CRISC EXAM STUDY GUIDE

HEMANG DOSHI

CRISC - Exam Study Guide

(Certified in Risk and Information Systems Control)

Updated in 2020 to align with latest CRISC Review Manual

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 6 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 CISA certificate, this book is for you.

To get the most out of this book

This book is aligned with ISACA's CRISC Review Manual 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 500 plus exam-oriented practice questions. The questions are designed in consideration of the language and testing 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

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

Table of Content

Chapter 1 IT Risk Identification

Risk management begins with risk identification. In this chapter, we'll introduce the risk identification process and its objectives. Risk identification is the process of identification and listing of risks in the risk register.

This chapter covers following topics:

1.1 Risk Capacity, Appetite and Tolerance
1.2 Risk Culture & Communication
1.3 Elements of Risk
1.4 Information Security Risks, Concepts and Principles
1.5 IT Risk Strategy of the Business
1.6 IT Concepts and Area of Concerns for the Risk Practitioner
1.7 Method of Risk Identification
1.8 IT Risk Scenarios
1.9 Ownership & Accountability

1.1 Risk Capacity, Appetite and Tolerance

First step of any risk management learning is to understand following three important terms:

- Risk Capacity
- Risk Tolerance
- Risk Appetite

Let us understand the difference between Risk Capacity, Risk Appetite and Risk Tolerance:

Parameter	Descriptions
Risk Capacity	Maximum risk an organization can afford to take.
Risk Tolerance	● Risk tolerance levels are acceptable deviations from risk appetite. ● They are always lower than risk capacity.
Risk Appetite	Amount of risk an organization is willing to take.

Example:

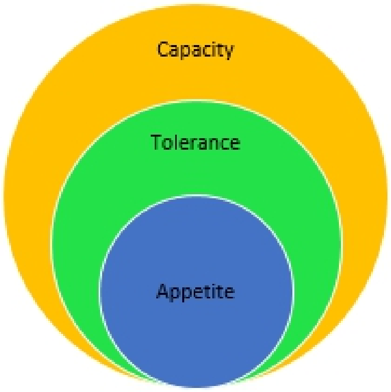
Mr. A's total saving is $1000. He wants to invest in equities to earn some income. Being risk conscious, he decides to invest only up to $700. If the markets are good he is willing to further invest $50. Let us derive risk capacity, risks appetite and risk tolerance from above example:

Risk Capacity: Total amount available i.e. $1000

RIsk Appetite: His willingness to take risk i.e. $700

Risk Tolerance: Acceptance deviation from risk appetite i.e. $750

Relationship between Risk Capacity, Risk Tolerance and Risk Appetite



- Risk Capacity is always greater as compared to tolerance and appetite.
- Tolerance can be either equal to or greater than appetite. Risk tolerance levels are acceptable deviations from risk appetite.
- Risk acceptance generally should be within the risk appetite of the organization. In no case, it should exceed risk capacity.

Periodic review of Risk Appetite & Tolerance

Risk appetite and tolerance need to be reviewed at regular intervals. Factors such as new technology, organizational restructuring, or changes in business strategy may require the organization to reassess its risk portfolio and reconfirm its risk appetite.

It is important that Risk appetite and tolerance should be defined and approved by senior management.

Alignment of Risk Appetite with Business Objective

Risk appetite should be aligned with business objectives to ensure that resources are directed towards areas of low risk tolerance. For critical business processes, risk appetite should be thoroughly monitored and controlled. This will help a risk practitioner to build more controls for the areas or processes where risk appetite and risk tolerance is low.

Let us understand this with an example. An organization has three business objectives. One of them is most critical with 80% of business derived from that area. Other two objectives are not as critical.

Organizations would like to spend more resources on this critical business objective to keep the residual risk within limit.

Compliance with Risk Appetite

Risk practitioners can determine the compliance with risk appetite by evaluating the residual risk i.e. residual risk should be within the risk appetite (i.e. acceptable risk). For example, an organization does not want to expose more than $50 for a given project i.e. their risk appetite or acceptable risk is $50. Organizations will have to keep their residual risk within $50 to comply with risk appetite.

Factors affecting Risk Appetite

Risk appetite differs from organization to organization. Risk prone organizations may have high levels of risk appetite whereas risk averse organizations may have low levels of risk appetite. Organization adopts their risk appetite on the basis of their culture and predisposition towards risk taking.

Responsibility of monitoring the Risk

Risks should be monitored on a continuous basis and results of the monitoring should be communicated to respective risk owners. Risk owners are responsible to ensure that risk is within the tolerance level.

Benefits of defining risk capacity, appetite and tolerance

Risk capacity, appetite and tolerance are the deciding factor for prioritization of risk response. Risks with low appetite need to be addressed immediately. Following are the benefits of defining risk capacity,appetite and tolerance.

- It provides evidence of the risk-based decision-making processes.
- It helps to understand how each component of the enterprise contributes to the overall risk profile.
- It helps in prioritization and approval of risk response.
- It helps in identifying specific areas where a risk response is warranted.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
Why should risk appetite be aligned with business objectives?	To ensure that resources are directed towards area of low risk tolerance
How to determine the compliance with risk appetite?	Risk appetite is said to be complied when residual risk is within acceptable risk level

Which is the most important factor that determines the level of risk appetite of the organization?	Culture and predisposition toward risk taking
Management generally allows some deviation from defined risk appetite. This is known as	Risk tolerance
What are the deciding factors for the prioritization and mitigation of risk?	Risk Tolerance and Risk Appetite
Results of continuous monitoring should be best communicated to	Risk owner

Self-Assessment Questions

(1) Most important reason for alignment between risk appetite and business objective is to ensure that:

A. objectives with high risk areas are given priority
B. all risks are identified and eliminated
C. common IT and business goals are identified
D. the risk framework is appropriately communicated

Answer: A. objectives with high risk areas are given priority.
Explanation: Risk appetite is the amount of risk an organization is willing to take. If risk appetite is aligned with business objectives, valuable resources can be deployed toward those objectives where the risk is high.

(2) Which of the following best provides information with respect to adherence to risk appetite of an enterprise?

A. level of preventive and detective controls
B. level of inherent risk and acceptable risk
C. level of residual risk and acceptable risk
D. level of threat and vulnerabilities

Answer: C. level of residual risk and acceptable risk
Explanation: Risk appetite is the amount of risk an organization is willing to take. Residual risk is measured after controls are implemented. Management can decide whether to accept the risk or apply more controls based on acceptable risk levels. Other options will not give relevant information about risk appetite.

(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 inclination 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 toward risk taking by the management of the enterprise.

(4) Which of the following describes acceptable deviation from risk appetite?

A. risk avoidance.
B. risk tolerance.
C. risk acceptance.
D. risk mitigation.

Answer: B. risk tolerance
Explanation: Risk tolerance levels are deviations from risk appetite. Risk tolerance is the permissible deviation from declared risk appetite levels.

(5) Risk appetite of an organization is moderate. However, a critical application has been evaluated and found to have high risk. Which is the best next action?

A. Replace high risk application with another system.
B. Risk appetite to be increased.
C. Evaluate controls to be implemented on the system to mitigate the high risk.
D. Evaluate other risk frameworks to bring down risk to acceptable levels.

Answer: C. Evaluate controls to be implemented on the system to mitigate the high risk.
Explanation: First step will be to determine whether new controls to be implemented on the system may lower the risk from high to moderate or low before taking any further action. Other options may not address the issue.

(6) Most important factor in determining risk mitigation strategy is:

A. Threat analysis
B. Risk appetite & tolerance level
C. Vulnerability assessment results
D. Control assessment results

Answer: B. Risk appetite & tolerance level
Explanation: Risk appetite is the amount of risk an organization is prepared to take. Risk tolerance levels are acceptable deviations from risk appetite. The risk tolerance level along with risk appetite determines the risk culture of organization and is the most important factor in determining risk mitigation strategy.

(7) Results of risk monitoring of a critical application are best communicated to:

A. risk owner
B. risk management department
C. external auditor
D. application developer

Answer: A. risk owner
Explanation: The risk owner is the most suitable target audience for results of monitoring because they own the risk and they need to ensure that appropriate risk responses are executed in alignment with the enterprise's risk appetite.

1.2 Risk Culture & Communication

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.

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

Self-Assessment 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.

1.3 Elements of Risk

It is very important for a CRISC aspirant to understand following terminology associated with risk identification:

Term	**Definition**
Impact	Magnitude of loss
Impact Analysis	Analysis to understand which assets are critical (on the basis of cost or consequences if those assets are not available or damaged).
Impact Assessment	Assessment of possible consequences of a risk.
Likelihood	Probability
Threat	Something that is capable of harming assets.
Threat Agent	Methods, resources, capacity etc. which is used to exploit vulnerability.
Threat Analysis	Analysis to understand the nature of events or actions that can result in adverse consequences.
Threat Vector	Path or route used by threat to gain access to the target.
Vulnerability	Weakness in the process or system.
Vulnerability Analysis	Analysis to identify, understand and classify different vulnerabilities.
Vulnerability Scanning	Proactive and automated process to identify weakness in the system or processes.

Risk Factors

It is very important to have knowledge of threats including motivations, strategy and techniques of those who perpetrate threats to manage the threat. The better understanding the risk practitioner has

of the mind of the attacker or the source of the threat, the more effective the risk management activities will be in controlling the threat.
At the same time an enterprise needs to know its own weaknesses, strengths, vulnerabilities and the gaps.

Assets

Following table list down IS assets and their related risks:

Assets	Risk
People	● Many organizations fail to identify key employees and ensure that appropriate back-up arrangements are in place. ● In case of exit of a key person by way of retirement or illness or recruitment by another organization, the organization may be in a vulnerable position.
Technology	● Risk practitioners should consider the risk of using outdated technology. ● For outdated technology lack of patching and updating of systems and applications leaves them vulnerable to malware. ● The risk practitioner should be sure that procedures are in place to securely delete data when systems are scheduled for disposal ● Common methods of destroying data include overwriting, degaussing and physical destruction of the equipment.
Data	● Data can be either sensitive or critical or may be both sensitive and critical. Sensitive data must be protected from disclosure or modification, while critical data must be protected from destruction or loss. ● Data should be protected at all times, in all forms (paper, magnetic storage, optical storage, reports, etc.) and in all locations (storage, networks, filing cabinets, archives, etc.).
Intellectual Property	● Intellectual property includes trademarks, copyrights, patent, trade secrets etc. ● Failure to protect intellectual property may result in the loss of competitive advantage. ● Intellectual property should be protected by adequate means such as access controls, shredding of documents, encryption techniques etc.
Business Processes	● It is advantageous to have flexible business processes to adapt to changes in the market or technology.

	● Outdated processes possess significant risks for the organization.

Asset Valuation

The risk practitioner should determine criticality of each asset so that priority may be given to protecting the critical assets first and addressing other assets as per requirement. This ensures that the cost of controls is not more than the cost of assets. Following are some factors for calculating asset value:

- Reputational loss and other penalties for legal noncompliance
- Impact on associated third parties, business partners
- Impact on business continuity
- Monetary loss
- Breach of contracts
- Loss of competitive advantage
- Legal costs

Generally, asset value is calculated on the basis of impact on confidentiality, integrity and availability (CIA). However, it is important to standardize the terms and values to be used by all the departments.

Threats

Key responsibility of a risk practitioner is to ensure that various types of threats applicable to an organization are identified and documented. Threats which are not identified are more vulnerable than a threat that is well documented.

Threat identification

Sources of threat identification include past incidents, audit reports, media reports, information from national computer emergency response teams (CERTs), data from security vendors and communication with internal groups. Risk scenarios are used at the time of threat and vulnerability assessment to identify various events and their likelihood and impact.

Controls for internal threats

Risk practitioner should ensure following controls for Internal Threats:

- System access to be provided on the basis of need-to-know and least privilege.

- To ensure stringent background verification (where permitted by law) process before hiring any employee. It is important to review the qualifications and attitude of prospective employees.

- Employees should be required to sign a nondisclosure agreement.

- Regular awareness sessions and management reviews to remind employees of organizational policies and their responsibilities.

- Exit policy to be properly defined and implemented. At the end of employment, an employee should return all organizational assets (e.g., laptops, mobile phones, access cards, etc.) so it cannot be misused. All logical and physical access should be disabled immediately.

Controls for external threats

Risk practitioner should ensure following controls for External Threats:

- Use of government data and weather monitoring services to identify natural events like flood, earthquake etc. and to take necessary steps to be prepared for such events.
- To carry out risk assessment and audit of IT infrastructure and bridge the gap by establishing necessary controls.
- Use of skilled workforce, effective tools and techniques to guard the assets against the highly skilled hacking community.
- Most breaches happen because targets are not well prepared. Many organizations are breached because they were identified as soft targets and hackers took advantage of their vulnerabilities.

Emerging Threats

Emerging threats are indicated by:

- unusual pattern or activity on a system,
- frequent alarms,
- unusual system or network performance,
- increase activity in logs.

- Even though logs are captured, they are not monitored or acted on a timely basis and hence compromise cannot be prevented.
- New technology without proper security consideration becomes a source of new vulnerabilities.
- It is very important for the risk practitioner to monitor the use of new technologies particularly if these technologies promise cost savings or competitive advantage.

Difference between Vulnerability & Threat

One of the favorite and most preferred game of ISACA is to get us confused between the terms 'vulnerability' and 'threat' during CRISC exams. Let us understand basic difference between the two so they cannot trick us anymore.

Threat	Vulnerability
A threat is what we're trying to protect against.	Vulnerability is a weakness or gap in our protection efforts.
Our enemy can be Earthquake, Fire, Hackers, Malware, System Failure, Criminals and many other unknown forces.	Vulnerability can be in the form of weak coding, missing anti-virus, weak access control and other related factors.
Threats are not in our control.	Vulnerabilities can be controlled by us.

Vulnerabilities

- Vulnerabilities are weaknesses in the security. Existence of vulnerability is a potential risk.
- It represents lack of adequate controls.
- An organization should conduct regular vulnerability assessments and bridge the gap before they are found by an adversary and exploited.

Network Vulnerabilities

- Network vulnerabilities are often related to poor installation and misconfiguration of equipment.
- Misconfiguration and failure to update operating system (OS) code correctly and on a timely basis possess very high risk.
- Network equipment should be hardened by disabling any unneeded services, ports or protocols. Any open services can be exploited by an attacker.
- Risk practitioners should have sufficient information about emerging technologies and related vulnerabilities.

Physical Access

Physical controls are a very important aspect in security as threat agents who are able to circumvent physical access to systems have the potential to bypass nearly every other type of control.
Physical security controls include locks, CCTV monitoring, biometric access control, security guards, fire suppression systems, heating ventilation and air conditioning controls, lighting, and motion sensors.

Applications and Web-facing Services

One of the most common entry points for hackers is web based applications. Applications are vulnerable to attacks like buffer overflows, logic flaws, injection attacks, bugs, and many other common vulnerabilities.

Applications located at insecure locations such as demilitarized zones are more vulnerable to an attack. It is recommended for risk practitioners to use tools from the Open Web Application Security Project (OWASP) to test web-facing applications.

Utilities

- The risk practitioner should ensure that an adequate backup facility is available in case of power failure or other environmental conditions.
- Equipment such as uninterruptible power supply (UPS), backup generators and surge protectors can help to prevent system damage or failure.
- Functioning of these equipment must be tested at regular intervals.

Supply Chain

It is important to identify and document all risks related to the supply chain. Any interruption in the supply chain may affect the ability of the organization to function.

Processes

Operational processes must be defined and implemented in a consistent manner across the organization. Unstructured processes result in inconsistent management, lack of governance and reporting, and failure to ensure compliance with regulations.

Equipment

Equipment should be monitored for its MTBF (mean time between failure) that indicates its anticipated life span and when it should be scheduled for removal or replacement.

Cloud Computing

Four cloud deployment models are listed below:

Private Cloud	Public Cloud	Community Cloud	Hybrid Cloud
Available for only private use of enterprise	Available for use of general public	Available for use by specific communities having common interest or mission.	A composition of two or more clouds (private, community or public)
Managed by either enterprise or by third party.	Managed by cloud service providers.	Managed by either enterprise or by third party.	
Physically may exist on- or off-premise	Physically exist off premise	Physically may exist on- or off-premise	

- Risk practitioners should be aware that outsourcing of IT services does not remove accountability of the organization.
- Risk of cloud computing should be considered before making outsourcing decisions.
- Laws and regulations of the country of origin may not be enforceable in the foreign country. At the same time, the laws and regulations of the foreign outsourcer may also impact the enterprise.
- Organizations can enforce strong security controls by the supplier only if the same is included in SLA. Without addressing security requirements directly in the outsourcing contract, the outsourcing company has no assurance that the provider will be compliant with specific security requirements.
- Right to audit is an important clause. However, service providers may not allow you to audit them directly. Instead they may provide a proof of compliance conducted by an independent auditor.

Big Data

Risk associated with big data:

- As all the data is stored at one place for analysis, any unauthorized access can have adverse impact.
- Analysis of data without the consent of the subject, can impact privacy laws.
- Also, when data is aggregated for analysis, information that is not individually identifiable information might become identifiable.

Vulnerability Assessment and Penetration Testing

- Lack of adequate controls indicates a vulnerability. Vulnerability can be exposed by a threat which results in risk of confidentiality, integrity and availability.
- Vulnerability assessment is a process to identify weakness in the system or processes.
- It can be carried out either by a manual process or automated tools.
- Automated tools have the ability to analyze large amounts of data, run multiple tests and identify weakness.
- A manual test will give better results when content is not easily quantifiable and requires judgment.
- To validate the results of a vulnerability assessment, the organization may conduct a penetration test.
- An expert penetration testing team uses the same tools and techniques as used by a real hacker.
- It is advisable to conduct penetration after any major infrastructure changes are made.
- Findings of VA & PT should be used by risk practitioners to bridge the gaps.
- At the same time, absence of any findings, should not be considered as a full proof system. The system may still remain vulnerable to unknown vulnerabilities (zero day exploits).
- Configuration management has the greatest likelihood of introducing vulnerabilities through misconfigurations and missing updates.
- To determine the threat and vulnerability, risk scenarios are used for all elements of a business process and attempt is made to identify the likelihood of occurrence and the business impact if the threats were realized.

Configuration Management

Configuration management is the process of managing and updating system features, parameters and other functional settings. Misconfiguration and missing updates is the reason why configuration management is considered as the most susceptible to the introduction of an information-security-related vulnerability.

Misconfiguration and failure to update operating system (OS) code correctly and on a timely basis possess very high risk. Hackers will first try to exploit the vulnerabilities due to poor configuration.

Risk practitioners should ensure that the organization is having a robust configuration management process in place.

Input Validation Check

Absence of input validation check is one of the most serious vulnerabilities and allows attackers access to data through a web application.

In absence of validation checks in data input fields, attackers can exploit other weaknesses in the system. For example, through SQL injection attacks, hackers can illegally retrieve application data.

Risk practitioner to ensure that all the web applications should have appropriate input validation control to restrict entry of any unusual code in the system.

Off-shore Data Processing

Most important factor to be considered while evaluating the proposal of off-shore data processing is prevalent laws and regulations. Risk practitioners should be aware about privacy laws and its requirements. Privacy law may prohibit transfer of sensitive customer data to an off-shore location.

Outsourcing Contracts

Risk practitioner should consider following important aspect with respect to outsourcing contracts:

- Outsourcing contracts should include information security requirements for the service provider. If security requirements are not covered in outsourcing contracts, it will be difficult to get the same implemented by service providers.
- Service providers should not be allowed to subcontract the critical processes. Subcontracting increases the risk of data leakage.
- Outsourcing contracts should have provision to access the compliance of the service provider. Compliance can be verified through internal audit or by obtaining a certificate from an independent auditor.

Compliance oriented business impact analysis

Purpose of a compliance oriented business impact analysis is to identify all the compliance related requirements applicable to the organization. These requirements are mapped with business processes and objectives.

It is the most effective method to evaluate the potential impact of legal, regulatory and contractual requirements on business objectives.

Key aspects from CRISC exam perspective

CRISC Question	Possible Answer

Which process is most susceptible to the introduction of a vulnerability?	Configuration Management
Lack of adequate controls indicates	Vulnerabilities
Risk scenario is primarily used in	Threat and Vulnerability Assessment
When should the penetration test be performed?	On periodic basis and when major infrastructure related changes are made
Hackers targeting well known start-up company is known as	Emerging threat
Most important consideration for data transferred to offshore location	● Laws and regulations (specifically privacy laws) ● Inclusion of security controls in the outsourcing contract
Which process helps to evaluate legal and regulatory impact on business objectives?	Compliance oriented business impact analysis (BIA)
Development of information security policy is primary based on	Assets

Self-Assessment Questions

(1) Which of the following areas is most vulnerable from an information security perspective?

A. Backup process
B. Database management process
C. Configuration management
D. Disaster Recovery management

Answer: C. Configuration management
Explanation: Most vulnerable among the above options is configuration management. Misconfiguration and failure to update operating system (OS) code correctly and on a timely basis possess very high risk. Other options are generally less susceptible as compared to configuration management.

(2) Which of the following represents lack of adequate controls:

A. Vulnerability.
B. Likelihood
C. Threat
D. Impact

Answer: A. Vulnerability.
Explanation: Vulnerabilities are weaknesses in the security. Existence of vulnerability is a potential risk. It represents lack of adequate controls.

(3) Which of the following vulnerabilities allows attackers access to data through a web application?

A. Validation checks are missing in data input fields.
B. Password history rule not implemented.
C. Application logs are not monitored at frequent intervals.
D. Two factor authentication not implemented.

Answer: A. Validation checks are missing in data input fields.
Explanation. In absence of validation checks in data input fields, attackers are able to exploit other weaknesses in the system. For example, through SQL injection attacks, hackers can illegally retrieve application data. Other options may make applications vulnerable but these can be countered in other ways.

(4) To estimate likelihood and impact of and probable event, risk scenarios are used by:

A. IT audit
B. GAP Assessment
C. Threat and vulnerability assessment
D. Security assessment

Answer: C. Threat and vulnerability assessment
Explanation: Risk scenarios are used at the time of threat and vulnerability assessment to identify various events and their likelihood and impact. In other options, risk scenarios are not used.

(5) Penetration test is to be best performed when:

A. there is change in systems staff.
B. an attempt to penetrate has occurred.
C. system infrastructure is modified.
D. gap assessment results are available.

