on the IT risk management plan?	Senior Management
Which approach (i.e., top down or bottom up) is more effective for governance?	In top-down approach, policies, procedures and goals are set down by senior management and hence policies and procedures are directly aligned with business objectives. Bottom-up approach may not directly address management priorities. Effectiveness of governance is best ensured by top-down approach.
Who is responsible for evaluating the effectiveness of internal controls system?	System Auditor
Who is ultimately accountable for the risk applicable to the enterprise?	Board of directors

Practice Questions

1. What is the primary role of senior management in implementing a risk management strategy?

A. to develop the metrics to measure the success of risk management program

B. to assess and incorporate the results of risk management into the decision-making process

C. to develop risk scenarios for identification of risk

D. to develop risk management training materials and programs

Answer: B. to assess and incorporate the results of risk management into the decision-making process

Explanation: Senior management is required to assess and incorporate the results of the risk management into decision making process. Senior management is not required to develop metrics or risk scenarios or training materials.

2. Final sign-off on IT risk management plan should be provided by:

A. IT auditors

B. business process owners

C. senior management

D. risk practitioner

Answer: C. senior management

Explanation: Approval from senior management is important to ensure that risk management plan is aligned with goals and objectives of the business. Other options are not authorized to given final sign-off.

3. Overall effectiveness of risk management framework can be ensured by:

A. getting feedback from all the users

B. appointing a dedicated risk manager

C. using statistical risk management approach

D. participation of relevant stakeholders

Answer: D. involvement of relevant stakeholders

Explanation: Overall effectiveness of risk management framework can be ensured by involvement of relevant stakeholders. Stakeholders who are aware of business goals and objectives and who understand the business processes play a meaningful role in the success of a risk management program. Other options are not as significant as involvement of relevant stakeholders.

4. Most effective role to manage and execute the enterprise's risk management program is:

A. mid-level manager

B. senior level manager

C. employees handling the processes

D. board of directors

Answer: A. mid-level manager

Explanation: Management as well as execution of the risk management program can be best handled by mid-level management who are centrally located within the organization hierarchy and they have sufficient understanding of day-to-day business operations. Senior management and board of directors are not required to execute the program. They are expected to provide oversight. Employees handling the processes are generally junior level employees and do not hold enough power and influence to manage and execute the program.

5.A newly joined risk practitioner noted that IT steering committee is responsible to manage and approve all IT policies and procedures. IT steering committee makes all the IT decision for the organization including budget approval. Organization have a:

A. program-based IT structure

B. centralized IT structure

C. decentralized IT structure

D. divisional IT structure

Answer: B. centralized IT structure

Explanation: In this case, all the decisions regarding IT is taken by only one group i.e., IT steering committee and hence organization have a centralized IT structure. In program-based IT structure a temporary group is created to control and monitor one program. In a decentralized organizational structure or divisional IT structurer, decisions are made by each division or business units.

For more CRISC practice questions visit: https://www.udemy.com/course/crisc-with-hemang-doshi/?referralCode=D9EE73CB3445E8BB1302

1.5 Organization Culture

Risk culture is a term describing the values, beliefs, knowledge, attitudes and understanding about risk by an organization. Risk culture is the attitude of senior management to either embrace risk or cautiously accept or avoid risk.

Relationship between Risk Culture & Risk Appetite

It is very important to understand the risk culture of the organization to determine a risk management methodology. Risk management methodology may be completely different for a risk prone organization as compared to a risk averse organization. Both will have different kinds of risk appetite. Risk appetite of the organization depends on the culture and tendency towards risk taking.

Symptoms of Problematic risk cultures

"Today we are going to decide who to blame."

- Clear difference between documented risk appetite and actual demonstrable behavior by employees of the organization.
- In problematic risk culture, discussions focus on blaming each other for problems rather than identifying the root causes.
- Such culture should be controlled, if collaboration is to be nurtured throughout the enterprise.

Benefits of Open communication on Risk

- Main benefit of risk aware culture is timely and accurate escalation of suspicious activity. This helps in more informed risk decisions by senior management.
- Open communication helps in greater awareness among all stakeholders.
- Open communication provides transparency to external stakeholders regarding risk applicable to organization and risk management processes.

Consequences of poor communication on Risk

- Acceptance of risk exceeding the organization’s risk appetite.
- Risk management efforts are not directed towards the organization's objectives.
- Incorrect and negative perceptions by third parties such as customers, investors and regulators.