Answer: C. system infrastructure is modified.
Explanation: The BEST time to perform a penetration test is after infrastructure changes are made. Changes in the systems infrastructure are most likely to inadvertently introduce new exposures and vulnerabilities.

(6) IS risk is best assessed by:

A. past incidents
B. analyzing statistics published by recognized bodies.
C. analyzing current threats associated with information systems.
D. evaluating last year audit reports.

Answer: C. analyzing current threats associated with information systems.
Explanation: IS risk is best assessed by evaluating threats associated with existing information systems assets and information systems projects. Other options will not provide a current level of exposure to the enterprise.

(7) Popularity of a startup company attracts the hacker and becomes the target of adversary. This is considered:

A. an emerging impact
B. an emerging vulnerability
C. an emerging threat.
D. an environmental risk factor.

Answer: C. an emerging threat.
Explanation: This situation describes the emerging threat of hackers attacking the start-up company.

(8) 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.

(9) 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.

(10) Which of the following is of greatest concern for a risk practitioner with respect to outsourcing contracts?

A. Cost benefit analysis not done for outsourcing arrangement.
B. Internal IS expertise has been lost.
C. Processing of critical data was subcontracted by the vendor.
D. High staff turnover of outsourced vendors.

Answer: C. Processing of critical data was subcontracted by the vendor.
Explanation: Subcontracting will increase the risk as the enterprise will not have any control on processes of subcontracted vendors. subcontracting process has to be reviewed because critical data are involved. Other options are not as critical as option C.

(11) Which of the following is the most important consideration for the risk professional in relation to the outsourcing arrangements?

A. Availability of policies and procedures to handle security exceptions.
B. Compliance with service level agreements by supplier.
C. Availability of IS audit team with supplier.
D. Inclusion of mandatory security controls in the outsourcing contract/agreement.

Answer: D. Inclusion of mandatory security controls in the outsourcing contract/agreement.
Explanation: Organization can enforce strong security controls only if the same is included in SLA. Without addressing security requirements directly in the outsourcing contract, the outsourcing company has no assurance that the provider will be compliant with specific security requirements.

(12) Which of the following clauses should be must in any outsourcing contract?

A. right to audit
B. provisions to assess the compliance of the provider
C. incident management procedure
D. encryption requirements

Answer: B. provisions to assess the compliance of the provider
Explanation: Right to audit is an important clause. However, service providers may not allow to audit them directly. Instead they provide a proof of compliance conducted by an independent auditor. If the provision to assess the compliance provider is not in the contract, then the outsourcing enterprise has no way to ensure compliance or proper handling of their data.

(13) Which of the following is a first step for a risk practitioner when an organization has recently outsourced one of its critical functions?

A. to assess the security of internal systems of the service provider.
B.to assess the functionality of internal systems of the service provider.
C. to ensure that security requirements are included in the agreement with service providers.
D. to conduct onsite audit of internal systems of the service provider.

Answer: C. to ensure that security requirements are included in the agreement with service providers.
Explanation: First step is to ensure that security requirements are included in the agreement with the service provider. Other options can be followed once the agreement is properly vetted from a risk perspective.

(14) Which of the following should be primarily considered in the development of information security policy?

A. assets
B. impacts
C. threats
D. likelihood

Answer: A. assets
Explanation: Asset is the primary factor on which information security policy is considered. Information security policy is based on management's commitment to protecting the assets of the enterprise from the various threats, risk and exposures that could occur.

(15) Which of the following factors have the most impact on the launch of an attack against an enterprise?

A. level of skill and motivation of the hacker.
B. log monitoring policy of the enterprise.
C. preparedness of information security team.
D. level of control measures implemented.

Answer: A. level of skill and motivation of the hacker.
Explanation: Level of skill and motivation of the attacker is the most important factor for launch of attack. Other factors are important to detect, prevent, deter or recover from an incident, however will not usually affect the likelihood of an attack.

(16) Which of the following is the major consideration for a risk practitioner with respect to Big data?

A. When data is aggregated for analysis, information that is not individually identifiable information might become identifiable.
B. Lack of expertise for big data analysis.
C. High cost in storing and analyzing the big data.
D. Lack of documented process for analysis.

Answer: A. When data are aggregated for analysis, information that is not individually identifiable information might become identifiable.
Explanation: When data are aggregated for big data analysis, some information (which was not personally identifiable earlier) may become PII data. Protection of Personal Identifiable information is very important considering stringent privacy laws.

(17) Which of the following is the major consideration for a risk practitioner with respect to Big data?

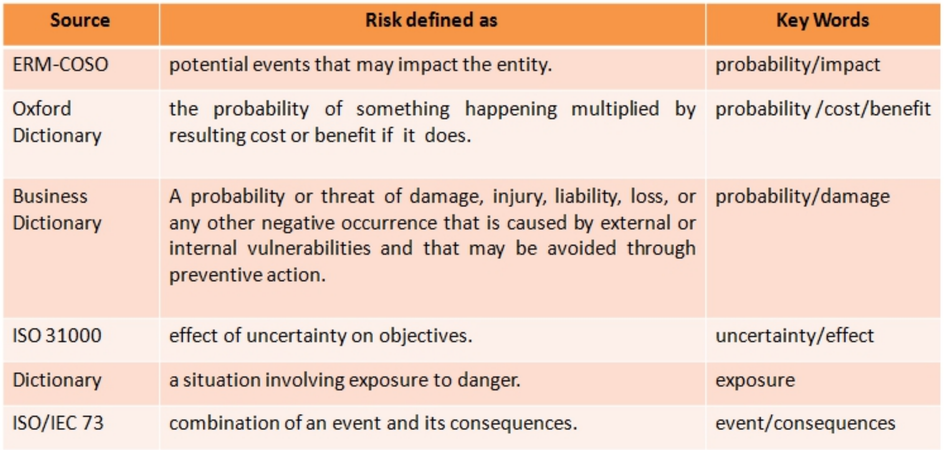
A. Analysis of data without the consent of the subject, can impact privacy laws.
B. Lack of expertise for big data analysis.
C. High cost in storing and analyzing the big data.
D. Lack of documented process for analysis.

Answer: A. Analysis of data without the consent of the subject, can impact privacy laws.
Explanation: Privacy laws require consent of the subject for use of the data. Considering stringent privacy laws, this is very important. Other options are comparatively not an area of major concern.

1.4 Information Security Risks, Concepts and Principles

What is Risk?

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

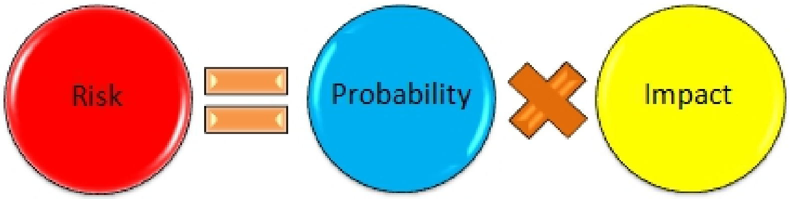


Source	Risk defined as	Key Words
ERM-COSO	potential events that may impact the entity.	probability/impact
Oxford Dictionary	the probability of something happening multiplied by resulting cost or benefit if it does.	probability /cost/benefit
Business Dictionary	A probability or threat of damage, injury, 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

Factors impacting likelihood

Likelihood or probability is used to calculate the risk that an organization faces based on the number of events that may occur within a given time period. Factors that can impact likelihood are:

Factors	Description
Volatility	Unpredictability of conditions from one moment to another.
Velocity	Speed of reaction & recovery to an event.
Proximity	Time from the event occurring and the impact on the organization.
Interdependency	Materialization of two or more types of risk might impact the organization differently, depending on whether the events occur simultaneously or consecutively
Motivation	Motivation of the perpetrator results in a higher chance of success.
Skill	Skilled perpetrator increases likelihood.
Visibility	If vulnerability is visible and known, likelihood of target increases.

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

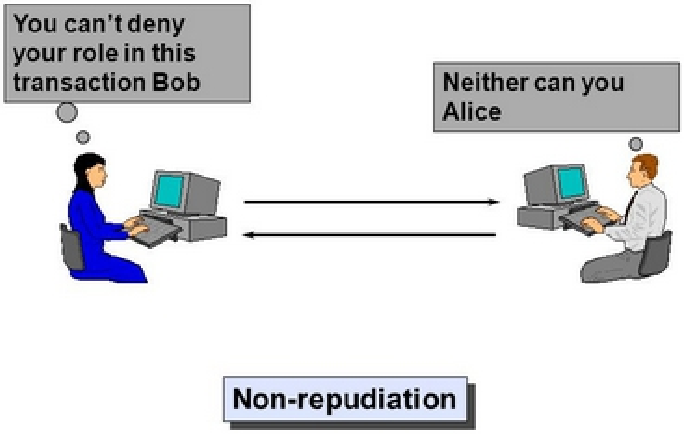
Integrity refers to correctness, completeness and accuracy of data. Principle of integrity requires guarding of data against improper modification, exclusion or destruction of information. Risk practitioners need to have technical expertise to verify integrity controls. Risk practitioners must carefully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

Self-Assessment 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 are 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.

(6) In an event of security breach at another entity utilizing similar technology, the first action by a risk practitioner would be:

A. to assess the probability of incident occurring in the risk practitioner's entity and related impact.
B. to discontinue use of that technology.
C. to enhance the control level for that technology.
D. to include incidents in the risk register.

Answer: A. to assess the probability of incident occurring in the risk practitioner's entity and related impact.
Explanation: The risk practitioner should first assess the likelihood of a similar incident occurring at his/her enterprise, based on available information. On the basis of assessment, other actions can be planned.

(7) Which of the following factors have the most impact on the launch of an attack against an enterprise?

A. level of skill and motivation of the hacker.
B. log monitoring policy of the enterprise.
C. preparedness of information security team.
D. level of control measures implemented.

Answer: A. level of skill and motivation of the hacker.
Explanation: Level of skill and motivation of the attacker is the most important factor for launch of attack. Other factors are important to detect, prevent, deter or recover from an incident, however will not usually affect the likelihood of an attack.

(8) Risk can be defined as:

A. product of probability and severity of impact.
B. likelihood of vulnerability being exposed by a threat.
C. magnitude of impact in case of a threat exploits vulnerability.
D. judgement of chief risk officer.

Answer: A. product of probability and severity of impact.
Explanation: Risk can be defined as a product of probability and severity of impact.

(9) Once the likelihood of an event has been determined, which of the below factors should be assessed next?

A. Severity of Impact
B. Control Cost
C. Residual Risk
D. Control Effectiveness

Answer: A. Severity of Impact
Explanation: Risk is defined as a product of probability and impact. Once likelihood has been determined, the next step is to determine the magnitude of impact.

(10) Which of the following is the most important factor to evaluate and assess the risk?

A. Control Effectiveness
B. Threat identification
C. Impact of previous incidents
D. Control Cost

Answer: B. Threat identification
Explanation: Data on the likelihood of identified threats is one of the key requirements for effective risk assessment. Other factors are essential but not as important as identification of threats.

(11) Most important factor for risk evaluation is to:

A. Consider the probability and likelihood of a loss.
B. consider inherent risk.
C. ensure protection of all assets.
D. review incidents occurred in similar companies.

Answer: A. Consider the probability and likelihood of a loss.
Explanation: Risk evaluation should take into account the potential size and likelihood of a loss. Although other factors are important, the impact of the risk (potential likelihood and impact of loss) should be the primary driver. It is not necessary to protect all the assets. Risk evaluation should not assume an equal degree of protection for all assets because assets may have different risk factors.

(12) Most important factor for risk mitigation strategy is to:

A. identify threats and vulnerability.
B. rank the risk on the basis of probability and impact.
C. identify the risk owner for each risk.
D. ensure that all risks have been appropriately addressed.

Answer: B. rank the risk on the basis of probability and impact.
Explanation: Ranking each risk based on impact and likelihood is critical in determining the risk mitigation strategy. Ranking of the risk helps the organization to determine the priority. Resources should be utilized to address the top level risks.

1.5 IT Risk Strategy of the Business

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.

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

'Now we have lots of Information Technology. Let us focus on gathering some information'

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.

Enhancing the risk management process

Risk practitioner can enhance the risk management process by:

- Understanding the business & strategy
- Taking proactive steps to secure new technologies and processes
- Embedding risk management process & culture into each business
- Be aware of and mitigate the risk of change
- Watching for new threats and future issues

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.

Organizational Structures and Impact on Risk

Risk management to be effective should provide a consistent way to manage risk. Risk framework should serve as a basis for risk management for all departments and business functions. The organization should have established three lines of defense as follow:

- First line should actively manage the risk (i.e. business process owners)
- Second line should guide, direct, influence and assess risk management processes (i.e. risk management dept., compliance dept.)
- Third line should have independent oversight, review and monitoring (i.e. audit)

Key factor in managing risk is the size and the diversity of the organization. Information security governance models are highly dependent on the overall organizational structure and complexity of the business. Risk management methodology depends on the risk culture of the organization.

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 Behavior and the Impact on Risk

It is very important for a risk practitioner to determine the risk appetite of the organization. It must be noted that risk appetite may change over time and hence requires periodic re-determination. 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.

Laws, Regulations, Standards and Compliance

It is very important for a risk practitioner to know what laws apply to the organization. It is advisable for organizations having global presence to build a global program of policies and a control suite to handle the common regulations and then have a regional or nation-specific addendum to handle the exceptions and their controls.

It is recommended to have a global policy that can be locally amended to comply with local laws.

In case of outsourcing to an offshore location, the most critical consideration is that laws and regulations of the origin country may not be enforceable to foreign countries.

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

Self-Assessment 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.

(6) Risk appetite should be aligned with business objective so that:

A. critical risks are identified and eliminated.
B. high risks on business objectives are evaluated and monitored.
C. IT budgets are appropriately utilized.
D. risk strategy is properly communicated.

Answer: B. high risks on business objectives are evaluated and monitored.
Explanation: Risk appetite is the amount of risk that an enterprise is willing to take on in pursuit of value. Aligning it with business objectives allows an enterprise to evaluate and deploy valuable

resources toward high risk areas which can impact business objectives.

(7) Final sign-off on IT risk management plan is to be given by:

A. IT Auditors
B. Risk practitioner
C. Business Process Owners
D. Senior Management

Answer: D. Senior Management
Explanation: 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.

(8) Which of the following is the least critical and having highest tolerance for moving to a public cloud?

A. Financial System
B. Corporate Email System
C. Research & Development System
D. Credit Card System

Answer: B. Corporate Email System
Explanation: Of the options offered, the corporate email system has the least competitive distinction,
complexity and sensitive/highly classified information.

(9) Which of the following is accountable for the risk to a critical IT system:

A. IT Manager
B. Risk Manager
C. User Department
D. Senior Management

Answer: D. Senior Management
Explanation: The accountable party is senior management. They are ultimately liable for the acceptance and mitigation of all risk.

(10) Information security governance model depends on which of the following factors?

A. count of employees
B. Budget
C. complexity and structure of organization
D. Type of technology

Answer: C. complexity and structure of organization
Explanation: Information security governance models are highly dependent on the overall organizational structure and complexity of the business.

(11) Information security governance model depends on which of the following factors?

A. geographical location
B. legislative requirements
C. complexity of the organizational structure
D. number of employees

Answer: C. complexity of the organizational structure
Explanation: Information security governance models are highly dependent on the overall organizational structure and complexity of the business.

(12) Risk management methodology depends on which of the following factors?

A. Risk culture of the organization
B. Budget
C. Industry in which organization operates
D. geographical locations

Answer: A. Risk culture of the organization
Explanation: Without an understanding of the risk culture, it is difficult to select risk management methodology.

(13) Which of the following can be defined as 'Access Risk'?

A. Risk of service/data not accessible when needed.
B. Risk of unauthorized access resulting in loss of confidentiality.
C. Risk of inadequate IT infrastructure and systems to effectively support the needs of the business.
D. Risk of incomplete, incorrect or inaccurate data.

Answer: B. Risk of unauthorized access resulting in loss of confidentiality.

(14) Which of the following can be defined as 'Availability Risk'?

A. Risk of service/data not accessible when needed.
B. Risk of unauthorized access resulting in loss of confidentiality.
C. Risk of inadequate IT infrastructure and systems to effectively support the needs of the business.
D. Risk of incomplete, incorrect or inaccurate data.

Answer: A. Risk of service/data not accessible when needed.

(15) Which of the following can be defined as 'Integrity Risk'?

A. Risk of service/data not accessible when needed.
B. Risk of unauthorized access resulting in loss of confidentiality.
C. Risk of inadequate IT infrastructure and systems to effectively support the needs of the business.
D. Risk of incomplete, incorrect or inaccurate data.

Answer: D. Risk of incomplete, incorrect or inaccurate data.

(16) Which of the following can be defined as 'Project Ownership Risk'?

A. 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.
B. Risk of IT projects failure due to lack of accountability and commitment.
C. Risk that the right information may not get to the right recipients at the right time to allow the right action to be taken.
D. Risk of IT projects not completing within expected timelines.

Answer: B. Risk of IT projects failure due to lack of accountability and commitment.

(17) Which of the following can be defined as 'Relevance Risk'?

A. 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.
B. Risk of IT projects failure due to lack of accountability and commitment.
C. Risk that the right information may not get to the right recipients at the right time to allow the right action to be taken.
D. Risk of IT projects not completing within expected timelines.

Answer: C. Risk that the right information may not get to the right recipients at the right time to allow the right action to be taken.

(18) Which of the following can be defined as 'Schedule Risk'?

A. 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.
B. Risk of IT projects failure due to lack of accountability and commitment.
C. Risk that the right information may not get to the right recipients at the right time to allow the right action to be taken.
D. Risk of IT projects not completing within expected timelines.

Answer: D. Risk of IT projects not completing within expected timelines.

(19) Which of the following can be defined as 'Investment or Expense Risk'?

A. 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.
B. Risk of IT projects failure due to lack of accountability and commitment.
C. Risk that the right information may not get to the right recipients at the right time to allow the right action to be taken.
D. Risk of IT projects not completing within expected timelines.

Answer: A. 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.

(20) RACI (Responsible, Accountable, Consulted, Informed) are the four roles that are involved in the risk management process. Which role defines: 'A single person who oversees and manages the person(s) responsible. He is liable and answerable for the project.'

A. Responsible
B. Accountable
C. Consulted
D. Informed

Answer: B. Accountable

(21) RACI (Responsible, Accountable, Consulted, Informed) are the four roles that are involved in the risk management process. Which role defines the following: 'They provide support and assistance to the risk management effort. They may be from other departments or from external sources or from regulators.'

A. Responsible
B. Accountable
C. Consulted
D. Informed

Answer: C. Consulted

(22) RACI (Responsible, Accountable, Consulted, Informed) are the four roles that are involved in the risk management process. Which role defines the following: 'They are updated of the risk management effort but may not necessarily be involved in its execution.'

A. Responsible
B. Accountable
C. Consulted
D. Informed

Answer: D. Informed

1.6 IT Concepts and Area of Concerns for the Risk Practitioner

Following are the some important IT concepts and area of concerns for the risk practitioner

Environmental Controls

Risk practitioner should consider following aspect of environmental controls:

- Following are four types of power failure:

Type	Description
Blackout	Complete loss of the power.
Brownout	Severely reduced voltage which may place strain on electronic equipment or even cause permanent damage
Sags, Spikes and surges	● Sag is a rapid decrease in voltage level. Spikes and surges are rapid increases in voltage level. These may result in data corruption in the server or the system. ● Sags, spikes and surges may be prevented by using properly placed protectors. ● Surge and spike device helps to protect against high voltage power bursts. ● Most effective control to protect against short term reduction in electric power is power line conditioner. Power line conditioner is a device intended to improve the quality of power that is delivered to electric equipment. They compensate for the peak and valleys in the power supply. When electric supply is low, it provides its own power and maintains a constant voltage.
Electromagnetic	● EMI is caused by electrical storms or noisy

Interference (EMI)	electrical equipment. ● This interference may cause computer systems to hang or damage.

- Uninterruptible power supply (UPS) can help to support the organization from interruptions, which last from a few seconds to 30 minutes. Alternate power supply (such as power generator) medium is most effective when there is long term power unavailability.

- Following are some of the best practices for maintenance of water and smoke detectors:
  - In the computer room, water detectors should be placed under raised floors and near drain holes.
  - Smoke detectors should be installed above and below the ceiling tiles throughout the facilities and below the raised computer room floor.
  - Location of the water and smoke detector should be highlighted for easy identification and access.
  - Responsibility to be assigned to a dedicated employee for remedial action in case of alarm. Standard operating procedure should be available.
  - Location of these devices is very important and should be placed in such a way to give early warning of a fire.
  - Power supply to these devices should be sufficient.
  - These devices should be tested at regular intervals.

- Emergency evacuation plans should be posted throughout the facility.

- Electrical wiring should be placed in fire-resistant panels and conduit. This conduit should ideally lie under the fire-resistant raised computer room floor.

- Following are some of the fire suppression system:

Type	Description
Wet Sprinkler (water based)	● In WBS, water always remains in the system piping. ● WBS is more effective and reliable. ● Disadvantage of exposing the facility to water damage if pipe leaks or breaks.
Dry Pipe Sprinkler	● DPSS do not have water in the pipes until an electronic fire alarm activates the water pump to send water into the system. ● Comparatively less effective and reliable. ● Advantage of not exposing the facility to water damage even if pipe leaks or breaks.
Halon System	● Halon gas removes oxygen from air thus starving the fire. ● They are not safe for human life. ● There should be audible alarm and brief delay before discharge to permit time for evacuation.

	● Halon gas is banned as it adversely affects the ozone layer. ● Popular replacements are FM-200 & Argonite.
FM 200	● FM-200 is colorless & odorless gas. ● FM-200 is safe to be used when people are present. ● FM-200 is environment friendly. ● It is commonly used as a gaseous fire suppression agent.
Argonite	● Argonite is a mixture of 50% Argon & 50% Nitrogen. ● It is used as a gaseous fire suppression agent. ● Though environment friendly & non-toxic, people have suffocated by breathing argon by mistake.
Carbon dioxide Systems	● CO_2 Systems release pressurized CO_2 gas in the area protected to replace the oxygen required for combustion. ● CO_2 is very dangerous for human life. ● In most countries, it is illegal for such systems to be set to automatic release if any human is present in the area. ● CO_2 installations are permitted where no humans are regularly present such as unmanned data centers.