Indication of matured risk management culture

Culture of the organization indicates the maturity of the risk management. In a highly matured organization, employees recognize the risk to their processes, discuss the risk without any hesitance with an objective to address the same. Employees are encouraged to discuss the risk transparently and to collaborate willingly to resolve it.

Determining the risk culture of the organization

Behavior is one of the key aspects of risk culture. Risk culture of the organization can be determined by observing the behavior of the management and employees. Policies, procedures and countermeasures are influenced by the behavior.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
What is the greatest benefit of a risk aware culture?	• Timely and accurate escalation of suspicious activity. • This helps in more informed risk decisions by senior management
Most important factor to be considered while selecting a risk management methodology?	Risk culture
Risk appetite of the organization depends on	Culture and predisposition toward risk taking
What is the most important factor for selecting an appropriate risk management methodology?	Risk culture of the organization
What is the indication of matured risk management culture?	Employees have appropriate awareness of risk and are comfortable talking about it.

Practice Questions

1. Which of the following is the main advantage of a risk aware culture?

A. suspicious activity is escalated immediately by staffs

B. more emphasis on control effectiveness

C. enhanced knowledge sharing among peers

D. staff are eager to learn about costs and benefits.

Answer: A. suspicious activity is escalated immediately by staff.
Explanation: Main benefit of risk aware culture is timely and accurate escalation of suspicious activity. This helps management to take immediate actions. Option (B),(C) and (D) ultimately makes employees more aware about risk in their environment and as a result events are escalated appropriately.

2. While selecting a risk management methodology, which of the following is the most important factor?

A. cost-benefit analysis

B. control effectiveness

C. risk Culture

D. nature of industry

Answer: C. Risk Culture
Explanation: It is very important to understand the risk culture of the organization to determine a risk management methodology. Risk culture is the attitude of senior management to either embrace risk or cautiously accept or avoid risk. Other options may not be that relevant for selecting risk methodology.

3. For considering risk appetite, which of the following factors is most important?

A. loss absorption capacity of the enterprise

B. complexity of the business

C. risk culture of the industry

D. risk culture and predisposition toward risk taking of the enterprise

Answer: D. risk culture and inclination toward risk taking of the enterprise

Explanation: Two major factors to be considered for risk appetite are risk management culture and the inclination towards risk taking by the management of the enterprise.

4. Selection of appropriate risk management process mostly depends on:

A. cause benefit analysis

B. nature of industry

C. risk culture of the organization

D. root cause analysis

Answer: C. risk culture of the organization

Explanation: It is very important to understand the risk culture of the organization to determine a risk management methodology. Risk management methodology may be completely different for a risk prone organization as compared to a risk averse organization. Both will have different kinds of risk appetite. Risk appetite of the organization depends on the culture and tendency towards risk taking.

5. High maturity of the organization's IT risk management process is best indicated by:

A. employees are aware about the risk and are comfortable talking about it

B. sufficient budget is allotted for IT security

C. risk assessment is encouraged in all the processes

D. IT is aligned with business processes

Answer: A. employees are aware about the risk and are comfortable talking about it

Explanation: Culture of the organization indicates the maturity of the risk management. In a highly matured organization, employees recognize the risk to their processes, discuss the risk without any hesitance with an objective to address the same. Other options are good risk management practice but risk aware culture is most important aspect of a organization with matured risk management processes.

For more CRISC practice questions visit: https://www.udemy.com/course/crisc-with-hemang-doshi/?referralCode=D9EE73CB3445E8BB1302

1.6 Policies and Standards

Risk management program is implemented through a specific set of policies, standards and procedures. Let's understand how each one of these operates.

Policies

A policy is a set of ideas or strategies that are used as a basis for decision making. They are the high-level statements of direction by management.

There can be multiple policies at the corporate level as well as the department level. It should be ensured that department-wise, policies are consistent and aligned with corporate-level policies.

Standards

A standard is a mandatory requirement to be followed in order to comply with a given policy or framework or certification or regulation. Standard provide detailed direction to comply with policy.

A standard helps to ensure an efficient and effective process resulting in reliable products or services. Standards are updated as and when required to incorporate new processes, technology, and regulatory requirements.

Standard is a dynamic document and is changed if control objectives are not achieved or on the basis of result of risk assessments.