Network Components

CRISC aspirant should be aware about following network components:

Cabling

Following types of cabling are used in networking

- Twisted Pairs (shielded twisted pairs (STP) and unshielded twisted pairs (UTP))
- Fiber-optics
- Co-axial

Shielded Twisted Pair (STP)

- Two insulated wires are twisted around each other, with current flowing through them in the opposite direction.
- This reduces the opportunity for cross talk and allows for lower sensitivity for electromagnetic disturbances.
- CAT7 cable is a shielded cable. that protects each pair of wires and the cable itself, thereby reducing noise and cross talk for ultra-high speed Ethernet.

Unshielded Twisted Pair (UTP)

- For unshielded twisted pairs a disadvantage is that it is not immune to the effect of electromagnetic interface (EMI).
- Unshielded twisted pairs should be away from potential interference such as fluorescent lights.
- Parallel runs of cable over long distances should be avoided since the signals on one cable can interfere with signals on adjacent cables (i.e. cross talk).
- The least expensive option used for many local area networks (LANs) is UTP cable with a grade of category 5e (CAT5e) or category 6 (CAT6).
- However, cable should not exceed the approved length of the cable runs (100 meters for CAT5e, 55 meters for CAT6).

Fiber Optics

- Glass fibers are used to carry binary signals as flashes of light.
- Fiber-optic systems have very low transmission loss.
- Fiber-optics are not affected by electromagnetic interference (EMI).
- Fiber-optic cables have proven to be more secure than the other media.
- Fiber is a preferred choice for high volume and long distance calls.

Repeaters

- Dictionary meaning of repeater is a person or thing that repeats something.
- In telecommunications, a repeater is an electronic device that receives a signal and retransmits it. Repeaters are used to extend transmissions so that the signal can cover longer distances or be received on the other side of an obstruction.
- They compensate for signals that are distorted due to a reduction of signal strength during transmission.

Hub

- Hub connects many devices together for exchange of data.
- Hub broadcast message to all the connected devices.
- Collisions occur commonly in setups using Hubs.
- Hub cannot learn or store MAC addresses.
- Hubs are classified as Layer 1 (Physical Layer) of OSI models.

Switches

- Switch is a more advanced /intelligent version of a Hub.
- Switch send message to only required device.
- No collusion occurs in the full duplex switch.
- Switch stores MAC addresses in a lookup table.

- Switches operate at Layer 2 (Data Link Layer) of OSI model.

Router

- Routers are a more intelligent version of Switch.
- Routers operate at the network layer.
- By examining the IP address, the router can make intelligent decisions to direct the packet to its destination.
- The network segments linked by a router, however, remain logically separate and can function as independent networks.
- Routers can block broadcast information, block traffic to unknown addresses, and filter traffic based on network or host information.

Firewall

Firewall is a device to monitor and control the network traffic. It is generally placed between an organization's internal network and internet for protection of the system and infrastructure of the organization.

Following are types of firewall:

Packet Filtering Router

- Simplest & earliest kind of firewall.
- Allow or Deny action is done as per IP address and port number of source & destination of packets.
- Works at Network Layer of OSI.

Stateful Inspection

- A stateful Inspection firewall keeps track of destination of each packet that leaves the internal network.
- It ensures that the incoming message is in response to the request that went out of the organization.
- Works at Network Layer of OSI.

Circuit Level

- Works on the concept of bastion host and proxy server.
- Same Proxy for all services.
- Works at Session Layer of OSI.

Application Level

- Works on the concept of bastion host and proxy server.

- Separate Proxy for each application.
- Works at Application Layer of OSI.
- Controls applications such as FTP and http.
- Out of the above firewalls, application level firewall is the most secure type of firewall.

Risk practitioners should conduct the review of firewall parameter settings to ensure that firewall rules are deployed as per security policy.

Proxy

- A proxy is a middleman. Proxy stands between internal and external networks.
- Proxy will not allow direct communication between two networks.
- Proxy technology can work at different layers of OSI models. A proxy based firewall that works at a lower layer (session layer) is referred to as circuit-level proxy. A proxy based firewall that works at a higher layer (application layer) is called an application level proxy.

Domain Name System

- Domain name system (DNS) provides a simple cross-reference between domain name and related IP address.
- For example, if the IP address for the particular website is 192.166.1.0 and the name of the website is www.criscstudy.blogspot.com.
- User will type www.criscstudy.blogspot.com and DNS server will redirect to logical address i.e. 192.166.1.0
- DNS can be used by hackers to gather the information about the organization for planning the attack.
- Also, tools and techniques are available to send false DNS replies to misroute the traffic.
- DNS replies are also used in amplification attacks to flood traffic to a particular system.
- In pharming attack, malware changes domain name system (DNS) server settings and redirects users to malicious sites

Demilitarized Zone

- Demilitarized zone (DMZ) is the area which is accessible to the external network.
- Objective of setting up a DMZ is to prevent the external traffic to have direct access to critical systems of the organization.
- All the systems placed in DMZ should be hardened and all required functionality should be disabled.
- Such systems are also referred to as bastion hosts.
- The firewall ensures that traffic from the outside is routed into the DMZ.
- Nothing valuable is kept in a DMZ because it is subject to attack and compromise from the attack.

Virtual Private Network

- A virtual private network (VPN) is used to extend a private network through use of the internet in a secured manner. It provides a platform for remote users to get connected to the organization's private network.

- Prime objective of VPN technology is to enable remote users and branch offices to access applications and resources available in private networks of organization. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunneling protocols.

- VPN technology, if properly configured, will reduce the risk associated with sensitive data travelling in an open public network.

Types of Network Topology

Following table shows various type of network topology:

Network Topology	Descriptions
Bus	● It is the simplest form of design where every device is connected by one communication path. ● Major vulnerability of bus topology is upstream dependency i.e. dependency on single cable. ● If this cable is damaged, all the devices beyond the point of damage will be unavailable. ● It is also relatively easy to intercept traffic on a bus network.
Star	● In a star network topology, each device is connected to a centralized switch. ● Design makes it very difficult for one device to intercept the traffic meant for another device. ● However, loss of central switch can affect all users.
Tree	● A tree network is a connection of multiple star networks. ● Tree networks are popular because of its scalability.
Ring	● A ring connects every device and allows traffic to pass in one or both directions. ● A ring network is used where reliable high-speed communications and fault tolerance is required.
Mesh	● In mesh topology, many devices are connected to many other devices in a mesh so they can directly communicate with one another. ● They are comparatively costly to implement.

Key aspects from CRISC exam perspective

CRISC Question	Possible Answer
What kind of devices can be placed within a demilitarized zone (DMZ)?	Devices that interacts outside the organization such Mail relay / Email Server
What is the objective of conducting peer review of firewall configuration?	To detect errors
Process to ensure that firewall deployments are in accordance with security policy	Review of firewall parameter settings
What is a pharming attack?	In pharming attack, malware changes domain name system (DNS) server settings and redirects users to malicious sites
What is the most prevalent risk of virtual private networks?	Entry of malicious code into the network
What is the most secured and cost effective method for remote access?	Virtual Private Network
Which is the most robust and secured kind of firewall?	Application Level Firewall

Self-Assessment Questions

(1) A risk practitioner noticed that the emergency door is kept open throughout the day, so that employees can leave the building faster. However, this gives rise to the risk of unauthorised entry from emergency doors. Best way to address this issue is to:

A. keep the door locked and key should be available only with facility manager
B. place a security guard near emergency door
C. install biometric access control for both entering and exiting the door
D. call local police to guard the door in case of fire

Answer: B. place a security guard near emergency door
Explanation: Best option to address the issue is to place a security guard near the emergency door. Locking the emergency door is a risky proposition if the key is not available during an emergency. Biometric access control is a risky proportion as it may give false negatives risking the lives of the employees. Calling the local police is not the best alternative.

(2) Device that can be installed in a demilitarized zone is:

A. email server
B. firewall
C. authentication server
D. corporate database server

Answer: A. email server

Explanation: Email server or mail relay can be installed in a demilitarized zone to protect the internal network. External emails may contain malicious contents to compromise the internal network of the organization. Authentication server and corporate database server should not be placed in a demilitarized zone (DMZ). Firewalls may provide another segment for DMZ, but do not technically reside within the DMZ network segment.

(3) Main reason for conducting a peer review of implementation of firewall configuration is:

A. to review performance of firewall administrator
B. to detect the configuration errors
C. to provide on job training to firewall administrator
D. to waive change management and approval process

Answer: B. to detect the configuration errors
Explanation: Objective of a peer review of firewall configuration is to detect the configuration errors. It does not intend to review the performance or provide training of firewall administrators. Also, peer review does not intend to waive change management and approval process.

(4) Best process to ensure that firewall deployments are not deviating from security policy is:

A. to interact with firewall administrator
B. to interact with author of security policy
C. to conduct review of firewall parameter settings
D to conduct review of firewall logs

Answer: C. to conduct review of firewall parameter settings
Explanation: Review of firewall parameter setting will help to determine whether deployments are in accordance with security policy. Other options do not directly help to determine the compliance with security policy.

(5) Which of the following is the greatest risk with respect to confidentiality of credit card data?

A. last four digits of credit card number are not masked
B. use of TLS protocol to transmit credit card data
C. credit card data is stored in a demilitarized zone (DMZ)
D. first six digits of credit card number are not masked

Answer: C. credit card data is stored in a demilitarized zone (DMZ)
Explanation: Credit cards stored in a DMZ are a major risk as DMZ directly interacts with external networks and can be subject to compromise. Masking of first six digits or last four digits is not mandated by PCIDSS. Only in between 6 digits should be mandatorily masked. TLS protocol is secured for data transmission.

(6) In which of the following attacks, malware changes domain name system (DNS) server settings and redirects the users to sites under the hackers' control?

A. social engineering attack
B. juice jacking
C. pharming attack
D. vishing attack

Answer: C. pharming attack

Explanation: In pharming attack, attackers compromised the DNS server setting which then redirects the user to some malicious site.

(7) With reference to virtual private networks, which of the following set up is the area of most concern?

A. computer located at organization’s remote office is getting connected through VPN
B. computer located at employee’s home is getting connected through VPN
C. computer located at organization’s backup site is getting connected through VPN
D computer located at organization’s internal network is getting connected through VPN

Answer: B. computer located at employee’s home is getting connected through VPN
Explanation: Home computers are considered as having least security as compared to other computers. If a home computer is compromised, an attacker can attempt to enter the organization’s internal network through VPN.
(8) Which of the following ensures security in a virtual private network?

A. data diddling
B. data encapsulation
C. data hashing
D. data compression

Answer: B. data encapsulation
Explanation: VPN uses data encapsulation or tunnelling method to encrypt the traffic payload for secured transmission of the data. VPN uses IPSec tunnel mode or IPSec transport mode. IPSec tunnel mode is used to encrypt the entire packet including the header. The IPSec transport mode is used to encrypt only the data portion of the packet. Mere data hashing and compression will not ensure data confidentiality. Data diddling is an attack method.

(9) Function of a virtual private network is to:
A. to implement security policies
B. to compress data travelling in the network
C. to hide data travelling in the network
D. to verify the content of the data packet

Answer: C. to hide data travelling in the network
Explanation: Objective of VPN is to hide the data from the sniffer. VPN uses data encapsulation or tunnelling method to encrypt the traffic payload for secured transmission of the data.

(10) Which of the following is the most prevalent risk of using a virtual private network for remote login?

A. entry of malicious code in the network
B. unauthorized access of data while in network
C. logon spoofing
D. adverse impact on network availability

Answer: A. entry of malicious code in the network
Explanation: One of prevalent risks of VPN is that firewalls cannot adequately examine the encrypted VPN traffic. If a remote computer is compromised, an intruder may send malicious code through VPN to enter inside the organization’s private network. Unauthorized access can be controlled through encryption. Logon spoofing can be addressed by two factor authentication. VPN does not directly impact the availability of the network.

(11) For a small organization, most economical and secured method for connecting a private network over internet is:

A. dedicated leased line
B. virtual private network
C. broadband connection
D. VoIP

Answer: B. virtual private network
Explanation: A virtual private network (VPN) is the most effective and secure way of connecting private networks over the internet. Prime objective of VPN technology is to enable remote users and branch offices to access applications and resources available in private networks of organization. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunneling protocols. VPN technology, if properly configured, will reduce the risk associated with sensitive data travelling in an open public network. Dedicated leased lines are quite expensive to maintain. Other options are not secured enough as compared to VPN.

(12) Most comprehensive method to protect a remote access network with multiple and diversified systems is:

A. firewall
B. virtual private network
C. intrusion detection system
D. demilitarized zone

Answer: B. virtual private network
Explanation: A virtual private network (VPN) is used to extend a private network through use of the internet in a secured manner. It provides a platform for remote users to get connected to the organization's private network. Prime objective of VPN technology is to enable remote users and branch offices to access applications and resources available in private networks of organization. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated circuits or with tunneling protocols. Firewall, IDS and DMZ are used to filter and control traffic between internal and external networks.

1.7 Method of Risk Identification

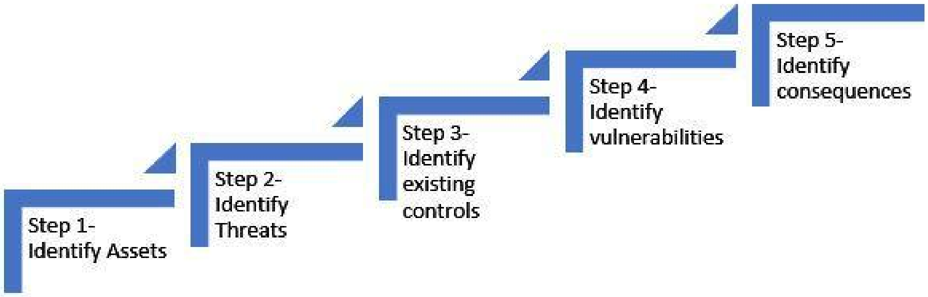
Primary objective of the risk identification process is to recognize the threats, vulnerabilities, assets and controls of the organization. Risk practitioner can use following source for identification of the risk:

- Review of past audit reports
- Review of incident reports
- Review of public media articles and press releases
- Through systematic approaches such as vulnerability assessment, penetration testing, review of BCP and DRP documents, interview with senior management and process owners, scenario analysis etc.

All the identified risks should be captured in the risk register along with details like description, category, probability, impact, risk owner and other details. Infact, maintenance of the risk register process starts with the risk identification process.

Risk Identification Process

Following are the steps of risk identification process:


Step 1- Identify Assets
Step 2- Identify Threats
Step 3- Identify existing controls
Step 4- Identify vulnerabilities
Step 5- Identify consequences

Conducting Interviews

Following are some of the good practice for use of interview technique to identify the risk:

- Risk practitioners should ensure that staff whose interview is being taken have sufficient authority and knowledge about the process.
- To the extent possible, risk practitioners should study the business process in advance of the interview. This will help in smooth conduct of interviews and risk practitioners can concentrate on areas of concern.
- Interview questions should be prepared in advance and shared with interviewee so they come prepared and bring any supporting documentation, reports or data that may be necessary.
- Risk practitioners should obtain and review relevant documentation like SOPs, reports and other notes which supports the statement of the interviewee.
- Risk practitioners should encourage interviewees to be open about various risk scenarios.

Delphi Technique

Many organizations resort to Delphi technique in which polling or information gathering is done either anonymously or privately between the interviewer and interviewee.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
In which technique employees are allowed to identify risk anonymously?	Delphi Technique
Preparation of a risk register starts with	Risk identification stage
What is the primary objective of risk identification?	To detect threats and vulnerabilities
What are the advantages of Risk Register?	All identified risks are documented in one place. It helps to drive the risk response
What is the first step in risk identification?	Information gathering

Self-Assessment Questions

(1) An organization wants to allow employees to identify risks anonymously. Most suitable technique for this is:

A. group workshop on risk scenarios
B. SWOT analysis
C. delphi technique
D. cause effect analysis

Answer: C. delphi technique
Explanation: Delphi technique helps to capture information on an anonymous basis. Many organizations resort to Delphi technique in which polling or information gathering is done either anonymously or privately between the interviewer and interviewee.

(2) Maintenance of the risk register starts from which of the following risk management phases?

A. risk identification
B. risk response
C. risk monitoring
D. risk reporting

Answer: A. risk identification
Explanation: Maintenance of risk register process starts with risk identification process. All the identified risks should be captured in the risk register along with details like description, category, probability, impact, risk owner and other details.

(3) Which of the following is the first step in risk identification and assessment procedure?

A. prepare risk ranking
B. gather information on current and future business environment
C. evaluate risk response

D. determine threats and vulnerabilities

Answer: B. gather information on current and future business environment
Explanation: Initial step would be to capture information on the current and future state of the business environment. On the basis of that next steps can be considered.

(4) Primary purpose of a risk identification is:

A. zero risk tolerance environment
B. regulatory requirements
C. to detect threats and vulnerabilities impacting the business
D. is to provide risk report to stakeholders

Answer: C. to detect threats and vulnerabilities impacting the business
Explanation: Primary objective of risk identification process is to recognize the threats, vulnerabilities, assets and controls of the organization. It is practically not feasible to have a zero risk environment. Regulatory reporting and risk reporting may be secondary objectives but primarily threats and vulnerabilities are detected so it can be mitigated.

(5) Primary purpose for maintenance of risk register is to:

A. identify and document all the risks
B. create zero risk environment
C. comply with regulatory requirements
D. identify critical processes of the organization

Answer: A. identify and document all the risks
Explanation: Risk register is maintained to document all the identified risks. It is practically not feasible to have a zero risk environment. Risk register does not identify the critical processes of the organization.

1.8 IT Risk Scenarios

A risk scenario is a visualization of a possible event that can have some adverse impact on the business objective. Organizations use the risk scenario to imagine what could go wrong and create hurdles in achievement of business objectives.

Risk scenario should be based on an identified risk. Risk scenario is developed on the basis of potential threats to the business assets. A risk practitioner can identify potential threats from the risk register. Risk scenarios may be based on risk scenarios such as system failure, natural calamities, network unavailability or any other event that can impact the business operations.

Risk scenarios are considered as the most effective technique to assess the business risk. Risk scenario helps to estimate the frequency and impact of the risk.

Risk Scenario Development Tools and Techniques

Risk scenarios should be based on real and relevant risk events. Though past incidents can serve as the basis of creating a risk scenario, risk practitioners should also look for new and emerging risks.

Imagination of risk scenarios requires creativity, thought, consultation and questioning. Risk scenarios can be either developed from a top-down perspective or a bottom up perspective.

Top-down Approach

In a top-down approach, risk events are identified from a senior management perspective. In top-down approach, risk scenario development is performed by identifying business objectives. Risk scenarios are developed for risk events that can directly impact the business goals and objectives. Involvement of senior management in designing the risk scenario is of utmost important. As top down approach deals with senior management goals, a risk practitioner can easily buy in for a risk management program.

Top-down approach looks at both IT & non IT risk events and hence can be referred to as general risk management.

Bottom-up Approach

In a bottom-up approach, risk events are identified from the process owner/employee's perspective. Risk scenarios are identified by employees performing the job functions in specific processes.

Best Approach

An organization should make use of both the top-down approach and bottom up approach for developing risk scenarios. They are complementary to each other and should be used simultaneously. In a top-down approach, major risks to business objectives are addressed where as in bottom up approach process level risks are addressed.

Benefits of Using Risk Scenarios

Following are some of the benefits of using a risk scenarios for threat identification:

- Risk scenario is the easiest and most effective way to explain risk to business process owners and other stakeholders.
- As the risk scenario requires involvement of all the process owners, information gathering becomes more relevant and realistic.
- Risk scenario helps to identify the risks that are aligned with business objectives.

Developing IT Risk Scenarios

A risk scenario includes following components:

Component	Descriptions
Agent	Agent is the element that generates the threat. Agents can be internal or external to the organization.
Threat Type	Type of threat i.e. natural, system failure, external attack, accidental etc.
Event	Nature of the incident i.e. data leakage, system down, theft etc.

Asset	Asset that is being impacted i.e. IT infrastructure, organization's reputation, data compromised etc.
Time	Impact on the basis of time element i.e. immediate impact of network failure, long term impact of system unavailability etc.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
In top-down approach, most important factor is to identify the	Business Objective
Which is the best approach for development of a risk scenario? (i.e. top down or bottom up)	Combination of both as they are complementary to each other
Which is the most effective technique in assessing business risk?	Risk scenarios
What is the most important information in a risk register that helps in developing a risk scenario?	Potential threats
Assessment in which risk scenarios are used to estimate the likelihood and impact of the risk is known as	Threat and vulnerability assessment

Self-Assessment Questions

(1) Most important factor in a top-down approach for developing a risk scenario is to identify:

A. business objective
B. IT infrastructure
C. critical processes
D. external risk

Answer: A. business objective
Explanation: In top-down approach, risk scenario development is performed by identifying business objectives. Risk scenarios are developed for risk events that can directly impact the business goals and objectives. Other options are more relevant from the bottom up approach.

(2) Best approach for developing a risk scenario is:

A. combining top down and bottom up approach for better synergy
B. top down approach for risk prone organization
C. bottom up approach for process oriented organization
D. top down approach for ease in management buy in

Answer: A. combining top down and bottom up approach for better synergy

Explanation: An organization should make use of both the top-down approach and bottom up approach for developing risk scenarios. They are complementary to each other and should be used simultaneously.

In a top-down approach, major risks to business objectives are addressed where as in bottom up approach process level risks are addressed.

(3) Most effective technique for a risk assessment is:

A. risk based audit
B. risk scenario
C. incident analysis
D. risk response action plan

Answer: B. risk scenario

Explanation: Risk scenarios are considered as the most effective technique to assess the business risk.

Risk scenario helps to estimate the frequency and impact of the risk. Incident analysis will not address new and emerging risks. Risk based audit and risk response action plan is arrived at post risk assessment.

(4) Primary reason for a risk scenario enabling the risk assessment process is:

A. risk scenario addresses all the potential risk
B. risk scenario minimize the risk response efforts
C. risk scenario helps to estimate the frequency and impact of risk
D. risk scenario addresses the higher level risks

Answer: C. risk scenario helps to estimate the frequency and impact of risk

Explanation: Risk scenario helps to estimate the frequency and impact of the risk. Risk scenario does not necessarily mean that all the risks are identified. Risk scenario does not minimize the risk response efforts. Risk scenario addresses all the levels of risks.

(5) Most important information in a risk register that helps the development of a risk scenario is:

A. risk owner
B. risk response plan
C. reported incidents
D. potential threats

Answer: D. potential threats

Explanation: Risk scenario should be based on an identified risk. Risk scenario is developed on the basis of potential threats to the business assets. A risk practitioner can identify potential threats from the risk register.

(6) Primary factor on which a risk scenario should be based is:

A. threats faced by the organization
B. advice from top officials
C. reported incidents
D. budget for risk response

Answer: A. threats faced by the organization
Explanation: Risk scenario should be based on an identified risk. Risk scenario is developed on the basis of potential threats to the business assets. A risk practitioner can identify potential threats from the risk register. Analysis of reported incidents will not address new and emerging risks. Advice from top officials and budget for risk response may not be relevant while conducting a risk scenario.

(7) Method that uses risk scenario to estimate the likelihood and impact of a risk is:

A. Internal audit procedure
B. incident analysis procedure
C. penetration testing
D. threat and vulnerability assessment

Answer: D. threat and vulnerability assessment
Explanation: Threat and vulnerability assessment uses risk scenarios to estimate the likelihood and impact of a risk. Other options do not use risk scenarios.

(8) Best method to provide comprehensive result by conducting qualitative risk analysis is:

A. scenario with threats and impact
B. asset valuation
C. risk valuation
D. loss estimate ratio

Answer: A. scenario with threats and impact
Explanation: Scenario with threats and impact provide comprehensive results by conducting qualitative risk analysis. Other options are not as significant as scenarios with threats and impact.

(9) Best method to estimate the likelihood of a risk event is:

A. cost benefit analysis
B. risk response analysis
C. root cause analysis
D. scenario analysis

Answer: D. scenario analysis
Explanation: In scenario analysis, likelihood of a risk event is estimated. Other options are not used for estimating the likelihood of a risk event.

1.9 Ownership & Accountability

Following are some of the important aspects with respect to risk ownership and accountability:

- For successful risk management, each risk should have assigned ownership and accountability.
- Risk should be owned by a senior official who has necessary authority and experience to select the appropriate risk response based on analyses and guidance provided by the risk practitioner.
- Risk owners should also own associated controls and ensure the effectiveness and adequacy of the controls.
- Risk should be assigned to an individual employee rather than as a group or a department. Allocating accountability to the department as a whole will circumvent ownership.
- Accountability for risk management lies with senior management and the board.
- Risk ownership is best established by mapping risk to specific business process owners.
- Details of the risk owner should be documented in the risk register.
- Results of the risk monitoring should be discussed and communicated with the risk owner as they own the risk and are accountable for maintaining the risk within acceptable levels.

Key aspects from CRISC exam perspective

CRISC Question	Possible Answer
What is the best way to assign the risk ownership?	Mapping risk to specific business process owner
Where should the risk ownership be documented?	Risk Register
Accountability for risk ultimately belongs to whom?	● Board of Director ● Senior Management
What is the purpose of the audit trail?	To establish accountability
Result of risk monitoring should be mandatorily communicated to	Risk owner

Self-Assessment Questions

(1)For effective risk management, it is important to:

A. assign risk owner for each risk
B. comply with regulatory requirements
C. integration of IT & non IT risks
D. avoid the risk

Answer: A. assign risk owner for each risk

Explanation: Without assigning the owners for each risk, it is difficult to monitor and control the risk. It is the most important aspect of the risk management process. Risk management does not address only compliance risk. Other options are not as significant as assigning the ownership.

(2)Risk ownership should be established by:

A. linking overlapping departments
B. analysing the risk response budget
C. IT department
D. mapping identified risk to specific process owner

Answer: D. mapping identified risk to specific process owner
Explanation: Best way to establish the ownership of a risk is to map that risk to the relevant process owner.

(3)Which of the following describes the roles and responsibilities of the business process owner and board?

A. business process owners owns the risk for their respective process whereas board members are responsible for risk identification and assessment and reporting to appropriate functions
B. business process owners owns the risk for their respective process and are responsible for risk identification and assessment and reporting to board of directors
C. business process owner carries out routine risk related functions whereas board members is responsible for designing the risk response action
D. business process owners owns the risk of their respective process and board members are responsible for updation of risk register

Answer: B. business process owners owns the risk for their respective process and are responsible for risk identification and assessment and reporting to board of directors
Explanation: Responsibility of board members is to oversee the risk management function. They are not supposed to involve in a routine risk management function.

(4)Risk ownership and risk mitigation details should be best documented in:

A. business continuity plan
B. BIA document
C. risk register
D. business case

Answer: C. risk register
Explanation: Risk register is the inventory of all the existing risks of the organization. For each risk, details like likelihood, potential impact, priority, status of mitigation and owner should be documented. Other options do not contain details of risk mitigation and ownership.

(5)Results of control monitoring should be best communicated to:

A. risk owner
B. audit department
C. IT department
D. security manager

Answer: A. risk owner

Explanation: Results of the risk monitoring should be discussed and communicated with the risk owner as they own the risk and are accountable for maintaining the risk within acceptable levels. Though as a best practice, results should be communicated to other support functions but primarily it should be made available to the risk owner.

(6)Who is ultimately accountable for the risk?

A. board of director
B. head of risk
C. head of audit
D. head of compliance

Answer: A. board of director
Explanation: Board of directors are ultimately responsible to oversee the functioning of risk management in the organization. Senior officials design the risk management strategy, however ultimate responsibility resides with board of directors.

(7)Primary objective of creating audit trail is:

A. to comply audit requirements
B. to monitor staff performance
C. to establish accountability
D. to comply regulatory requirements

Answer: C. to establish accountability
Explanation: Audit trails capture the details of the transactions such as time, data and employee has executed the particular transaction. It helps to establish accountability for the transaction. Other options may be secondary objectives of the audit trail.

Chapter 2 IT Risk Assessment

Once the risk is identified and documented in the risk register, the next step is to assess the level of the risk. IT risk assessment in the process of determining the probability and impact of identified risks. This chapter covers following topics:

2.1 Risk Assessment Technique

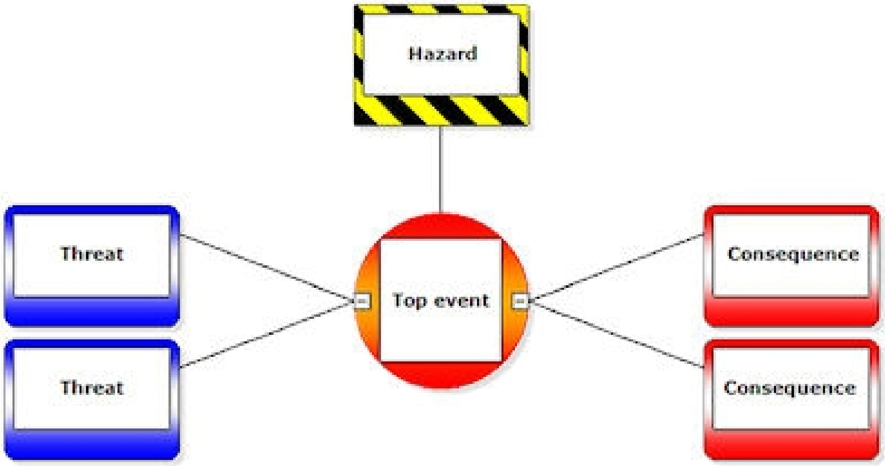
A consistent risk assessment technique should be used whenever the goal is to produce results that can be compared over time. Each approach has certain advantages and possible weaknesses, and the risk practitioner should choose a technique appropriate for the circumstances of the assessment.

Following are some of the risk assessment technique"

Bayesian Analysis

- It is a method of statistical inference that uses prior distribution data to determine the probability of a result.
- This technique relies on the prior distribution data to be accurate in order to be effective and to produce accurate results.

Bow Tie Analysis



- Bow tie analysis is a simple process for identifying areas of concern.
- It makes the analysis more effective by linking possible causes, controls and consequences.
- The cause of the event is depicted in the middle of the diagram (the "knot" of the bow tie) and on left side threats are placed whereas on right side consequences are placed.

Brainstorming/Structured Interview

Brainstorming is the process of gathering the information through structured meetings and interviews. Interview or brainstorming may be completed using prompts or interviews with an individual or small group.

Business Impact Analysis

Business impact analysis (BIA) is a process to determine the critical process of the organization and decide the recovery strategy during a disaster.

Cause and Consequence Analysis

A cause and consequence analysis combines techniques of a fault tree analysis and an event tree analysis and allows for time delays to be considered.

Cause-and-effect Analysis

- Cause and effect analysis is used to determine the factors responsible for the occurrence of the event.
- A cause-and-effect analysis looks at the factors that contributed to a certain effect and groups the causes into categories (using brainstorming), which are then displayed using a diagram, typically a tree structure or a fishbone diagram.

Checklists

- A checklist is a predefined list of potential threats or other concerns that need to be addressed.

- The risk practitioner may use previously developed lists, codes or standards to assess the risk using this method.

Delphi Method

- In the Delphi method, opinion from experts is obtained using two or more rounds of questionnaires.
- After each round of questioning, the results are summarized and communicated to the experts by a facilitator.
- This collaborative technique is often used to build a consensus among experts.
- In Delphi technique, polling or information gathering is done either anonymously or privately between the interviewer and interviewee.

Event Tree Analysis

- In event tree analysis, an event is analyzed to examine possible outcomes.
- An event tree analysis is a forward-looking model to assess the probability of different events resulting in possible outcomes.

Fault Tree Analysis

- In a fault tree analysis, an event is identified and then possible means for the event is determined.
- Results are displayed in a logical tree diagram and attempts are made to reduce or eliminate potential causes of the event.

Hazard Analysis and Critical Control Points (HACCP)

HACCP was originally developed for the food safety industry. HACCP is a system for proactively preventing risk and assuring quality, reliability and safety of processes.

Human Reliability Analysis (HRA)

In human reliability analysis (HRA), attempt is made to understand the effect of human error on systems and their performance.

Markov Analysis

- Markov analysis is a method used to forecast the value of a variable whose predicted value is influenced only by its current state.
- The Markov model assumes that future events are independent of past events.
- Markov analysis is often used for predicting behaviors and decisions within large groups of people

- A Markov analysis is used to analyze systems that can exist in multiple states.

Monte-Carlo Analysis

- Monte Carlo Analysis is a risk management technique that is used for conducting a quantitative analysis of risks.
- This technique is used to analyze the impact of risks on your project.
- Monte Carlo methods, or Monte Carlo experiments, are a broad class of computational algorithms that rely on repeated random sampling to obtain numerical results.

Preliminary Hazard Analysis

It is a process of identifying the threats or hazards that may harm an organization's activities, facilities or systems. The result is a list of potential risks.

Reliability-centered Maintenance

Objective of reliability-centered maintenance is to analyze the functions and chances of failure for a specific asset, mostly physical assets such as equipment.

Root Cause Analysis

Objective of a root cause analysis is to identify and establish the origins of events. This helps to prevent the recurrence of the problem.

Scenario Analysis

- Scenario analysis examines possible future scenarios that were identified during risk identification, looking for risk associated with the scenario should it occur.
- Scenario analysis along with vulnerability analysis helps to determine whether a particular risk is relevant to the organization and determine the likelihood of significant events impacting the organization.

Sneak Circuit Analysis

Objective of a sneak circuit analysis is used to identify design errors or sneak conditions which are often undetected by system tests.

Structured "What If" Technique (SWIFT)

The Structured What-If Checklist Technique (SWIFT) combines the use of checklists with a brainstorming 'What if?' approach to identify risk, typically within a facilitated workshop.

Key aspects from CRISC exam perspective

CRISC Question	Possible Answer
Which technique is used to determine the factors responsible for a loss event?	Cause and Effect Analysis
Which technique allows the employees to identify risk anonymously?	Delphi Method
Process to track the metrics related to error and incident is followed in	Problem management
Which method is used to estimate the likelihood of occurrence of an event?	Scenario Analysis
Statistical inference that uses prior distribution data	Bayesian Analysis
Which technique that depicts the cause of the event in the middle of the diagram (the “knot”)?	Bow Tie Analysis
Model that assumes that future events are independent of past events.	Markov Analysis
Technique to understand the effect of human error on systems and their performance.	Human reliability analysis (HRA)
Technique to identify design errors or sneak conditions such as latent hardware, software or integrated conditions that are often undetected by system tests	Sneak circuit analysis

Self -Assessment Questions

(1) Which of the following risk assessment techniques should be used to determine the factors responsible for loss events?

A. business impact analysis
B. checklist
C. cause and effect analysis
D. key risk indicators

Answer: C. cause and effect analysis
Explanation: Cause and effect analysis is used to determine the factors responsible for the occurrence of the event. Cause and effect analysis is used to determine the factors responsible for the occurrence of the event. A cause-and-effect analysis looks at the factors that contributed to a certain effect and groups the causes into categories (using brainstorming), which are then displayed using a diagram, typically a tree structure or a fishbone diagram.

(2) Which of the following risk assessment techniques should be used to conduct interviews and use of anonymous questionnaires by subject matter experts?

A. qualitative risk analysis

B. quantitative risk analysis
C. financial risk modelling
D. monte carlo analysis

Answer: A. qualitative risk analysis
Explanation: Qualitative risk analysis method involves conducting interviews of various stakeholders. There are some techniques like Delphi method wherein information can be gathered by way of anonymous questionnaires. Monte Carlo simulation combines both qualitative and quantitative assessment methods. Quantitative and financial modelling uses statistical based analysis.

(3) Which of the following risk assessment techniques allows the employees to identify the risk anonymously?

A. root cause analysis
B. delphi technique
C. swot analysis
D. event tree analysis

Answer: B. delphi technique
Explanation: In Delphi method, opinion from experts is obtained using two or more rounds of questionnaires. After each round of questioning, the results are summarized and communicated to the experts by a facilitator. This collaborative technique is often used to build a consensus among experts. In Delphi technique, polling or information gathering is done either anonymously or privately between the interviewer and interviewee.

(4) A risk practitioner observed that the IT department is not tracking any metrics for incident management. Risk practitioner should recommend:

A. implementing user awareness program
B. implementing change management
C. implementing configuration management
D. implementing problem management

Answer: D. implementing problem management
Explanation: Problem management is the process of monitoring and managing metrics related to error and incident. Objective of a problem management process is to track the metrics related to error and incident to minimize the impact of problem in the organization.

(5) Best method to estimate the likelihood of occurrence of an event is:

A. through threat analysis
B. trough cost benefit analysis
C. through identification of risk scenarios
D. through countermeasure analysis

Answer: C. through identification of risk scenarios
Explanation: Best method to estimate the likelihood of occurrence of an event is scenario analysis. Scenario analysis examines possible future scenarios and likelihood of the event impacting the

organization. Other options do not provide a complete picture to estimate the likelihood of the event.

2.2 Analyzing Risk Scenarios

Risk Scenarios

A risk scenario is a process to identify various risk events and their impact on business processes. For example, a risk practitioner may determine following risk scenario:

- What can be the impact on the business process if the network is not available?
- What can be the impact on the business process in case of system downtime?
- What can be the impact on the business process if the database is hacked?

Risk scenarios are the potential risk events which are used to determine the current state of preparedness and probable impact on business processes. Analysis of various risk scenarios helps the organization to keep themselves prepared for possible events and thus minimizing the impact of the event by taking appropriate measures.

Policies & Standards

- Approved policies provide the direction regarding acceptable and unacceptable behaviors and actions to the organization.
- Guidelines and procedures provide details do’s and don’ts to support the organization’s policies.
- A standard is a mandatory requirement to be followed to comply with a given framework or certification. Standard help to ensure an efficient and effective process which results in reliable products or services. Standards are updated as and when required to embed with the current environment. In absence of documented policies, guidelines and procedures, it is difficult to achieve the intended objective of the organization.
- It is very important for a risk practitioner to determine the availability and adequacy of organization level policies.

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

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.

Effectiveness of Security Programs

Adherence to information security requirements is the best way to monitor the effectiveness of security programs. If exceptions are minimum, then it indicates that employees are aware about the security requirements. More exceptions indicate that there is lack of awareness amongst the employees and information security programs are not effective.

Control Categories

Risk practitioners should evaluate the current control environment to determine effectiveness, efficiency and adequacy of the controls implemented. For effective control management, risk practitioner should determine:

- Whether controls are adequate
- Whether controls have any scope for bypassing
- Whether controls are reviewed and tested
- Whether segregation of duties is maintained

Risk practitioner should be aware of following control categories:

Control Categories	Descriptions
Preventive	Objective is to prevent an event from occurring. Examples include locked doors, user authentication, encryption etc.

Detective	Objective is to detect an event. Examples include audit, IDS, CCTV cameras, checksum etc.
Corrective	Objective is to correct the error or omissions. Examples include data backup, forward error control etc.
Deterrent	Objective is to deter an event by providing warning Example include warning signs etc.
Directive	Objective is to mandate the behaviour aspect by specifying do’s and don’ts. Examples include acceptance usage policy.
Compensating	Objective is to address the absence of control or weak control in a particular domain. Example includes a weak physical control is compensated by a stringent logical access control

Segregation of duties

Segregation of duty requires more than one person to complete a task. Objective of segregation of duties is to prevent fraud and error. Violation of segregation of duties means the same person doing two different functions which are segregated to prevent fraud. To prevent violation of SoD, a person should be provided with role-based access. He should not have access to the role for which he is not authorized.

Implementing New Infrastructure

Most important requirement for setting up a new system is to conduct a risk assessment before implementation. Risk assessment should primarily include business justification for new systems, capability of existing infrastructure to support new systems and security assessment of new systems.

Key aspects from CRISC exam perspective

CRISC Question	Possible Answer
Which policy determines the level of information protection within the organization?	Data classification policy
Most important requirement for setting up an information security infrastructure for a new system	Risk Assessment
Primary influencer for data retention policy	● Business Requirement ● Legal and contractual requirement
What is the greatest risk of inadequate ownership?	Inappropriate access rights
Best approach for creating a policy for global organization	A global policy that is locally amended to comply with local laws
Best approach for exception management	Documented escalation process
Violation of segregation of duties can be prevented by	Role-based access

Document that provides status of all current identified risk along with corrective actions and residual risk	Risk Register
Primary influencer for risk appetite of the organization	The culture and predisposition toward risk taking
Example of Management Control	Security Policy
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
What is the most important factor for selecting an appropriate risk management methodology?	Risk culture of the organization

Self-Assessment Questions

(1) Which of the following policies governs the rule for level of information security protection for different classes of assets?

A. security training policy
B. data classification policy
C. acceptable usage policy
D. Network policy

Answer: B. data classification policy
Explanation: 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, system owners and data owners. Other options do not have direct impact on protection rules for different categories of assets.

(2) While setting up an infrastructure for a new system, most important security requirement is:

A. audit of proposed infrastructure plan
B. conducting a business impact analysis
C. risk assessment of proposed infrastructure plan
D. training of all the security personnel

Answer: C. risk assessment of proposed infrastructure plan
Explanation: Most important requirement for setting up an information security infrastructure for a new system is to conduct a risk assessment before implementation. Risk assessment should primarily include business justification for new systems, capability of existing infrastructure to support new systems and security assessment of new systems.

(3) Data retention policy should be framed in accordance with:

A. industry standards
B. business requirements
C. storage policy
D. storage budget

Answer: B. business requirements
Explanation: Data retention policy defines the retention period for each class data. Two major factors on which data retention period is defined are business requirements and legal and contractual requirements.

(4) Major risk of inadequate procedure for assigning data and system ownership?

A. difficult to conduct the audit
B. difficult to control user access
C. difficult to determine the network requirements
D. difficult to determine the maintenance budget

Answer: B. difficult to control user access
Explanation: In absence of defined ownership, it will be difficult to manage the user access and rights may be given to users who may be otherwise unauthorized. This is a major risk. Unauthorized users can access, modify or delete the data. Other options are not as significant as unauthorized user access.

(5) Which of the following is the best approach for designing a security policy for an organization having multi-geographical operations?

A. to have a stringent global policy applicable to all the regions
B. to have a global policy that can be modified at regional level to comply with local laws
C. to have separate policy for separate regions
D. to have a global policy incorporating local laws of all the regions

Answer: B. to have a global policy that can be modified at regional level to comply with local laws
Explanation: 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.

(6) Which of the following is the first approach for establishing policies and procedures by a new organization?

A. establish the IT strategy plan
B. establish data classification policy
C. establish infrastructure plan
D. establish infrastructure benchmark

Answer: A. establish the IT strategy plan
Explanation: 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. Other options may follow once the IT strategy plan is ready.

(7) Best method for exception management is:

A. availability of escalation process
B. exceptions should not be allowed
C. exception should be allowed on the basis of judgement of senior management
D. exception should be allowed on the basis of judgement of process owner

Answer: A. availability of escalation process
Explanation: 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.

(8) Main reason for having a policy exception process is:

A. to address the exceptional cases where risk is justified by benefit
B. to comply with regulatory requirements
C. to address the complex business environment
D. it is difficult to comply the requirement of policy

Answer: A. to address the exceptional cases where risk is justified by benefit
Explanation: Exceptions to policy are required in few cases where benefits exceed the costs or where taking risk is justified by the relevant benefits. Other options are not the primary factor for having the exception policy.

(9) Best metric to monitor the effectiveness information security program:

A. number of systems covered in penetration testing
B. hours of downtime due to security incidents
C. number of exceptions from information security requirements
D. number of employees covered in security program

Answer: C. number of exceptions from information security requirements
Explanation: Adherence to information security requirements is the best way to monitor the effectiveness of security programs. If exceptions are minimum, then it indicates that employees are aware about the security requirements. More exceptions indicate that there is lack of awareness amongst the employees and information security programs are not effective. Other options are not as important as exceptions to security requirements.

(10) Once the security exception is highlighted, it should be first:

A. validated
B. reported to senior management
C. highlighted to audit committee
D. updated in the risk register

Answer: A. validated
Explanation: It is always advisable to validate the exception before reporting the same. This will help to rule out any false positives.

(11) Segregation of duties violations can be best prevented by:

A. providing role-based access
B. capturing transactions logs
C. implementing two factor authentications
D. documented information security policy

Answer: A. providing role-based access
Explanation: Violation of segregation of duties means the same person doing two different functions which are segregated to prevent fraud. To prevent violation of SoD, a person should be provided with role based access. He should not have access to the role for which he is not authorized. Log capturing and information security policy cannot prevent SoD violations. Implementation of two factor authentication will not be effective in absence of role based access control.

(12) Security policy is an example of:

A. preventive control
B. technical control
C. operational control
D. management control

Answer: D. management control
Explanation: Security policy is an example of management control.

(13) A newly appointed risk practitioner wants to understand compliance related risks and control. Which will be the best document to provide the details?