Procedures

Procedures are detailed steps and actions that help to support the policy and standards. Generally, procedures are changed more frequently as compared to policy and standards.

Guidelines

In some cases, guidelines are required to implement procedures. Guidelines include information such as examples, suggestions, requirements, and other details for executing procedures.

Document review and updation

All the above documents should be reviewed at periodic intervals to address new and emerging risks. The appropriate version history should be maintained. Security manager should check for currency.

The last review date confirms the currency of the documents and helps to determine that, management has reviewed the standard to meet and address the current business environment.

Security manager should also consider the applicability of policies, standards, procedures and guidelines to third-party vendors and service providers and their adherence to said documents.

Data Classification Policy

Data classification policy plays a pivotal role in defining the level of controls required for each class of assets. Data classification policy includes:

- categories for asset classification
- level of protection to be provided for each category of data
- roles and responsibilities of end users
- roles and responsibilities of system and data owner

Data Retention Policy

Data retention policy defines the retention period for each class data. Two major factors on which data retention period is defined are:

- Business requirements
- Legal and contractual requirements

When data are no longer needed by a particular process, they should be handled according to the law.

Global Policy

- It is very difficult for a multiple national organization to manage different policies for each region. They cannot make a standard policy as different regions have their own local laws.

- Best approach is to have a global policy which can be amended by regions as per their local laws and requirements.

Policy Exceptions

Exceptions to policy are required in few cases where benefits exceed the costs or where taking risk is justified by the relevant benefits. An exception to policies and procedures should only be allowed through a documented and formal escalation process. There should be a structured process for providing exceptions and not merely on the basis of judgement of the process owner or manager. It is always advisable to validate the exception before reporting the same. This will help to rule out any false positives.

Key aspects from CRISC exam perspective

Following are some of the key aspects from exam perspective

Question	Possible Answer
Which document contains high level statement indicating the direction of the management?	Policy
Who should approve the exception to information security policy?	The policy approver
Which policy determines the level of information protection within the organization?	Data classification policy
Primary influencer for data retention policy	• Business Requirement • Legal and contractual requirement
What is the best approach for creating a policy for global organization?	A global policy that is locally amended to comply with local laws
What is the best approach for exception management?	Documented escalation process
Example of management control	Policy and Procedures
Primary reason for a policy exception process is	To allow exception when risk is justified by the benefit
Best metric to monitor the information security program	Adherence to information security requirements
Password is an example of	Preventive Control
Enterprise's approach to risk management is primarily influenced by:	Enterprise policies
Risk aware business decision is primarily based on	Availability of accurate and timely information
What is the major risk of inadequate procedure for assigning data and system ownership?	users may have unauthorized access to create, modify or delete data

Practice Questions

1. "All computer is required to have windows 10 operating system and all server is required to have windows 2008"

A. statement is an example of policy

B. statement is an example of guidelines

C. statement is an example of standard

D. statement is an example of procedure

Answer: C. statement is an example of standard

Explanation: A standard is a mandatory requirement to be followed to comply with a given policy or framework or certification or regulation. Standard help to ensure an efficient and effective process which results in reliable

products or services. Policy is high level statement of management intent and it does not cover above type of requirements. Guidelines and procedures provide details do's and don'ts to support the organization's policies.

2. Functions that should be exclusively performed by information security department is:

A. monitoring the performance of operating system
B. implementing user access of operating systems
C. approving operating system access standards
D. setting firewall rules to protect operating system

Answer: B. implementing user access of operating systems
Explanation: Approving the standards should be performed by information security team. Security team should ensure that standards meet the requirements of security policy. Implementation of the approved standard is to be performed by IT department. Other options are generally performed by IT department.

3. Procedures are correctly linked to security policy through:

A. standards
B. audit
C. maturity model
D. guidelines

Answer: A. standards
Explanation: Standards are the set of minimum requirements to be followed to comply with requirement of security policy. Standards (minimum requirement) are included procedures to ensure that they comply with the intent of policies. Guidelines are generally detailed description of the procedures. Maturity model is adopted to ensure continuous improvement is security process.

4. To ensure compliance with specific regulatory requirement, most appropriate document is:

A. Policies
B. Standards
C. Procedures
D. Guidelines

Answer: B. Standards
Explanation: A standard is a mandatory requirement to be followed to comply with a given framework or certification or regulation. Standard help to ensure an efficient and effective process which results in reliable products or services. Policy is high level statement of management intent and it does not cover specific regulatory requirements. Guidelines and procedures provide details do's and don'ts to support the organization's policies and standards.