A. risk register
B. risk response action
C. business Impact Analysis
D. audit report

Answer: A. risk register
Explanation: Best method to understand any kind of risk is to review the risk register. It includes details of all the risks along with relevant control activities. Other options will not give all the relevant details.

(14) Most effective method to ensure that corrective action has been taken after a risk assessment is:

A. to interact with staff member
B. to repeat the risk assessment process
C. to conduct a follow up review
D. to discuss with senior management

Answer: C. to conduct a follow up review
Explanation: Most effective method to ensure that corrective action has been taken after a risk assessment is to conduct a follow up review. Discussion with staff members and senior management will not serve the purpose. Repeating a risk assessment process is not a feasible activity.

(15) Identified vulnerability should be immediately reported to:

A. system owner
B. data owner
C. system administrator
D. incident management team

Answer: A. system owner
Explanation: Vulnerability should be reported to the system owner immediately to enable him to take corrective action. System owner is responsible and accountable for ensuring an appropriate control environment for the system.

(16) OTP based password is an example of which type of control?

A. corrective control
B. preventive control
C. deterrent control
D. detective control

Answer: B. preventive control
Explanation: Purpose of implementing a OTP based authentication is to prevent unauthorized access. It is a preventive control.

(17) 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.

2.3 Current State of Controls

It is very important for a risk practitioner to determine the current state of control before making any recommendation. Regular review of IT risk and control environments will help to determine current position. A gap analysis is done to determine the gap between desired state of control vis-à-vis current state. It helps to identify the disparity and to determine further level controls to bridge the gap or disparity.

A risk practitioner can determine current state of control by evaluating following documents and procedures:

- Risk Assessment

- Audit Reports & Third-Party Assurance
- Business Continuity and Disaster Recovery Plans
- Capability maturity models
- Control Self-Assessment
- Incident Reporting Procedure and Logs
- Vulnerability Assessment and Penetration Testing

Let us discuss each in detail:

Risk Assessment

Risk assessment is the process to identify and evaluate the risk and its potential impact.Main objective of performing a risk assessment is to:

- To determine the current state of risk
- To justify and implement a risk mitigation strategy

Risk assessment should be performed at a frequent interval to address the change in business processes and new threats.

Audits

Audit is an evidence-based verification process and helps to determine effectiveness, efficiency and adequacy of current controls. Review of audit reports, helps the risk practitioner to determine the internal control system of the organization. It is the responsibility of the system auditor to provide continuous feedback to senior management about the effectiveness of internal controls within the organization.

Business Continuity Plan

Objective of the business continuity plan is to prepare the organization for continuity of critical processes during the disaster. In absence of a well-documented business continuity plan, a disaster can adversely impact the business processes. Thus, BCP supports an organization to survive a disaster.

Disaster Recovery Plan is about IT capability to support the business continuity and recovery objectives.

Both BCP and DRP should be kept updated and tested at periodic intervals for continuous improvement.

Business Impact Analysis

- Business Impact Analysis (BIA) determines the critical business processes by analyzing the impact of disaster on each process.
- BIA is a process to determine critical processes that have considerable impact on business processes. It determines processes to be recovered on priority to ensure organization's survival.

- For determining business impact, two independent cost factors are to be considered. First one is the downtime cost. Example of downtime cost includes drop in sales, cost of idle resources, interest cost etc. Another element of cost is with respect to alternative collective measures such as activation of BCP and other recovery costs.
- Once the business impact is available for each process, it is important to prioritize the processes which need to be recovered at the earliest. This criticality analysis should be performed in co- ordination with IT & business users.
- Business process owners possess most relevant information about processes and hence they are considered as the best source for determining criticality of the process.
- Once the critical assets are determined through BIA, the next step is to develop a recovery strategy that ensures that critical assets are recovered at the earliest to minimize the impact of disaster. Recovery strategy is primarily influenced by business impact analysis.
- Prime criteria to determine severity of service disruption is the period for which system will remain down. Higher the system downtime, higher the severity of disruption.

Capability Maturity Models

- Capability maturity models are useful to determine the maturity level of the risk management process.
- Following table indicates different maturity level of an organization:

Maturity Level	Description
0 - Incomplete	Process is not implemented or does not achieve its intended purpose.
1 - Performed	Now the process is able to achieve its intended purpose.
2 - Managed	● Process is able to achieve its intended purpose ● Also, the process is appropriately planned, monitored and controlled.
3 - Established .	● Now the process is able to achieve its intended purpose ● Also, the process is appropriately planned, monitored and controlled. ● Also, there is a well defined, documented and established process to manage the process.
4 - Predictable	Process is predictable and operates within defined parameters and limits to achieve its intended purpose.
5 - Optimized	Process is continuously improved to meet current as well as projected goals.

- The capability maturity model (CMM) indicates a scale of 0 to 5 on the basis of their maturity level and CMM is the most common method applied by the organization to measure their existing state and then to determine the desired one.

- Maturity models identify the gaps between the current state of process and the desired state to help the organization to determine necessary remediation steps for improvement.
- Capability maturity model is best technique to enable a peer review of an organization's risk management process
- Capability maturity model requires an organization to have the defined and reliable processes that it follows consistently and continuously seeks to improve.
- A matured organization is much more likely to prevent incidents, detect incidents sooner and recover rapidly from incidents.
- A maturity model determines the current status as against the desired level and thus is most helpful for improvement of the risk management process.
- Level of performance is the most important factor when using a capability maturity model. Performance is achieved when the objective of the implemented process is met.

Control Tests

Through control testing, a risk practitioner can evaluate the effectiveness, efficiency and adequacy of control and advise the risk owner of any gap identified.

Incident Reports

Risk practitioners should evaluate the incident management procedure to determine the current state of controls. Incident management process includes awareness amongst staff for incident reporting, analysis and root cause analysis for the incidents, corrective as well as preventive actions, appropriate training for the response team etc.

Main objective of the incident management process is to minimize the impact on an incident by getting the affected systems and processes back into normal service at the earliest.

Qualitative analysis of threat will help to design an effective incident response plan. Knowledge of type, kind and impact of the incident will be of great help for incident response efforts.

Enterprise Architecture

Enterprise Architecture provides a current state of IT along with a futuristic strategy and vision. The risk practitioner should determine the maturity of enterprise architecture and where EA is either immature or absent, the risk practitioner must place greater emphasis on technology specific risk assessment and compatibility.

Logs

Log files should be properly protected considering it helps immensely during forensics. Maintenance of log file should have appropriate segregation of duties. Log should be only read only mode i.e. write, edit and delete should be prohibited.
It is important to ensure the regulatory requirements are complied with. The organization may be fined for non-compliance and failing to properly track regulation-related transactions.

Media Reports

Media Reports provides useful sources of information about industry level threats or incidents. The risk practitioner should ensure that the organization has capability to track the media communication impacting the organization or its employees, customers or business partners. Organization should have a well-defined and documented policy to respond to a threat mentioned in the media impacting the organization.

Self – Assessments

Control self-assessment requires the involvement of the line managers in monitoring risk and control effectiveness within their areas of responsibility. Control self-assessment provides assurance about control effectiveness and may also reduce the need for more intense audits.

Third Party Assurance

Third-party assurance in forms reviews, audits and compliance verification provides an independent source of information about the current state of control. In case of an outsourcing of a service, the first step for a risk practitioner is to validate that all the required security clauses are addressed in service level agreement .

User Feedback

Feedback from the system users helps to determine risk and control the environment of the system.

Vendor Reports

Computer emergency response teams (CERTs) and other security vendors provided inputs on current threats and vulnerabilities, new types of malware or emerging attack methods are of immense help for making control environments more stringent.

Vulnerability Assessments and Penetration Testing

- VAPT reports are reliable means of estimating the level of IT risk in the organization.
- Penetration tests should be conducted at regular intervals and also after a major infrastructure change as changes in the infrastructure is more likely to introduce new vulnerabilities.
- In black box testing kind of attack scenario, the tester is provided with limited or no knowledge of the target's information systems. Inappropriate plan and timing of the attack may cause the system to fail. It is very important that the tester is well experienced and aware about the clear scope of the test.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
In which type of assessment, risk scenario is used to estimate the likelihood and impact of risk?	Threat and vulnerability assessment
What is the objective of Business Impact Analysis?	To determine criticality of business processes to plan recovery strategy
What is the most valuable input to improve the incident response efforts?	Knowledge about threats
Measuring the existing level of risk management processes against their desired state is best done through	Capability Maturity Model
What is the objective of maturity models?	Constant improvement in risk management process
What is the most important criterion to evaluate the process when using a capability maturity model?	Performance
Capability maturity model (CMM) is based on	Standard, repeatable and measurable processes
Risk is measured as	Impact on business operations
Why is risk assessment conducted at frequent intervals?	Constant change in risk scenarios and threats
What is the objective of a gap analysis?	To determine control deficiencies (i.e. the gap between desired control objectives and actual controls available)
What is the main objective of performing a risk assessment?	To determine the current state of risk
What is the best frequency to conduct risk evaluation?	Annually or when there is a significant change
Responsibility of data classification resides with	Data Owner
Document which includes details of the risk and the corrective actions	Risk Register
What is the most important factor for log management?	To comply with regulation
What is the best time to perform penetration tests?	Annually and also after major infrastructure changes
What is the major risk of black box testing?	Inappropriate plan and timing of the attack may cause the system to fail.
What is the most important aspect of black	It is very important that the tester is well

box testing?	experienced and aware about the clear scope of the test.

Self-Assessment Questions

(1) Which of the following is most helpful to improve the organization’s risk management process?

A. maturity model
B. internal audit
C. industry benchmarking
D. key risk indicators

Answer: A. maturity model
Explanation: Capability maturity models are useful to determine maturity level of the risk management process. The capability maturity model (CMM) indicates a scale of 0 to 5 on the basis of their maturity level and CMM is the most common method applied by the organization to measure their existing state and then to determine the desired one. A maturity model determines the current status as against the desired level and thus is most helpful for improvement of the risk management process. Other options, though important, are not as significant as the maturity model.

(2) Practice that helps the risk manager to determine the existing level of risk management processes as against the desired level is:

A. internal audit
B. capability maturity model
C. penetration test
D. balance score card

Answer: B. capability maturity model
Explanation: Capability maturity models are useful to determine maturity level of the risk management process. The capability maturity model (CMM) indicates a scale of 0 to 5 on the basis of their maturity level and CMM is the most common method applied by the organization to measure their existing state and then to determine the desired one.

(3) A peer review of risk management process is best enabled by:

A. capability maturity model
B. industry benchmarking
C. internal audit
D. balance score card

Answer: A. capability maturity model
Explanation: Capability maturity models are useful to determine maturity level of the risk management process. The capability maturity model (CMM) indicates a scale of 0 to 5 on the basis of their maturity level and CMM is the most common method applied by the organization to measure their existing state and then to determine the desired one. Capability maturity model is the best technique to enable a peer review of an organization's risk management process.

(4) Most important capability dimension of maturity model for assessing risk management process:

A. performance
B. effectiveness
C. budget adherence
D. efficiency

Answer: A. performance
Explanation: Performance is the most important capability dimension for capability maturity model. Performance is achieved when the implemented process achieves its purpose.

(5) Primary benefit of a maturity model for assessing the risk management process is:

A. it helps in benchmarking with industry
B. it helps to identify the gaps
C. it helps to determine the goals and objectives
D. to helps to reduce the security budget

Answer: B. it helps to identify the gaps
Explanation: Capability maturity models are useful to determine maturity level of the risk management process. Maturity models identify the gaps between the current state of process and the desired state to help the organization to determine necessary remediation steps for improvement. Other options are not the primary objective of the capability maturity model.

(6) To assess the capability of a risk management process of the organization, a regulatory body would rely on:

A. review by internal team
B. review by external independent team
C. peer review
D. management certification

Answer: B. review by external independent team
Explanation: Reliance on assessment done by an independent third party will always be more as compared to the internal team. Review by an external independent team will rule out any scope for biased approach.

(7) Capability maturity model is primarily based on:

A. development of new controls
B. staff awareness
C. application of standard, repeatable processes that can be measured
D. experience of risk practitioner

Answer: C. application of standard, repeatable processes that can be measured
Explanation: Capability maturity models are useful to determine maturity level of the risk management process. It is based on standard and repeatable processes that can be measured over a period of time to determine the improvement or otherwise of the stated process.

(8) An organization is in the process of selecting a consultant to conduct the maturity assessment of its risk management program. Most important element for selection of consultant is:

A. methodology to be used in the assessment
B. experience of the consultant
C. reference from industry
D. fees of the consultant

Answer: A. methodology to be used in the assessment
Explanation: Methodology helps to understand the process and formulae for the assessment. This is the most important element for selection of the consultant. Other options though important are not as significant as assessment methodology.

(9) In which of the following method, risk scenarios used to estimate the likelihood and impact of a probable event?

A. IT audit
B. Gap Analysis
C. Threat and vulnerability assessment
D. Security assessment

Answer: C. Threat and vulnerability assessment
Explanation: Risk scenarios are used at the time of threat and vulnerability assessment to identify various events and their likelihood and impact. In other options, risk scenarios are not used.

(10) Main purpose of a business impact analysis is to determine:

A. project prioritization
B. critical business processes
C. recovery budget
D. external threats

Answer: B. critical business processes
Explanation: Business Impact Analysis (BIA) determines the critical business processes by analyzing the impact of disaster on each process. BIA is a process to determine critical processes that have considerable impact on business processes. It determines processes to be recovered on priority to ensure organization's survival.

(11) Which of the following is most helpful to improve incident response efforts?

A. results of penetration test
B. analysis of threats
C. expected loss analysis
D. secure coding practices

Answer: B. analysis of threats
Explanation: Main objective of the incident management process is to minimize the impact on an incident by getting the affected systems and processes back into normal service at the earliest.

Qualitative analysis of threat will help to design an effective incident response plan. Knowledge of type, kind and impact of the incident will be of great help for incident response efforts.

(12) Most important reason for use of risk assessment technique is:

A. to maximize the profit
B. to comply with regulatory requirements
C. to justify the selection of risk mitigation plan
D. for risk quantification

Answer: C. to justify the selection of risk mitigation plan
Explanation: Risk assessment is the process to identify and evaluate the risk and its potential impact. Main objective of performing a risk assessment is to:

- To determine the current state of risk
- To justify and implement a risk mitigation strategy

Risk assessment should be performed at a frequent interval to address the change in business processes and new threats.

(13) Risk assessment should be conducted at periodic interval primarily because:

A. it helps to address the omission from previous assessment
B. it helps to explore different methodologies
C. it helps to address constantly changing business threats
D. it helps to improve risk awareness

Answer: C. it helps to address constantly changing business threats
Explanation: Risk assessment should be performed at a frequent interval to address the change in business processes and new threats. Other options are not primary objectives.

(14) Penetration test is to be best performed:

A. after major infrastructure changes
B. once new CISO joins
C. when there is high turnover is system staff
D. after internal audit

Answer: A. after major infrastructure changes
Explanation: Penetration test should be conducted at regular interval and also after a major infrastructure change as changes in the infrastructure is more likely to introduce new vulnerabilities.

(15) Most important requirement before conducting a black box penetration is:

A. clear scope of test
B. documented incident response plan
C. recommendation from internal audit team
D. proper communication to incident management team

Answer: A. clear scope of test

Explanation: In black box testing kind of attack scenario, the tester is provided with limited or no knowledge of the target's information systems. Inappropriate plan and timing of the attack may cause the system to fail. It is very important that the tester is well experienced and aware about the clear scope of the test. Other options are not as significant as the clear scope of the test.

(16) Information system deficiencies can be best identified through a:

A. gap analysis
B. risk register
C. control framework
D. countermeasure analysis

Answer: A. gap analysis

Explanation: Objective of a gap analysis is to identify the gap between current level of control as against desired level of control. This gap is also known as control deficiencies. Risk practitioners first analyze the desired state of risk management requirement of the organization and then determine the current condition of risk management affairs. This helps him to identify the gaps. He should recommend the actions to close the gaps. Other options are not as effective as gap analysis for identification of deficiencies.

(17) Risk is measured by:

A. deficiency in IT system
B. impact on business operations
C. cost of control
D. control framework

Answer: B. impact on business operations
Explanation: Risk is measured as a combination of probability of occurrence and impact on business operations.

(18) A risk practitioner noted that a local management has mitigated the risk owned by corporate management. This means that:

A. risk is transferred to local management
B. corporate management remains responsible for the risk
C. risk should not be monitored
D. risk is owned by corporate management as well as local management

Answer: B. corporate management remains responsible for the risk
Explanation: Risk owner may delegate the management of risk to some other party. However, the risk owner is ultimately responsible for monitoring and controlling the risk.

(19) Responsibility for evaluating the effectiveness of existing internal information security (IS) controls resides with:

A. internal audit team
B. penetration team
C. operations team
D. legal team

Answer: A. internal audit team

Explanation: Audit is evidence-based verification process and helps to determine effectiveness, efficiency and adequacy of current controls. It is the responsibility of the system auditor to provide continuous feedback to senior management about the effectiveness of internal controls within the organization.

(20) Major risk associated with log capturing process is:

A. log related regulations are not adhered
B. back-up of logs are not maintained
C. log data are recycled every 15 days
D. log data are reviewed on monthly basis

Answer: A. log related regulations are not adhered
Explanation: Regulatory compliance is the most important aspect of any process. Not adhering to regulation may have financial as well as reputational consequences. Other options are not as significant as regulatory compliance.

(21) Which of the following is a major risk with respect to log capturing when only failed and success access attempts are logged?

A. source IP address is not captured
B. destination IP address is not captured
C. details of executed commands are not captured
D. logs are not automatically moved to secondary storage

Answer: C. details of executed commands are not captured
Explanation: Apart from login details, log should also capture details of transactions and other commands executed by the users. In absence of details of transactions and commands, forensic investigation will not be meaningful. IP address is captured as part of login access details. Moving of log to secondary storage is not as critical as capturing of transactions and commands.

(22) An organization reviewed its risk profile a year back and all the gaps are addressed. Most important method for the organization to evaluate its current risk profile is:

A. to review effectiveness of previously placed controls
B. to conduct internal audit for newly implemented controls
C. to perform a new risk assessment by an independent expert
D. to monitor the results of key risk indicator

Answer: C. to perform a new risk assessment by an independent expert
Explanation: Conducting a new risk assessment is the best approach to determine the current risk profile. Other options will help to understand the effectiveness of already implemented control but they will not help to determine new or emerging risk.

(23) Risk assessment should be conducted on a consistent basis to:

A. lower the cost of assessment
B. determine the trends in risk profile
C. waive the requirement of internal audit
D. make optimum utilization of risk management team

Answer: B. determine the trends in risk profile
Explanation: Performing the risk assessment on a consistent basis will provide trends in risk profile over a period of time. Tracking trends in evolving risk is very important for managing risk and ensuring that appropriate controls are in place.

(24) Main objective of performing a risk assessment is:

A. to waive the requirement of internal audit
B. to make optimum utilization of risk management team
C. to determine current state of risk
D. to comply with regulatory requirements

Answer: C. to determine current state of risk
Explanation: Risk assessment is the process to identify and evaluate the risk and its potential impact. Main objective of performing a risk assessment is to:

- To determine the current state of risk
- To justify and implement a risk mitigation strategy

Risk assessment should be performed at a frequent interval to address the change in business processes and new threats.

(25) Risk should be evaluated:

A. on annual basis
B. on annual basis or when there is significant change in business process
C. when there is significant change in business process
D. as and when required by risk practitioner

Answer: B. on annual basis or when there is significant change in business process
Explanation: Risk should be evaluated at frequent intervals may be annually and also when there is significant change in business process to address the new and emerging threats.

(26) Data classification is the responsibility of:

A. end user
B. risk practitioner
C. data owner
D. system administrator

Answer: C. data owner
Explanation: Data owner is accountable to ensure that his data is having appropriate security controls. It is the data owner who is ultimately responsible for defining the access rules. The owner of the data or system is finally responsible for the safe custody of the assets. System administrator, risk practitioner and end user supports the owner for safeguarding of the assets.

(27) Which of the following indicates the inappropriate risk practices?

A. IT department has its own methodology for risk assessment
B. risk ownership is assigned to senior official of user department
C. last risk assessment carried out before 11 months

D. risk identification process is led by risk management team

Answer: A. IT department has its own methodology for risk assessment
Explanation: Risk assessment method should be standard and consistent through the organization. This will help to identify and prioritize the risk and ensure mitigation controls. Assigning risk ownership to a senior official of the concerned department is a good practice. Risk assessment should be conducted at frequent intervals may be annually and also when there is significant change in business process to address the new and emerging threats. Risk management team should lead and facilitate the risk identification process.

2.4 Change in Risk Environment

As the business processes and technology changes, the risk environment also gets changed with new types of threats. No systems can be considered as secured perpetually. This indicates that risk assessment should be done at a regular interval to address the emerging risks. Main benefit of performing a risk assessment on a consistent basis is that it helps to understand the trends in the risk profile.

Technological changes are inevitable in today’s world. However, new technology should be properly assessed and tested before implementation. Risk practitioners are responsible to ensure that any new technology implemented should be subject to risk assessment.

A risk practitioner should determine the maturity of the enterprise toward monitoring and adapting to new market trends. An independent benchmark of capabilities helps an organization to determine its level of capability compared to other organizations within its industry.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
Primary advantage of performing a risk assessment on a consistent basis	Helps to understand the trends in the risk profile
Best way to determine the capability of the organization as compared to industries	An independent benchmark of capabilities

Self-Assessment Questions

(1) Hacker targets the popular start up organization. This is known as:

A. emerging threat
B. emerging vulnerability
C. environmental risk
D. incident response

Answer: A. emerging threat
Explanation: When an organization grows, it exposes itself to new and emerging threats. Threat is something which is not in the control of the organization. Vulnerability means weakness in the control system of the organization.

(2) Main advantage of conducting a risk assessment on consistent basis is:

A. adherence to regulatory requirements
B. lower cost of risk assessment
C. indication of change in risk profile
D. waiver of audit requirements

Answer: C. indication of change in risk profile
Explanation: Performing the risk assessment on a consistent basis will provide trends in risk profile over a period of time. Tracking trends in evolving risk is very important for managing risk and ensuring that appropriate controls are in place.

(3) Which of the following will provide the best assessment about alignment of organization's processes with industry prescribed practices?

A. internal audit
B. independent benchmark of capabilities
C. internal benchmark of capabilities
D. balance score card

Answer: B. independent benchmark of capabilities
Explanation: Reliance on assessment done by an independent third party will always be more as compared to the internal team. Review by an external independent team will rule out any scope for biased approach.

2.5 Project and Program Management

Following are some of the important aspects of project and program management:

- It is very important for a risk practitioner to monitor the risk related to the management of the projects.
- Some of major reason for failing of IT projects are:
    - Scope creep i.e. requirements are not properly defined at the initial phase.
    - Lack of planning resulting in over budget and unavailability of skilled resources.
    - Lack of structured project management process.
    - Systems not tested before implementation
    - Compliance or regulatory issues
- Root cause for the system failure is to be determined so the learnings can be applied to all the future projects.
- Major cause for a project failure is delay in completion. It may happen to make for the time lapsed, critical steps of projects (like testing) is skipped. This can lead to major failure of the project.
- Best way to monitor the progress of the project in terms of scope, schedule and budget is through Earned Value Analysis (EVA).

- Projects frequently go over time or budget due to various reasons. However, risk tolerance for project delays should be documented. Risk tolerance is the acceptance deviation from the expected project budget or timelines.
- Most important element for successful SDLC is involvement of senior business representatives of different functions.
- Risk practitioner should be aware of the following system development life cycle (SDLC) phases:

Phase	Description
Phase 1 – Initiation/ Feasibility	· Objective, purpose and scope of the system is discussed, finalized and documented. · In this phase system design is finalized and approved. Internal controls should be incorporated during the initial design stage. · During the feasibility phase (planning or initiation), the process for change management should be defined. It is very important to prevent a scope creep.
Phase 2 – Development / Acquisition	In this phase, alternatives are evaluated and the system is developed or acquired from a third party.
Phase 3 – Implementation	In this phase, the system is tested and migration activities are carried out.
Phase 4 – Operations / Maintenance	In this phase, regular updates and maintenance is carried out for upkeep of the system.
Phase 5 - Disposal	In this phase, obsolete systems are discarded by moving, archiving, discarding or destroying information and sanitizing the hardware and software.

- Risk practitioners should be involved in all the above phases of SDLC and security requirements should be integrated into all SDLC phases. Performing risk assessments at each stage of the system development life cycle (SDLC) is the most cost-effective way to address the flaws at the earliest.
- Security requirements should be validated and tested to ensure that it addresses the risk associated with confidentiality, integrity and availability. Project members should be made aware about the risk implications on the project.
- Following aspects to be addressed during risk assessment of the project:
  - What level of confidentiality is required for the system?
  - What level of availability is required for the system?
  - Impact of any laws or regulation on the project (for example: privacy laws)
  - Architectural and technological risk
  - Use of a secure information systems development process

- Security training for the developers and staff members

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
Availability of skilled resources should be addressed during which phase of SDLC?	Design Phase
Migration risk should be addressed during which phase of SDLC?	Implementation Phase
Internal control should be incorporated during which phase of SDLC?	Design Phase
A business case should be retained till	Application's end of life.
Which tool is used to evaluate a project in terms of project scope, schedule and cost?	Earned Value Analysis (EVA)
In which phase of SDLC risk assessment is conducted?	During each stage of the system development life cycle (SDLC)
To prevent scope creep, the process to change and approve any requirement or deliverable should be defined in which phase of SDLC?	Feasibility Stage / Design Phase

Self-Assessment Questions

(1) Acceptable deviation from a defined budget of a project is known as:

A. risk tolerance
B. risk avoidance
C. risk assessment
D. risk transfer

Answer: A. risk tolerance
Explanation: Risk tolerance levels are deviations from risk appetite. Risk tolerance is the permissible deviation from declared risk appetite levels.

(2) During the application design phase, which of the following risks should be addressed?

A. unavailability of skilled resources
B. system migration risk
C. system implementation risk
D. system testing risk

Answer: A. unavailability of skilled resources
Explanation: Resource requirement and availability should be addressed during the design phase. Migration risk and implementation risk to be addressed during the implementation stage. Testing risk to be addressed during the testing stage.

(3) In which of the following activities, the project management department makes use of risk analysis?

A. during incident response planning
B. during go/no go decision making
C. during workplace safety planning
D. during compliance bulletin issuance

Answer: B. during go/no go decision making
Explanation: Project team is required to select the best approach after doing risk analysis of various available alternatives. Their decision making is based on risk analysis. Incident response planning is done by the BCP team. Safety planning is done by the safety team and compliance issues are looked after by the compliance team.

(4) Internal control should be incorporated during which of the following SDLC phases?

A. testing stage
B. design stage
C. implementation stage
D. acceptance stage

Answer: B. design stage
Explanation: For success of a project, control requirements should be analyzed and incorporated during the design phase of the SDLC. Incorporating controls at later stages will be a risky affair.

(5) A business case developed of the project should be retained till:

A. end of the application's life
B. application is implemented
C. completion of user acceptance testing
D. project is approved by senior management

Answer: A. end of the application's life
Explanation: A business case developed for the project should be retained till the end of the application's life cycle.

(6) Which of the following tools is used to determine the progress of the project in terms of cost, schedule and scope?

A. function point analysis
B. CPM and PERT
C. Gantt Chart
D. earned value analysis

Answer: D. earned value analysis
Explanation: Earned Value Analysis (EVA) is a method of measuring a project's progress at any given point in time, forecasting its completion date and final cost, and analyzing variances in the schedule and budget as the project proceeds EVA determines and evaluates following factors on periodic basis:

- What is actual spending till date as compared to budget?

- What will be the estimated completion time?
- What will be the estimated total expenditure?

PERT, CPM and Gantt charts will help to determine the project time but lack projection for estimates as completion. Function point analysis is for estimating the size of the software.

(7) Which of the following steps is required before moving to the system design phase?

A. acceptance of risk with respect to proposed system by management
B. designing test scenarios
C. user acceptance testing
D. procuring security equipment

Answer: A. acceptance of risk with respect to proposed system by management
Explanation: Acceptance by management with respect to the proposed system is an important aspect in the project development cycle. It is the first and most important step that is required before moving to the system design phase.

(8) Risk assessment in a project development will be most effective if:

A. it is conducted before the project
B. it is conducted at every stage of system development life cycle
C. it is conducted during post implementation review
D. it is conducted during development of business case

Answer: B. it is conducted at every stage of system development life cycle
Explanation: Risk assessment is not a one-time activity. It should be conducted at every stage of the system development life cycle for the most effective result.

(9) To prevent scope creep, requirements and deliverables should be defined during which stage of SDLC?

A. feasibility stage
B. post implementation stage
C. development stage
D. user acceptance stage

Answer: A. feasibility stage
Explanation: Requirements of the system should be defined, approved and freeze during feasibility and design stage itself. Most common reason for a system failure is constant change of requirements. For successful implementation of a project, requirements should be finalized during the initial stage itself.

(10) Most important factor for implementing a risk based approach in a project management is:

A. involvement of business representative
B. availability of risk management framework
C. change management process
D. documented risk mitigation techniques

Answer: A. involvement of business representative
Explanation: Most important factor for implementing a risk based approach in a project management is involvement of a business representative. This ensures accurate assessment of risk and subsequent mitigations. Other options are not as significant as involvement of business representation.

2.6 Risk and Control Analysis

Risk Assessment

Risk assessment is conducted by evaluating the current state of risk as against the desired level. It also takes into consideration the effectiveness of existing control. Main objective of risk assessment is to identify all the areas where current level of risk exceeds the acceptable risk level and use this information as the basis of risk response.

Risk Appetite

Risk appetite is the level of risk that an organization is willing to take to achieve the business objectives. Risk appetite of the organization will help to determine the desired state of IT risk. Two important factors for determining the risk appetite is: the management culture and the predisposition toward risk taking.

When risk appetite is aligned with business objectives, organizations can allot more resources to the areas where risk tolerance is low. If residual risk is within the acceptable risk, it provides comfort for management. If residual risk is higher than acceptable risk, management can decide whether to accept the risk or apply more controls to bring down the residual risk.

Risk Analysis

Risk analysis is ranking of risk on the basis of its impact on business processes. Risk with high impact is ranked higher and given priority to address the same. More resources are allocated to high risk areas.
Risk analysis results help for prioritization of risk responses and the allocation of resources.

Data Analysis

Most important concern with data analysis is to ensure completeness and trustworthiness of the data. Below table indicates some of the methods for data analysis:

Methods	Description
Cause and Effect Analysis	• Cause-and-effect analysis is used for both prediction as well as diagnostic analysis. • It is used to identify the root cause for outcome and thus helps to determine the potential risk. • A typical form is the Ishikawa diagram or fishbone diagram is one of the examples of cause and effect analysis.

Fault tree analysis	• Fault tree is the analysis of all possible events that can make the project a failure. • Most serious event is considered a top-level event.
Sensitivity analysis	• Sensitivity analysis is a quantitative risk analysis method to evaluate the impact of each risk event. • Results are displayed in the form of a tornado diagram.

Risk practitioners should be careful to understand any emerging trend from data analytics. This can be done only when normal trends are available and documented.

Threat and Misuse Case Modelling

- In threat modelling, a risk practitioner uses the same methods and techniques used by a hacker or intruder to perpetrate an attack. These techniques include both technical as well as non-technical. An example of this is the "ping of death" attack.
- Purpose of threat modelling is to design adequate controls to address all the possible threats.
- Objective of threat modelling is to build defense in depth system controls to prevent systems from being compromised.
- In misuse case modelling, analysis is done for major errors, mistakes and events that can impact the functionality of the system. Objective of misuse case modelling is to ensure that a system is resilient enough to withstand the errors and misuse.
- Attackers can misuse the functionality of internet control message protocol (ICMP) or network time protocol (NTP) or Domain Name System (DNS) services to attack and take control of the system. For example, an attacker can change the size of an ICMP packet to disable the target system.

Root Cause Analysis

Root cause is the process of identification of the underlying reason for an event or problem. Objective of root cause is to prevent the recurring of events by addressing the root cause. It is important to conduct a root cause to determine the factors leading to the event rather than just addressing the symptoms of the problem.

Pre-mortem is a type or root cause analysis in which it is pretended that a project has failed and the group is asked to deliberate and discuss why it has failed. It then provides significant insight and perspectives on risk.

The risk practitioner can use root cause analysis as a means of identifying related events which have significant impact on business processes and which cannot be traced to a single common cause. In such cases it is important to address all the events or problems.

Gap Analysis

Objective of a gap analysis is to identify the gap between current level of control as against desired level of control. This gap is also known as control deficiencies. Risk practitioners first analyze the desired state of risk management requirement of the organization and then determine the current condition of risk management affairs. This helps him to identify the gaps. He should recommend the actions to close the gaps.

Gap analysis is used in iteration to monitor the project deliverables and milestones. Key performance goals are considered as desired level and this is compared with actual level. This helps to execute projects in a timely and logical manner.

Predicting Risk

Risk practitioners should use tools and techniques to predict the risk events. He should look for risk factors which do not have much impact if occurred individually but can lead to major outages if they occur simultaneously. Also, risks have cascading effects where a minor issue may indicate a serious event in the future.

A risk practitioner should be able to evaluate and determine the possibility of re-occurrence of past incidents. It is very important to learn from the past incidents.

Key aspects from CRISC exam perspective

CRISC Question	Possible Answer
Advantage of alignment of risk appetite with business objective	To monitor the area with low risk tolerance
Compliance with risk appetite is determined by	Residual risk and acceptable risk
Level of risk appetite is best determined by	Culture and predisposition toward risk taking
Best way to determine control deficiencies	Gap Analysis (Gap analysis is used to determine the gap between desired level of control and actual level of control)
Objective of risk analysis	To prioritize risk response
Resources for risk response should be allotted on the basis of	Risk analysis results

Self-Assessment Questions

(1) Main purpose of aligning risk appetite with business objective is:

A. to ensure that resources are directed towards area of low tolerance
B. to reduce the risk management budget
C. to eliminate all the major risks
D. to communicate risk profile to the senior management

Answer: A. to ensure that resources are directed towards area of low tolerance
Explanation: Risk appetite is the amount of risk an organization is willing to take. If risk appetite is aligned with business objectives, valuable resources can be deployed toward those objectives where

the risk is high.

(2) Risk appetite can be considered as complied after determining:

A. control risk and acceptable risk
B. inherent risk and acceptable risk
C. residual risk and acceptable risk
D. inherent risk and control risk

Answer: C. residual risk and acceptable risk
Explanation: Risk appetite means the amount of risk an organization is willing to take. Risk practitioners can determine the compliance with risk appetite by evaluating the residual risk i.e. residual risk should be within the acceptable risk. If residual risk is within the acceptable risk, it provides comfort for management. If residual risk is higher than acceptable risk, management can decide whether to accept the risk or apply more controls to bring down the residual risk.

(3) Most important factor when considering the risk appetite of the organization:

A. loss absorption capacity
B. culture and predisposition toward risk taking
C. complexity of business processes
D. size of risk management team

Answer: B. culture and predisposition toward risk taking
Explanation: Risk appetite means the amount of risk an organization is willing to take. Two important factors for determining the risk appetite is: the management culture and the predisposition toward risk taking.

(4) Risk appetite of the organization is moderate however a newly purchased application possesses a high risk. What should be next course of action:

A. high risk application should not be installed
B. to increase the risk appetite
C. to determine controls for mitigating the high risk
D. to benchmark the process followed by industry

Answer: C. to determine controls for mitigating the high risk
Explanation: First step will be to determine whether new controls to be implemented on the system may lower the risk from high to moderate or low before taking any further action. Other options may not address the issue.

(5) Risk is said to be acceptable when:

A. residual risk is within tolerance level
B. residual risk is lower than inherent risk
C. control risk is minimized
D. inherent risk is minimized

Answer: A. residual risk is within tolerance level

Explanation: Risk appetite means the amount of risk an organization is willing to take. Risk practitioner can determine the compliance with risk appetite by evaluating the residual risk i.e. residual risk should be within the acceptable risk. If residual risk is within the acceptable risk, it provides comfort for management. If residual risk is higher than acceptable risk, management can decide whether to accept the risk or apply more controls to bring down the residual risk.

(6) Most effective method to determine the factors responsible for an event is:

A. cause and effect analysis
B. business impact analysis
C. business process reengineering
D. key performance monitor

Answer: A. cause and effect analysis

Explanation: Cause and effect analysis is the process of identification of the underlying reason for an event or problem. Objective of the same is to prevent the recurring of events by addressing the root cause.
It is important to conduct a root cause to determine the factors leading to the event rather than just addressing the symptoms of the problem. Other options do not directly determine the factors responsible for the event.

(7) Control deficiencies can be identified through:

A. business impact analysis
B. gap analysis
C. control framework
D. risk register

Answer: B. gap analysis

Explanation: Objective of a gap analysis is to identify the gap between current level of control as against desired level of control. This gap is also known as control deficiencies. Risk practitioners first analyze the desired state of risk management requirement of the organization and then determine the current condition of risk management affairs. This helps him to identify the gaps. He should recommend the actions to close the gaps.

(8) IT risk analysis should be subject to which of the following before it is placed to senior management?

A. peer review
B. gap analysis
C. internal audit
D. compliance review

Answer: A. peer review
Explanation: Peer reviewer is the evaluation of work done by a person having similar competencies. It is a kind of double check to ensure the accuracy of the risk analysis. It is effective, efficient and good practice to perform a peer review of IT risk analysis results before sending them to

management. Other options are more suitable once the risk analysis results are placed and approved by the senior management.

(9) Which of the following is the most important objective of IT risk analysis?

A. to prioritize the risk response
B. to minimize the cost of security investment
C. to comply with regulatory requirements
D. to identify threats and vulnerabilities

Answer: A. to prioritize the risk response
Explanation: Risk analysis is ranking of risk on the basis of its impact on business processes. Risk with high impact is ranked higher and given priority to address the same. More resources are allocated to high risk areas. Risk analysis results help for prioritization of risk responses and the allocation of resources.

(10) Resources for risk response should be allotted on the basis of:

A. internal audit reports
B. risk analysis reports
C. security assessment reports
D. penetration test results

Answer: B. risk analysis reports
Explanation: Risk analysis is ranking of risk on the basis of its impact on business processes. Risk with high impact is ranked higher and given priority to address the same. More resources are allocated to high risk areas. Risk analysis results help for prioritization of risk responses and the allocation of resources.

2.7 Risk Analysis Methodologies

Risk analysis is the process of ranking various risks so that areas of high risk can be prioritized for treating them. Risk can be measured and ranked by use of any of the following methods:

- Quantitative Risk Assessment
- Qualitative Risk Assessment
- Semi-quantitative Risk Assessment

Factor that influences the selection for the above technique is availability of accurate data for risk assessment. When a data source is accurate and reliable, an organization will prefer quantitative risk assessment as it will give risk value in some numeric terms like monetary values. Monetary value is easy to evaluate to determine the risk response.

Quantitative Risk Assessment

In quantitative risk assessment, risk is measured on the basis of numerical values. This helps in cost benefit analysis as risk in monetary terms can be easily compared to cost of various risk responses. In quantitative risk assessment, various statistical methods are used to derive the risk.

Risk is quantified as per this formula: Risk = Probability * Impact

CRISC aspirants should always remember that risk is quantified by combination of probability and impact. Let us understand this with help of an example: Probability of damage for an equipment costing $ 1000 is 0. Here probability is zero and impact is $ 1000. Now, risk is probability * impact i.e. P * I. In this case risk is 1000*0 i.e. 0. Now for some other asset if probability is 0.5 and asset costs $ 100, then risk will be $ 50 (0.5 * 100). Risk of equipment costing $ 100 is more than risk of equipment costing $1000. This is because probability plays an important role in quantification of risk.

Challenge in implementing quantitative risk assessment

Major challenge for conducting quantitative risk assessment is availability of reliable data. To quantify a risk, accurate details of probability and impact is required. Determining the probability or frequency of the occurrence of threat is a challenging aspect. Mostly, probability can be arrived at on the basis of historical data. However, it is very difficult to ascertain the probability of natural events such as hurricanes, earthquakes, tsunamis etc.

Quantitative risk assessment is not feasible for the events where probability or impact cannot be quantified or expressed in numerical terms.

Thus, a quantitative risk assessment:

- Make use of statistical method to derive risk
- Make use of likelihood and impact
- Helps to derive a financial impact

Qualitative Risk Assessment

In a qualitative risk assessment, risks are measured on some qualitative parameters such as high, medium a low or on a scale of 1 to 5.
· Qualitative assessment is considered more subjective as compared to quantitative assessment.
· Few risks cannot be calculated in numeric terms. Qualitative assessment is useful in such scenarios.
· For comprehensive outcome of qualitative risk assessment, a risk practitioner should use different risk scenarios with threats and impacts. Scenarios can be based on threats or vulnerabilities or impact or combination of any of these. In this approach, risk practitioners examine various internal and external scenarios and try to determine the impact of each scenario on business processes. Through these scenarios, feedback is obtained from various stakeholders to determine the level of risk. This will facilitate a more informed discussion and decision.

Following table gives details of different scenario-based assessment:

Scenario	Description
Vulnerability-based approach	● In this approach, vulnerabilities are determined and then threats are identified that could exploit those vulnerabilities.

	● Next step is to determine the current level of control and evaluate whether they are capable of addressing all the threats. ● Vulnerability-based scenarios are especially valuable after completing vulnerability assessments and penetration testing.
Asset / Impact approach	● In this approach, critical assets are identified and all possible ways that can impact confidentiality, integrity and availability. ● Next step is to determine the current level of control and evaluate whether they are capable of addressing all the threats.

Qualitative risk assessment is more relevant to examine the new emerging threats and advanced persistent threats (APTs). Qualitative risk analysis method involves conducting interviews of various stakeholders. There are some techniques like Delphi method wherein information can be gathered by way of anonymous questionnaires.

Quantifying the impact of a failed equipment

Impact of a failed equipment is not only restricted to the cost of the equipment but also includes impact on business processes due to failure of equipment. Risk practitioners should use various approaches to determine the overall impact on the business due to failure of equipment.

Semi Quantitative Risk Assessment

- Semi-quantitative risk assessment is the combination of qualitative and quantitative risk assessment. It is a hybrid approach which considers input of qualitative approach combined with numerical scale to determine the impact of a quantitative risk assessment.
- In semiquantitative analysis, the descriptive rankings are associated with a numeric scale.
- For example, the qualitative measure of “high” may be given a quantitative weight of 5, “medium” may be given 3 and “low” may be given 1
- Such methods are frequently used when it is not possible to use a quantitative method or to reduce subjectivity in qualitative methods.
- Risk practitioners should ensure that a standardized process and scale is used throughout the organization for semi quantitative risk assessment. Also risk owners should not mistake the origins of these values as coming from purely objective sources.

Best method for Risk Analysis

A risk practitioner would always prefer a quantitative approach. Quantitative approach helps in cost benefit analysis as risk in monetary terms can be easily compared to cost of various risk responses. However, a major challenge in conducting a quantitative risk analysis is availability of accurate data. In absence of proper data or when data accuracy is questionable, qualitative analysis is more preferable.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
Which factors are required to quantify the risk?	Probability & Impact ● probability is also referred as possibility or likelihood ● impact is also referred as consequences
In which risk analysis method, statistical methods are used to derive risk?	Quantitative Risk Analysis
Which risk analysis process uses likelihood and impact?	Quantitative Risk Analysis
Which risk analysis method is used to derive financial impact of a risk ?	Quantitative Risk Analysis
Method to get comprehensive results when performing a qualitative risk analysis	To determine scenarios with threats and impacts
Primary factor which determines either to use qualitative or quantitative approach?	Availability of the data
What is the most difficult data to perform quantitative analysis?	To derive accurate frequency/ probability/likelihood of occurrence

Self-Assessment Questions

(1) Risk quantification can be arrived through combination of:

A. impact and consequence
B. threat and exposure
C. probability and consequences
D. criticality and sensitivity

Answer: C. probability and consequences
Explanation: CRISC aspirants should always remember that risk Is the combination of probability and impact. Let us understand this with help of an example: Probability of damage for an equipment costing $ 1000 is 0. Here probability is zero and impact is $ 1000. Now, risk is probability * impact i.e. P * I. In this case risk is 1000*0 i.e. 0.
Now for some other asset if probability is 0.5 and asset costs $ 100, then risk will be $ 50 (0.5 * 100).
Risk of equipment costing $ 100 is more than risk of equipment costing $1000. This is because probability plays an important role in quantification of risk.