5. Information security standard should primarily include:

A. date of creation

B. author of the document
C. approval of the document
D. last review date

Answer: D. last review date
Explanation: Most important element is last review date which helps to ensure currency of the standard and provides assurance that document is reviewed and updated to address the current issues.

For more CRISC practice questions visit: https://www.udemy.com/course/crisc-with-hemang-doshi/?referralCode=D9EE73CB3445E8BB1302

1.7 Business Process Review

- Purpose of a business process review is to the effectiveness and efficiency of processes in achieving its objective.

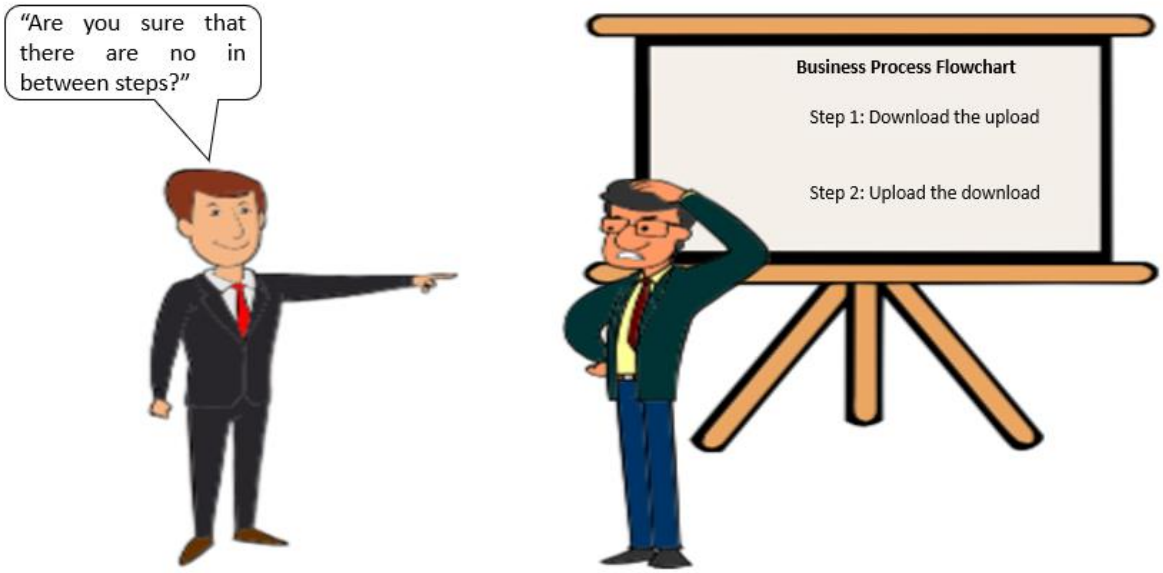
- Business process review is carried out for following objective:

    - To identify the issues with current process
    - To gather information for improvement of the process
    - To review and monitor the progress of the project and milestone

- Business process owners are best to provide feedback about the effectiveness of the IT system. To determine whether an IT system supports the business objectives; it is best to interact with the business process owners. Process owners are well versed about the system functionalities and its linkage to business objectives. They are the first one to notice any loopholes or limitations of the system. Their viewpoint will be unbiased.

- Primary reason an external team reviews documentation before starting the actual risk assessment is to understand the current business process. Risk assessment will be effective only if the assessor is aware about business objectives, business processes and business environment.

- Reviewer should have through understanding of business processes and technology under the scope of review as generally tendency of the process owner is not to reveal enough details for the review. On a lighter note, below picture depicts the same



Business Case

A business case is a justification for a proposed project. The business case is prepared to justify the effort and investment in a proposed project. It captures the reasoning for initiating a project or task. Generally, the business case is the precursor to the start of the project. The business case is a key element in decision-making for any project.

Development of the business case is the responsibility of the project sponsor. The proposed ROIs, along with any other expected benefits, are the most important consideration for decision-making in any new project.