(2) Use of statistical method to derive probability and impact is best considered in:

A. qualitative risk analysis
B. quantitative risk analysis
C. probability approach

D. risk scenario

Answer: B. quantitative risk analysis
Explanation: In quantitative risk assessment, risk is measured on the basis on numerical values. This helps in cost benefit analysis as risk in monetary terms can be easily compared to cost of various risk responses. In quantitative risk assessment, various statistical methods are used to derive the risk.

(3) Most important factor in quantitative risk analysis process is:

A. net present value (NPV)
B. earned value analysis (EVA)
C. decision support system
D. expected monetary value (EMV)

Answer: D. expected monetary value (EMV)
Explanation: Expected monetary value (EMV) is the weighted average of probable outcomes. It helps to determine expected average payoff by assuming a certain amount of probabilities. This calculation is very important in quantification of risk over the period of time. Other options are not as significant as expected monetary value.

(4) Impact of a failed equipment can be arrived by:

A. determining the actual cost of equipment damaged
B. determining current cost of new equipment
C. use of quantitative and qualitative approach to determine impact of business
D. reviewing contractual requirement to determine liability

Answer: C. use of quantitative and qualitative approach to determine impact of business
Explanation: Impact of a failed equipment is not only restricted to the cost of the equipment but also includes impact on business processes due to failure of equipment. Risk practitioners should use various approaches to determine the overall impact on the business due to failure of equipment.

(5) Main factor for deciding between qualitative approach and quantitative approach is:

A. availability of the data
B. budget for risk assessment
C. culture of the organization
D. availability of time

Answer: A. availability of the data
Explanation: A risk practitioner would always prefer a quantitative approach. Quantitative approach helps in cost benefit analysis as risk in monetary terms can be easily compared to cost of various risk responses. However, a major challenge in conducting a quantitative risk analysis is availability of accurate data. In absence of proper data or when data accuracy is questionable, qualitative analysis is more preferable.

(6) In which of the following risk assessment processes, probability and impact is used to calculate level of risk?

A. qualitative risk analysis
B. quantitative risk analysis
C. financial approach
D. fault tree analysis

Answer: B. quantitative risk analysis
Explanation: CRISC aspirants should always remember that risk is quantified by combination of probability and impact. Let us understand this with help of an example: Probability of damage for an equipment costing $ 1000 is 0. Here probability is zero and impact is $ 1000. Now, risk is probability * impact i.e. P * I. In this case risk is 1000*0 i.e. 0. Now for some other asset if probability is 0.5 and asset costs $ 100, then risk will be $ 50 (0.5 * 100). Risk of equipment costing $ 100 is more than risk of equipment costing $1000. This is because probability plays an important role in quantification of risk.
(7) Most important challenge in conduct of quantitative risk analysis is:

A. getting accurate details on impact of risk event
B. getting accurate details on frequency of risk event
C. getting accurate details on asset valuation
D. getting accurate details of annual loss expectancy

Answer: B. getting accurate details on frequency of risk event

Explanation: Greatest challenge for conduct of quantitative risk assessment is availability of reliable data. To quantify a risk, accurate details of probability and impact is required. Determining the probability or frequency of the occurrence of threat is a challenging aspect. Mostly, probability can be arrived at on the basis of historical data. However, it is very difficult to ascertain the probability of natural events such as hurricanes, earthquakes, tsunamis etc. Getting details on impact or asset valuation or annual loss expectancy is not as difficult as determining the frequency of the event.

(8) Which of the following approaches is used to arrive at the financial impact of a specific individual risk scenario?

A. qualitative risk analysis
B. quantitative risk analysis
C. financial risk modelling
D. fault tree analysis

Answer: B. quantitative risk analysis
Explanation: In quantitative risk assessment, risk is measured on the basis on numerical values. This helps in cost benefit analysis as risk in monetary terms can be easily compared to cost of various risk responses. This is the best approach. Financial risk modelling is generally used to determine aggregate risk as compared to individual risk scenarios.

(9) Which of the following risk assessment methods involves conducting interviews and using anonymous questionnaires by subject matter experts?

A. qualitative risk analysis
B. quantitative risk analysis
C. financial risk modelling

D. monte carlo analysis

Answer: A. qualitative risk analysis
Explanation: Qualitative risk analysis method involves conducting interviews of various stakeholders. There are some techniques like Delphi method wherein information can be gathered by way of anonymous questionnaires. Monte Carlo simulation combines both qualitative and quantitative assessment methods. Quantitative and financial modelling uses statistical based analysis.

(10) Best method to provide comprehensive result by conducting qualitative risk analysis is:

A. scenario with threats and impact
B. asset valuation
C. risk valuation
D. loss estimate ratio

Answer: A. scenario with threats and impact
Explanation: Best method to provide a comprehensive result by conducting qualitative risk analysis is a scenario with various threats and impacts. In this approach, risk practitioners examine various internal and external scenarios and try to determine the impact of each scenario on business processes. Other options are not as effective as scenarios with threats and impact.

Chapter 3 Risk Response & Mitigation

Risk response and mitigation are the action plans that are put in place to minimize the impact of risk events, Risk response process occurs after risks have been identified and analyzed and provides an answer to the question of “What are we going to do about it?” This chapter covers following topics:

3.1 Aligning Risk Response with Business Objective
3.2 Risk Response Options
3.3 Analysis Techniques
3.4 Vulnerabilities associated with new controls
3.5 Developing a Risk Action Plan
3.6 Business Process Review Tools and Techniques

3.1 Aligning Risk Response with Business Objective

Enterprise Wide Risk Management Framework

Enterprise wide risk management framework means adoption of common framework throughout the organization. Organizations adopting an enterprise risk management framework have an advantage of consistent risk management approach. All the functions and departments use the same standard risk management framework.

It helps to club all the risks faced by the organization at one place and thus risk can be prioritized in an effective manner and accordingly risk response strategy can be designed.

Involvement of Stakeholders

It is utmost important for an effective risk management program to have participation and involvement of relevant stakeholders in risk related decision and risk monitoring. 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. Process owners and other stakeholders have ground level knowledge and detailed understanding related to risk faced by their function. Their involvement in the risk management program improves the overall effectiveness of the risk management program.

To determine whether a system is serving the needs of the business process, risk practitioners should interact with business process owners.

Involvement of Senior Management

Involvement of senior management in information security investment can be best ensured by explaining the impact of security risk on business objectives. Once the senior management understands the impact of risk on business goals and achievement, they get themselves involved in the risk management process.

Alignment of Risk Appetite with Business Objective

Organizations should align each risk and risk appetite with business objectives. Risk appetite is the amount of risk an organization is willing to take. This will help to prioritize the risk response and also helps to monitor the areas of low risk tolerance. For example, an organization with 10 business objectives may have a different risk appetite for each objective. They may have 2 critical business objectives with very low risk appetite and for other objectives risk appetite is higher. Resources should be utilized primarily to address the risks of these 2 business objectives with low risk appetite.

Risk Prioritization

Risk impacting the laws and regulations and top business objectives should be addressed on priority. Risk assessment report and risk register should indicate the priority level of each risk. In a top down risk analysis, business objectives are identified first and then risk related to business objectives are determined. These risks are given priority for mitigation. Organizations should determine the best response and develop a mitigation plan to address the risk.

IT Steering Committee

The role of an IT steering committee is to ensure that the IT department is in harmony with the organization's mission and objectives. To ensure this, the committee must determine whether IT processes support the business requirements. The IT steering committee monitors and facilitates deployment of IT resources for specific projects in support of business plans. Steering committee should consist of Key executives and representatives from user management.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
What is the benefit of adopting an organization wide risk management framework?	Consistent approach for risk management
Effectiveness of a risk management program can be best ensured by	Participation of relevant stakeholders
What is the benefit of aligning the risk appetite with business objectives?	Monitoring the areas of low risk tolerance
In a top down approach, most important factor is to identify:	Business Objectives
To determine that systems are meeting their individual business process needs, interview should be conducted with	Business Process Owner

Self-Assessment Questions

(1) Main objective of adopting organization wide risk management framework is:

A. flexibility in risk response program

B. reduction is risk management cost
C. centralize maintenance of risk response program
D. consistent approach of risk response throughout the organization

Answer: D. consistent approach of risk response throughout the organization
Explanation: Enterprise wide risk management framework means adoption of common framework throughout the organization. Organizations adopting an enterprise risk management framework have an advantage of consistent risk management approach. All the functions and departments use the same standard risk management framework. This ensures a standardized risk management approach through the organization. It helps to club all the risks faced by the organization at one place and thus risk can be prioritized in an effective manner and accordingly risk response strategy can be designed.

(2) 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. involvement 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.

(3) Main objective of aligning risk appetite to business objective is to ensure:

A. objectives with high risk areas are given priority
B. all risks are identified and eliminated
C. common IT and business goals are identified
D. the risk framework is appropriately communicated

Answer: A. objectives with high risk areas are given priority.

Explanation: Risk appetite is the amount of risk an organization is willing to take. If risk appetite is aligned with business objectives, valuable resources can be deployed toward those objectives where the risk is high. This will help to prioritize the risk response and also helps to monitor the areas of low risk tolerance. For example, an organization with 10 business objectives may have a different risk appetite for each objective. They may have 2 critical business objectives with very low risk appetite and for other objectives risk appetite is higher. Resources should be utilized primarily to address the risks of these 2 business objectives with low risk appetite.

(4) Most important factor in a top-down approach for developing a risk scenario is to identify:

A. business objective
B. IT infrastructure
C. critical processes
D. external risk

Answer: A. business objective

Explanation: In top-down approach, risk scenario development is performed by identifying business objectives. Risk scenarios are developed for risk events that can directly impact the business goals and objectives. Other options are more relevant from the bottom up approach.

(5) Involvement of senior management in information security investment can be best ensured by:

A. explaining technical risk to senior management
B. explaining best practices adopted by the industry
C. explaining security budget
D. explaining impact of security risk on business objective

Answer: D. explaining impact of security risk on business objective
Explanation: Involvement of senior management in information security investment can be best ensured by explaining the impact of security risk on business objectives. Once the senior management understands the impact of risk on business goals and achievement, they get themselves involved in the risk management process.

(6) IT steering committee should be best composed of:

A. members of the board of directors
B. external IT experts
C. members of the IT dept.
D. key members from each department

Answer: D. key members from each department
Explanation: The role of an IT steering committee is to ensure that the IT department is in harmony with the organization's mission and objectives. To ensure this, the committee must determine whether IT processes support the business requirements. The IT steering committee monitors and facilitates deployment of IT resources for specific projects in support of business plans. Steering committee should consist of Key executives and representatives from user management. Only IT members will not serve the objective of the committee. Board members generally are not expected to be involved in implementation.

3.2 Risk Response Options

Following are the four options for responding to the risk:

Risk Avoidance

- In this approach, projects or activities that cause the risk are avoided.
- Risk avoidance is the last choice when no other response is adequate.
- For example, declining a project when business cases show a high risk of failure.

Risk Mitigation

- In this approach efforts are made to reduce the probability or impact of the risk event by designing the appropriate controls.
- Objective of risk mitigation is to reduce the risk to an acceptable level.

Risk sharing/Transferring

- In this approach, risk is shared with partners or transferred via insurance coverage, contractual agreement or other means.
- Natural disasters have a very low probability but a high impact. Response for such risk should be risk transfer.

Risk Acceptance

- In this approach, risk is accepted as it is in accordance with risk appetite of the organisation.
- Risk is accepted where cost of controlling the risk is more than the cost of risk event.
- For example, for few non critical systems, the cost of anti-malware installation is more than the anticipated cost of damage due to malware attack. In such cases, the organization generally accepts the risk as it is.
- In risk acceptance, no steps are taken to reduce the risk.
- However, organizations need to be utmost careful while accepting the risk. If risk is accepted without knowing the correct level of risk, it may result in a higher level of liabilities.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
Which is the most suitable risk response where cost of control exceeds the cost of risk event?	Risk Acceptance
Risk avoidance can be done by	Exiting the process that causes the risk
Adoption of which risk response may result in higher liability?	Risk Acceptance (Organization may choose to accept risk without knowing the correct level of risk that is being accepted; this may result in higher liabilities)
Risk response in which process is outsourced to a professional organization having expertise knowledge	Risk Mitigation
Which is the most suitable risk response where risk related to a specific business process is greater than the potential opportunity?	Risk Avoidance
Purchasing an insurance is an example of which risk response?	Risk transfer
What is the use of a business case?	Business case helps to determine the costs and

	benefits of the risk response.
What is the most important aspect in risk mitigation?	To reduce the risk to an acceptable level
What is the most effective way to treat a risk with a low probability and a high impact (such as natural disaster)?	Risk Transfer

Self-Assessment Questions

(1) Most effective risk response where the cost of installation of anti-malware software exceeds the expected loss of threat is:

A. risk avoidance
B. risk acceptance
C. risk transfer
D. risk mitigation

Answer: B. risk acceptance
Explanation: In the risk acceptance approach, risk is accepted as it is without taking action to mitigate the same. This is a more prevalent approach where the cost of controlling the risk is more than the cost of the risk event. For example, for few non critical systems, the cost of anti-malware installation is more than the anticipated cost of damage due to malware attack. In such cases, the organization generally accepts the risk as it is.

(2) Characteristic of risk avoidance is:

A. no action is taken on the perceived risk
B. transfer the perceived risk to third party
C. stop the process that give rise to perceived risk
D. implement controls to minimize the perceived risk

Answer: C. stop the process that give rise to perceived risk
Explanation: In risk avoidance approach, projects or activities that cause the risk are avoided. Risk avoidance is the last choice when no other response is adequate. For example, declining a project when business cases show a high risk of failure.

(3) When a risk practitioner recommends implementation of several controls to protect IT resources, which of the following approaches is recommended?

A. risk avoidance
B. risk acceptance
C. risk transfer
D. risk mitigation

Answer: D. risk mitigation
Explanation: In risk mitigation approach efforts are made to reduce the probability or impact of the risk event by designing the appropriate controls. Objective of risk mitigation is to reduce the risk to an acceptable level.

(4) Risk response that most likely increases the liability of the organization is:

A. risk avoidance
B. risk acceptance
C. risk transfer
D. risk mitigation

Answer: B. risk acceptance
Explanation: Risk response that most likely increases the liability of the organization is risk acceptance. However, organizations need to be utmost careful while accepting the risk. If risk is accepted without knowing the correct level of risk, it may result in a higher level of liabilities.

(5) Outsourcing of a process is an example of:

A. risk avoidance
B. risk acceptance
C. risk transfer
D. risk mitigation

Answer: D. risk mitigation
Explanation: Outsourcing of a process is an example of risk mitigation. Through outsourcing various process risks are mitigated with help of service providers having relevant expertise and experience. It must be noted that outsourcing does not reduce or remove the accountability of the organization.

(6) In a scenario where risk is greater than potential opportunity, the best risk response is:

A. risk avoidance
B. risk acceptance
C. risk transfer
D. risk mitigation

Answer: A. risk avoidance
Explanation: In the risk acceptance approach, risk is accepted as it is without taking action to mitigate the same. This is a more prevalent approach where the cost of controlling the risk is more than the cost of the risk event. For example, for few non critical systems, the cost of anti-malware installation is more than the anticipated cost of damage due to malware attack. In such cases, the organization generally accepts the risk as it is.

(7) Taking an insurance is an example of:

A. risk avoidance
B. risk acceptance
C. risk transfer
D. risk mitigation

Answer: C. risk transfer
Explanation: Taking insurance is an example of risk transfer. In risk transfer, risk is shared with partners or transfer via insurance coverage, contractual agreement or other means. Natural disasters have a very low probability but a high impact. Response for such risk should be risk transfer.

(8) Which of the following is utilized by risk practitioners to propose a risk mitigation activity?

A. technical feasibility
B. business case

C. security budget
D. vulnerability assessment

Answer: B. business case
Explanation: Risk mitigation activity is based on business case. Business case includes cost benefit analysis of implementing a mitigation plan.

(9) To ensure that information systems control deficiencies are appropriately remediated, a risk practitioner should review:

A. risk mitigation plan
B. countermeasure analysis
C. threat analysis
D. business impact analysis

Answer: A. risk mitigation plan
Explanation: A risk mitigation plan is a detailed document which includes name of officer responsible for risk mitigation, risk mitigation monitoring process, milestone achievement and timelines for implementation of plan. Review of risk mitigation plan will provide the details of remediation of control deficiencies.

(10) Objective of a risk mitigation is:

A. to remove all the threats and vulnerabilities
B. to reduce the probability of the occurrence of the event
C. to reduce the risk within acceptable level
D. to appoint a risk practitioner

Answer: C. to reduce the risk within acceptable level
Explanation: Objective of a risk mitigation is to reduce the risk within acceptable level. It is not possible to remove all the threats and vulnerabilities or to reduce the probability of the occurrence of an event.

(11) Best response for a risk scenario with low probability and high impact like natural disaster is:

A. risk avoidance
B. risk acceptance
C. risk transfer
D. risk mitigation

Answer: C. risk transfer
Explanation: Taking insurance is an example of risk transfer. In risk transfer, risk is shared with partners or transfer via insurance coverage, contractual agreement or other means. Natural disasters have a very low probability but a high impact. Response for such risk should be risk transfer.

3.3 Analysis Techniques

Organizations need to evaluate various risk responses to determine appropriate responses for the given risk. Organization should consider following factors for selecting a risk response:

1. Risk priority
2. Recommendation of risk assessment report

3. Cost of risk response as against possible cost of risk event
4. Legal and regulatory compliance
5. Alignment of the response as per the organization's strategy
6. Efforts for control implementation in terms of time, resources and expenditure
7. Compatibility with existing controls

Organization should determine what the cost of implementing a specific risk response provides enough value to the organization. Business case provides detailed analyses on various risk responses on which management may take a decision. Business case is prepared with use of following two common methods of analysis:

1. Cost benefit analysis
2. Return on investment (ROI)

Cost-benefit Analysis

- Cost benefit analysis is conducted during the risk response planning stage.
- Objective of a cost benefit analysis is to determine cost of implementing controls and relevant benefit realization.
- If the benefit realized from the control is less than the cost of implementation of control, then It does not justify the implementation of the control.
- Cost and benefit is calculated either through qualitative or through quantitative methods.
- While determining the cost, total cost of ownership (TCO) should be considered to cover total cost spread across the life cycle of control implementation.
- The impact or benefit realization is considered on the basis of length of the outage, the frequency of the outage and other associated damage to the organization.
- Selection of a risk response is primarily based on the cost benefit analysis.

Return on Investment

Return on investment is a method in which it is determined how long it will take to recover the cost of control through value added or other savings produced. It is also known as return on security investment for expenditure made on security controls.

For investing in control, this is a tricky calculation as it depends on predicting the likelihood and impact of an attack. Most important criteria for selection of risk response is cost benefit analysis. Investment in implementing a control should bring appropriate benefit to the organization.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
What is the basis on which risk response is selected and prioritized?	Cost benefit analysis
Most relevant cost to be included in a cost	Total cost of ownership (TCO)

benefit analysis	(to cover total cost spread across the life cycle of control implementation)
At what stage of risk management, cost-benefit analysis is conducted?	Risk Response

Self-Assessment Questions

(1) A risk practitioner noted that various alternatives are available for risk response. Risk response is selected and prioritized on the basis of:

A. cost benefit analysis of various risk response alternatives
B. experience of risk practitioner
C. business impact analysis
D. security budget

Answer: A. cost benefit analysis of various risk response alternatives
Explanation: Most important criteria for selection of risk response is cost benefit analysis. Investment in implementing a control should bring appropriate benefit to the organization.

(2) Most important aspect to be included in cost benefit analysis is:

A. security budget
B. total cost of ownership
C. likelihood of incidents
D. impact of incidents

Answer: B. total cost of ownership
Explanation: Objective of a cost benefit analysis is to determine cost of implementing controls and relevant benefit realization. While determining the cost, total cost of ownership (TCO) should be considered to cover total cost spread across the life cycle of control implementation.

(3) In which of the risk management phases, cost benefit analysis is mainly conducted?

A. risk assessment
B. risk response planning
C. risk valuation
D. vulnerability assessment

Answer: B. risk response planning
Explanation: Cost benefit analysis is mainly conducted during the risk response planning stage. Objective of a cost benefit analysis is to determine cost of implementing controls and relevant benefit realization.

3.4 Vulnerabilities associated with new controls

Once the new control is implemented, it is recommended to test the control to ensure that risk has been appropriately mitigated. It must be noted that each new control implemented should be evaluated for additional vulnerabilities.

In few cases, it may happen that these additional risks may exceed the risk that it is meant to address.Conduct of user acceptance testing may help to identify vulnerabilities with respect to new controls.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
What is the best action after implementation of a new control?	To test the control to ensure that it mitigates the risk

Self-Assessment Questions

(1) Best course of action once the new control in being implemented is:

A. to test the control to validate its effectiveness
B. to update the risk register with respect to implemented control
C. to conduct a fresh risk assessment
D. to conduct cost benefit analysis of the new control

Answer: A. to test the control to validate its effectiveness
Explanation: Best course of action once the new control in being implemented is to test the control to validate its effectiveness. Once the new control is implemented, it is recommended to test the control to ensure that risk has been appropriately mitigated. It must be noted that each new control implemented should be evaluated for additional vulnerabilities.

3.5 Developing a Risk Action Plan

- Risk practitioners should play a consultative role in assisting risk owners and help them to decide appropriate risk responses.
- Final decision on risk response should be taken by the risk owner but risk practitioners should guide him on technologies, policies, procedures, control effectiveness and leveraging of existing controls.
- If the current risk is above the risk appetite of the organization, then a further risk response is required to bring down the level of risk.
- Different alternatives for risk response are evaluated and analyzed. Risk responses are prioritized by considering the cost-benefit analysis of each alternative.
- Once a risk response is finalized, a risk action plan is created and documented in the risk register. Risk action plan should include a start date, end date, details about strategy, details about the responsible person or team.
- For effective implementation of an action plan, it is recommended to assign the responsibility of implementing the action plan to concerned individuals along with timelines for the implementation.
- Risk action plan should be considered as a project. Critical paths of the project should be properly monitored because delays in these elements increase overall project risk.
- Implemented control should be reviewed at frequent intervals to ensure that identified risk is kept at an acceptance level.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
What is the best way to ensure that identified risk is kept at an acceptable level?	Periodic review of the control
Risk action plan must include	● Start data ● End data ● Responsible person ● Detail action plan

Self-Assessment Questions

(1) How should a risk practitioner ensure that risk is kept at an acceptable level?