Statement of Work

A statement of work is a contractual document that defines the ownership, liabilities, responsibilities and work agreements between two parties, usually clients and service providers. If statement of work does not include adequate language for intellectual property, it may result in limited or no rights to resulting deliverables. Therefore, it is critical to review statement of work with third-party engagements.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
Who should be interviewed to determine the effectiveness of the system?	Business process owners

What is the primary reason for an external team reviewing the documentation before starting the actual risk assessment?	To understand the current business process

Practice Questions

1.Interaction with which of the following will help to determine whether the IT system supports the business objective?

A. senior management

B. IT dept.

C. business process owners

D. Audit dept.

Answer: C. business process owners

Explanation: To determine whether an IT system supports the business objectives; it is best to interact with the business process owners. Process owners are well versed about the system functionalities and its linkage to business objectives. They are the first one to notice any loopholes or limitations of the system. Their viewpoint will be unbiased. Interaction with senior management, IT dept. and audit dept. will not be as effective.

2. Main purpose of review of documentation before starting risk assessment procedure is:

A. to identify the gaps in the documentations

B. to understand the business processes and business objectives

C. to determine the cost of assignment

D. to understand the technical architecture

Answer: B. to understand the business processes and business objectives

Explanation: Main purpose of review of documentation before starting a risk assessment procedure is to understand the business processes and business objectives. Primary reason an external team reviews documentation before starting the actual risk assessment is to understand the current business process. Risk assessment will be effective only if the assessor is aware about business objectives, business processes and business environment.

3. Accountability for the risk to an IT system that supports a critical business process resides with:

A. senior management

B. IT dept.

C. end users

D. risk management dept.

Answer: A. senior management

Explanation: Accountability for the risk to an IT system that supports a critical business process resides with senior management. IT, risk management dept. and end users support the senior management is implementing various risk mitigation processes and policies.

4.A risk practitioner want to recommend the use of encryption for mobile devices. What is the best way to get this approved from senior management?

A. update management about industry practices

B. analyze the public reports on encryption techniques

C. developing a business case

D. identify vulnerability of unencrypted systems

Answer: C. developing a business case

Explanation: Business case includes cost benefit analysis of implementing a control. Senior management is more interested in reviewing return on investment. Other options will not be as effective as developing a business case.

5. Area of major concern with the use of governance, risk and compliance (GRC) tools is:

A. results may be misinterpreted

B. tool may not cover entire enterprise

C. obsolescence of content

D. complexity in managing the diverse requirements

Answer: C. obsolescence of content

Explanation: Objective of GRC tool is to integrate all the applicable regulations and other requirements at one place for ease of monitoring and ensuring the compliance. However, if GRC application is not updated regularly, tool becomes obsolete with outdated regulations and requirements. This is the area of major concern.

Misinterpreting the results is easily corrected by appropriate training. Organization can implement tool as per their requirements and it is not necessary to cover the entire enterprise. GRC tools are generally designed to manage complex environment.

Complete Book

Complete book is available at following market place. Please write to us at career@infosec-career.com/hemangdoshi99@yahoo.co.in for any queries.

USA

https://www.amazon.com/dp/B08JF5FWLY/ref=cm_sw_em_r_mt_dp_684W9F3ERGMXNXR2WHJ3

India

https://notionpress.com/read/crisc-exam-study-guide

UK

https://www.amazon.co.uk/dp/B08JF5FWLY/ref=cm_sw_em_r_mt_dp_F72VVHY6J0KW6P1CY09N

Denmark

https://www.amazon.de/dp/B08JF5FWLY/ref=cm_sw_em_r_mt_dp_614QSGG89W7Y40JZ6BP6

France

https://www.amazon.fr/dp/B08JF5FWLY/ref=cm_sw_em_r_mt_dp_REEDWVWK5HSJFE0K4TRA

Spain

https://www.amazon.es/dp/B08JF5FWLY/ref=cm_sw_em_r_mt_dp_54F5MS3B1XW1XPKSDGX0

Italy

https://www.amazon.it/dp/B08JF5FWLY/ref=cm_sw_em_r_mt_dp_2KSNJYS7PD3TVMR2E417

Japan

https://www.amazon.co.jp/dp/1636694721/ref=cm_sw_em_r_mt_dp_811XN3N7J8QYMHN774V2

Canada

https://www.amazon.ca/dp/B08JF5FWLY/ref=cm_sw_em_r_mt_dp_D0TTYEHK1QNSK566NWR8

Australia

https://www.amazon.com.au/dp/B08JF5FWLY/ref=cm_sw_em_r_mt_dp_JZKPSCBAHFB0CX411BY6