A. periodic review of controls as per risk action plan
B. documenting all the risk in the risk register
C. maintaining department wise risk register
D. maintaining a key risk indicator in risk register

Answer: A. periodic review of controls as per risk action plan
Explanation: Control should be reviewed periodically to ensure that they are effective to keep the risk at acceptable level. Other options are not as effective as periodic review of control. Mere documenting the risk will not serve the purpose.

(2) Once the mitigation action plan is approved by the management, which of the following best supports the implementation of mitigation action plan?

A. presenting root cause analysis to the management
B. use of centralized software to track the action point
C. communicating the risk to the shareholders
D. assigning action plans to responsible individual along with deadlines

Answer: D. assigning action plans to responsible individual along with deadlines
Explanation: For effective implementation of an action plan, it is recommended to assign the responsibility of implementing the action plan to concerned individuals along with timelines for the implementation. Other options are not as effective as option D.

(3) Risk action plan must include:

A. assigned responsibility to an individual
B. cost of implementation
C. probability of occurrence
D. impact of the event

Answer: A. assigned responsibility to an individual
Explanation: Risk action plan should include a start date, end date, details about strategy, details about the responsible person or team for implementing the action plan. For effective implementation of an action plan, it is recommended to assign the responsibility of implementing the action plan to concerned individuals along with timelines for the implementation.

3.6 Business Process Review Tools and Techniques

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

- Process review can be carried out from knowledgeable representatives within the organization or with the help of external experts.

- 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 review is conducted in following steps:
  1. Review the current documentation and processes and understand roles and responsibilities of each process. Understand the current risk and control environment.
  2. Identify the areas of improvement through focus groups and workshops.
  3. Implement the changes
  4. Obtain feedback about changes and evaluate the same for further improvement.

- 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.

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

Self-Assessment 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.

3.7 Control Design & Implementation

Control design and implementation is one of the important steps in risk management. An effective control should be able to prevent or detect and recover from the event with minimum adverse impact.All the implemented controls should be documented in a risk register.

Proactive or Reactive Controls

Control can be either proactive or reactive. Proactive controls attempt to prevent an adverse impact whereas reactive control attempts to detect and recover from an incident. Proactive control is also known as safeguards whereas reactive control is also known as countermeasures. Use of a physical security guard outside the processing area is a proactive control or safeguard to prevent any unauthorised entry. Use of a fire extinguisher is a reactive control or countermeasure against the risk of fire.

Stakeholders Requirements

The most important factor for designing IS controls is that they should be aligned with the requirements of the business processes and should be able to address the stakeholder's requirement.

Process owners should provide the control requirements on the basis of the business needs and objectives.Internal controls should be incorporated in the new system development at the design phase itself. This will help in designing and developing effective and efficient internal control systems.

Board of directors and senior management is accountable for risk policies, guidelines and standards.Board of directors and senior management is accountable for risk policies, guidelines and standards.

Role of Risk practitioner

Role of risk advisor is to provide advice on the control selection and implementation procedure. Risk practitioners should evaluate the adequacy of the current controls. In case current controls are not sufficient, he should recommend implementation of new controls.

Threat vis-à-vis Vulnerability

CRISC aspirants should be able to establish the difference between threat and vulnerability. Vulnerability means weakness in the system. Threat is a factor that attempts to exploit the vulnerability. For example, when an anti-virus is not updated it is a vulnerability. Hacker who attempts to exploit the vulnerability (un-updated anti-virus) is a threat. Objective of an internal control is to reduce the vulnerability i.e. weakness. Internal control cannot directly control the threat.

Control Standards and Frameworks

- Implementation of control requires documented policies and procedures. Accountability should be established for control implementation and monitoring. Implementation of industry specific standards and frameworks helps an organization to build a structured control environment.

- ISO 27001 standard is a widely accepted and recognized standard for information security management systems (ISMS). Payment Card Industry Data Security Standard (PCI DSS) is used by all organizations that process debit or credit cards. HIPAA is a recognized standard for the health industry.

- Many countries require mandatory implementation of certain standards by the organization.

Administrative, Technical and Physical Controls

Following table depicts details of different types of control:

Managerial/ Administrative

Managerial control involves oversight of the processes. Examples of managerial controls are policies and procedures, audit, risk and compliance reporting etc. Managerial control aims to monitor the function of technical as well as physical control.

Technical

In technical controls, control is implemented through use of technology and with minimum human intervention.They are also termed as logical controls. Examples of technical controls include logical access, firewalls, antivirus software, IDS etc.A technical control requires proper managerial (administrative) controls to operate correctly.

Physical

In physical controls, the objective is to control physical movement of employees and assets. Examples of physical control include security guards, locks, fences, CCTV and devices that are installed to physically restrict access to a facility or hardware.

Preventive, Corrective, Detective, Deterrent, Compensating Controls

Following table depicts details of different types of control:

Preventive Control

Preventative controls are designed to be implemented in such a way that it prevents the threat event and thus avoid the potential impact. Examples of preventive controls include:

- Use of qualified personnel
- Segregation of duties
- Use of SOPs to prevent errors
- Transaction authorization procedures
- Edit checks
- Access control procedures
- Firewalls
- Physical barriers

Detective Control

Detective controls are designed to detect a threat event once the event has occurred. Detective controls aim to reduce the impact of the event. Examples of detective controls include:

- Internal Audit & other reviews
- Log monitoring
- Hash totals
- Checkpoints in production jobs
- Echo controls in telecommunications
- Error messages over tape labels
- Variance Analysis
- Quality Assurance

Corrective Control

Corrective controls are designed to minimize the impact of a threat event once it has occurred and helps in restoring to normal operations. Examples of corrective controls include:

- Business continuity planning
- Disaster recovery planning
- Incident response planning
- Backup procedures

Deterrent Control

Purpose of a deterrent control is to give a warning signal to deter or discourage the threat event. Examples of deterrent controls include:

- CCTV cameras - under surveillance signs
- Warning signs

Compensating Controls

Compensating controls are alternate measures that are employed to ensure that weakness in the system is not exploited. In many cases, a strong control in one area can compensate for weakness in another area. For example, in small organizations, segregation of duties may not always be feasible. In such cases, compensatory controls such as review of log should be implemented.

Compensating controls are an indirect way to monitor and control the transaction. For lack of segregation of duties, compensating control may be monitoring of transaction logs and conducting audits.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Questions
What is the most important factor for designing the controls?	To address the stakeholder's requirements
What is the best method for creating access rights for temporary staff?	● With auto expiration date ● Only need to know access
What is the best control to protect data in a USB device?	Encryption
System backup and restore procedures is example of	Corrective control
Internal control should be incorporate in which SDLC phase	Design Phase
Accountability for risk policies, guidelines and standards	● Board of Directors ● Sr. Management
Internal control requirement should be provided	Process owners
Controls are most effective when they are designed to reduce	Vulnerabilities
Example of managerial controls	● Policies and procedures ● Audit, risk and compliance reporting etc.

Self-Assessment Questions

(1) Most important factor for designing a control is:

A. implementation methods
B. technical requirements
C. security budget
D. requirement of the stakeholder

Answer: D. requirement of the stakeholder

Explanation: The most important factor for designing IS controls is that they should be aligned with the requirements of the business processes and should be able to address the stakeholder's requirement. Process owners should provide the control requirements on the basis of the business needs and objectives.

(2) Best control for providing access to temporary staff:

A. is to log all the transactions
B. is to provide need to know access with predefined expiry date
C. is to obtain security acknowledgement from each user
D. is to circulate security do's and don'ts to each user

Answer: B. is to provide need to know access with predefined expiry date
Explanation: Best method for creating access rights for temporary staff is to provide access with auto expiry date and with need to know the basis only. Other options are good control but they are not as effective as option B.

(3) Best control to secure data on USB is:

A. authentication based access
B. read only data in USB device
C. encrypting the USB device
D. restricted use of USB device

Answer: C. encrypting the USB device
Explanation: Encryption provides the most effective protection of data on mobile devices. Encryption converts the data in the USB in an unreadable form. It can be read only by the person possessing the encryption key. Other options are good control but they are not as effective as encryption of the USB device.

(4) Backup arrangement is considered as:

A. corrective control
B. deterrent control
C. preventive control
D. detective control

Answer: A. corrective control
Explanation: Corrective controls are designed to minimize the impact of a threat event once it has occurred and helps in restoring to normal operations. Objective of a backup data is to restore the functioning in case original data is lost or corrupted.

(5) In which phase of SDLC, internal control should be best to be incorporated?

A. design phase
B. development phase
C. testing phase
D. implementation phase

Answer: A. design phase
Explanation: For success of a project, control requirements should be analyzed and incorporated during the design phase of the SDLC. Incorporating controls at later stages will be a risky affair. Internal control should be incorporated at the initial stage itself.

(6) Who is accountable for the organization's risk policies, procedures and frameworks?

A. management
B. legal
C. risk management
D. audit

Answer: A. management
Explanation: Final accountability for organization’s risk policies, procedures and frameworks resides with management. Audit, risk management and legal provides support to the management for effective risk management.

(6) Internal control requirement should come from:

A. audit dept.
B. risk management dept.
C. process owners
D. IT dept.

Answer: C. process owners
Explanation: The most important factor for designing IS controls is that they should be aligned with the requirements of the business processes and should be able to address the stakeholder’s requirement. Process owners should provide the control requirements on the basis of the business needs and objectives.

(7) Objective of an internal control is to reduce:

A. threats
B. vulnerability
C. probability
D. uncertainty

Answer: B. vulnerability
Explanation: CRISC aspirants should be able to establish the difference between threat and vulnerability. Vulnerability means weakness in the system. Threat is a factor that attempts to exploit the vulnerability. For example, when an anti-virus is not updated it is a vulnerability. Hacker who attempts to exploit the vulnerability (un-updated anti-virus) is a threat. Objective of an internal control is to reduce the vulnerability i.e. weakness. Internal control cannot directly control the threat.

(8) Security policy is an example of:

A. operational control
B. technical control
C. detective control
D. management control

Answer: D. management control
Explanation: Managerial control involves oversight of the processes. Examples of managerial controls are policies and procedures, audit, risk and compliance reporting etc. Managerial control aims to monitor the function of technical as well as physical control.

3.9 Types of Risk

Understanding Inherent and Residual Risk

Let us understand this with an example. You purchased a machine costing 100000$ which is placed in an earthquake sensitive zone. Any damage to the machine will cost you 100000$. To safeguard against this loss, you take insurance worth 80000$ for the machine. Now if anything happens to your machine, the insurance company will reimburse you upto 80000$. Your final loss will be only 20000$.

In this case, your risk before taking an insurance is 100000$. This risk is known as inherent risk i.e. gross risk or risk before implementing any control.

Risk after taking insurance is only 20000$. This risk is known as residual risk i.e. net risk or risk after implementing any control.

Inherent Risk

The risk that an activity would pose if no controls or other mitigating factors were in place (the gross risk or risk before controls). It is Susceptibility of a business or process to make an error that is material in nature, assuming there were no internal controls.

Inherent risk depends on the number of users and business areas. Higher the number of users and business processes, higher will be the level of inherent risk.

Residual Risk

The risk that remains after controls are taken into account (the net risk or risk after controls). Residual Risk = Inherent Risk - Controls. For a successful risk management program, residual risk should be within the risk appetite. When residual risk is within the risk appetite, it is acceptable risk level.

Primary objective of a risk management program is to ensure that residual risk is within the acceptable level by the management. If residual risk is within the risk appetite of the organization, it determines the compliance with risk appetite. Achievement of acceptable risk indicates that residual risk is minimized and within control.

Detection Risk

Risk that the auditors fail to detect a material misstatement in the financial statements.

Control Risk

Risk that a misstatement could occur but may not be detected and corrected or prevented by the entity's internal control mechanism.

Key aspects from CRISC exam perspective

CRISC Question	Possible Answer
Which risk indicates susceptibility of a business or process to make an error that is material in nature, assuming there were no internal controls?	Inherent Risk

Which risk indicates that the controls put in place will not prevent, correct, or detect errors on a timely basis?	Control Risk
What is the primary objective of a risk management program?	To ensure that residual risk is within the acceptable level by the management
Which risk increases due to multiple business areas?	Inherent Risk
Achievement of acceptable risk indicates that	Residual risk is minimized and within control.

Self-Assessment Questions

(1) The susceptibility of a business or process to make an error that is material in nature, assuming there were no internal controls is:

A. Inherent risk
B. Control risk
C. Detection risk
D. Correction risk

Answer: A. Inherent risk
Explanation: Inherent risk means the risk that an activity would pose if no controls or other mitigating factors were in place (the gross risk or risk before controls).

(2) The risk that the controls put in place will not prevent, correct, or detect errors on a timely basis is:

A. Inherent risk
B. Control risk
C. Detection risk
D. Correction risk

Answer: B. Control risk
Explanation: Control risk means the risk that a misstatement could occur but may not be detected and corrected or prevented by the entity's internal control mechanism.

(3) Main objective of a risk management program is:

A. to make residual risk as zero
B. to implement technical control for every threat
C. to eliminate all inherent risk
D. to maintain residual risk at acceptable level

Answer: D. to maintain residual risk at acceptable level
Explanation: Main objective of a risk management program is to control and maintain the residual risk within acceptable levels. For a successful risk management program, residual risk should be within the risk appetite. When residual risk is within the risk appetite, it is acceptable risk level. It is not practical and feasible to make residual risk as zero or to implement technical control for every threat or to eliminate all inherent risk.

(4) To determine compliance with risk appetite of the organization, risk practitioner should review:

A. residual risk and acceptable risk
B. inherent risk and acceptable risk
C. control risk and acceptable risk
D. preventive control and detective control

Answer: A. residual risk and acceptable risk
Explanation: Residual risk is the risk that remains after the controls are implemented. If residual risk is within the risk appetite of the organization, it can be considered as acceptable. Hence to determine compliance with the risk appetite of the organization, risk practitioners should review residual risk and acceptable risk.

(5) Which of the following risks is naturally high for the projects that impact multiple businesses?

A. compliance risk
B. residual risk
C. inherent risk
D. control risk

Answer: C. inherent risk
Explanation: Inherent Risk is the risk that an activity would pose if no controls or other mitigating factors were in place (the gross risk or risk before controls). It is Susceptibility of a business or process to make an error that is material in nature, assuming there were no internal controls. Inherent risk depends on the number of users and business areas. Higher the number of users and business processes, higher will be the level of inherent risk.

(6) To achieve acceptable risk, which of the following should be minimized?

A. inherent risk
B. transferred risk
C. accepted risk
D. residual risk

Answer: D. residual risk
Explanation: Residual risk is the risk that remains after the controls are implemented. For a successful risk management program, residual risk should be within the risk appetite. When residual risk is within the risk appetite, it is acceptable risk level. If residual risk is within the risk appetite of the organization, it can be considered as acceptable. Hence to achieve acceptable risk, residual risk should be minimized.

(7) Risk is said to be acceptable when:

A. transferred risk is reduced
B. inherent risk is reduced
C. control risk is reduced
D. residual risk is within the acceptable limit

Answer: D. residual risk is within the acceptable limit
Explanation: Residual risk is the risk that remains after the controls are implemented. If residual risk is within the risk appetite of the organization, it can be considered as acceptable. Hence risk is

said to be acceptable when residual risk is within the acceptable limit.

(8) Risk management practices can be considered as successful if:

A. control risk is controlled
B. inherent risk is eliminated
C. residual risk is within acceptable limit
D. overall risk is quantified

Answer: C. residual risk is within acceptable limit
Explanation: Main objective of a risk management program is to control and maintain the residual risk within acceptable levels. Other options are not as significant as minimizing the residual risk.

3.8 Control Monitoring and Effectiveness

Risk practitioners should ensure that appropriate processes are in place to evaluate and monitor the effectiveness of the control. Best way to determine the control effectiveness is to test the controls. Controls are to be tested at frequent intervals. The risk professional role is very important in control monitoring. Role of risk practitioner in the control monitoring process is to assist in planning, reporting and scheduling tests of IS controls.

Optimum level of controls

Maintaining controls at an optimal level helps to maintain a balance between control cost and control effectiveness & benefit. Control is said to be optimum when cost of control is less than the perceived risk. At optimum level of control, there is balance between control effectiveness and control cost. Control should be able to provide value to the organization.

Control monitoring for adherence to laws and regulations

Adherence to laws and regulations is one of the most important external requirements for an organization. Control should be implemented and monitored at periodic intervals to ensure that the organization is complying with legal and regulatory requirements. Legal and Regulatory requirements are the most important external requirements to which compliance should be monitored.

Control Monitoring and Reporting Tools and Techniques

While designing the control, care should be taken to address the control monitoring process. Monitoring and reporting of controls should be performed in the risk monitoring phase of risk management. In case controls are monitored through a managed security service provider (MSSP) or a security information and event management (SIEM), the system should have capability to capture and analyze the data.

Key aspects from CRISC exam perspective

CRISC Question	Possible Answer
What is the role of a risk practitioner in the IS control monitoring process?	Assists in planning, reporting and scheduling tests of IS controls
Maintenance of control at optimum level indicates	Balance between control effectiveness and cost

What is the key objective for maintaining control effectiveness for external requirements?	Compliance with regulatory and legal requirements
Best way to determine the control effectiveness	To the test the controls

Self-Assessment Questions

(1) Role of risk practitioner in control monitoring process is:

A. to implement and operate the control
B. to approve the control monitoring policy
C. to audit the internal control process
D. to assist in planning, reporting and scheduling tests of IS controls

Answer: D. to assist in planning, reporting and scheduling tests of IS controls
Explanation: Role of risk practitioner in control monitoring process is to assist in planning, reporting and scheduling tests of IS controls. Risk practitioners are not expected to implement and operate the control. It is the responsibility of the process owner. Control monitoring policy is approved by senior management.

(2) What does the optimum level of control mean?

A. at optimum level of control, lead time is shortest for control breach to be notified
B. at optimum level of control, there is balance between control effectiveness and control cost
C. at optimum level of control, residual risk is always zero
D. at optimum level of control, key risk indicator does not fluctuate

Answer: B. at optimum level of control, there is balance between control effectiveness and control cost
Explanation: Control is said to be optimum when cost of control is less than the perceived risk. At optimum level of control, there is balance between control effectiveness and control cost. Control should be able to provide value to the organization.

(3) Greatest reason for inclusion of change in control effectiveness in risk reporting is:

A. it helps in audit reporting
B. it impacts the risk profile
C. it helps in risk mitigation
D.it helps in selecting risk response

Answer: B. it impacts the risk profile
Explanation: Changes in the control impact the risk profile of the organization. Change may either make a control ineffective or may strengthen the enterprise's risk profile. Thus changes should be included in the risk report as it impacts the risk profile. Mere mention of change is risk report does not help in audit reporting or risk mitigation or selecting the risk response.

(4) Main reason to monitor the control effectiveness with respect to organization’s external requirement is:

A. to prepare for external audit

B. to create security policy for third party service provider
C. to comply with legal and regulatory requirements
D. to identify the legal aspects applicable to the organization

Answer: C. to comply with legal and regulatory requirements
Explanation: Adherence to laws and regulations is one of the most important external requirements for an organization. Control should be implemented and monitored at periodic intervals to ensure that the organization is complying with legal and regulatory requirements. Other options are not the prime reason for monitoring control effectiveness with respect to external requirements.

(5) Best way to determine control effectiveness is:

A. reviewing the test results
B. determining the preventive or detective nature of control
C. capability of control to notify the breach
D. reviewing key risk indicators

Answer: A. reviewing the test results
Explanation: Best way to determine the control effectiveness is to test the controls. Controls are to be tested at frequent intervals. Also, internal controls to be evaluated at regular intervals.

3.10.1 Third Party Risks

Risk practitioners should evaluate and determine the risk related to outsourcing of business processes. He should ensure that ownership of the data and processes remains with the organization. Risk practitioners should ensure that third party service providers have appropriate controls to address the security requirements as well as regulatory requirements. Risk practitioners should also ensure that security requirements of the organization are addressed in the outsourcing contract to make the service provider bound to comply with specific security requirements. Service level agreement should include declaring the jurisdiction of the agreement and which courts would hear any dispute related to the terms and conditions of the contract.

Right to Audit Clause

Periodic audit is the most effective method to ensure that service provider is complying with the security requirements of the service receiver. Service level agreement should include clauses with respect to the right to audit the system and processes of the service provider. The service provider may not allow the service receiver to audit them directly. In such cases, there should be a provision to assess compliance by an independent auditor. If such provision is not included in the agreement, then the service receiver has no way to ensure compliance or proper handling of their data.

Sub - contracting / Fourth Party

Service level agreement should specifically restrict the sub - contracting to a fourth party. In case it is allowed considering the business requirement, risk practitioners should consider the risk of subcontracting. In the case of subcontracting service receivers generally do not have control of the fourth party. The subcontracting process has to be thoroughly reviewed when the process involves sharing critical data.

Impact of Privacy Laws on Outsourcing

Risk practitioners should also ensure that laws and regulations are adhered to while outsourcing a process. For example, privacy law may prevent storage of personal data at offshore locations.

Compliance Responsibility

Service receiver retains the responsibility for ensuring compliance with regulatory requirements. Service receiver is the deemed to be owner of the data and responsible for the safe custody of the data. If the service provider fails to safeguard the data, authority will generally hold the organization responsible for non-compliance and take appropriate action including penalties.

Key aspects from CRISC exam perspective

CRISC Question	Possible Answer
What is the most important consideration for a risk practitioner while reviewing a outsourcing control?	Whether security requirements are addressed in the contract
What is the most important consideration for storage of private data at an offshore location?	Privacy laws may prevent a cross-border flow of information.
Who will be responsible for regulatory non-compliance? (Service receiver or service provider)	Organization who outsources the work (i.e. service receiver)
What is the best method to protect the confidentiality of data being transmitted over a network?	● Encapsulating the data packets ● Encryption
What is the best security measure when a third party is engaged in application development?	To conduct a security code review for the entire application to detect all the malware including back doors.

Self-Assessment Questions

(1) Risk practitioners are reviewing the process of outsourcing arrangements. Which of the following is the greatest concern?

A. high employee attrition rate of service provider
B. cost of outsourcing exceeds budget
C. critical data processing was subcontracted by service provider
D. service provider does not maintain system downtime register

Answer: C. critical data processing was subcontracted by service provider
Explanation: Service level agreement should specifically restrict the sub - contracting to a fourth party. In case it is allowed considering the business requirement, risk practitioners should consider the risk of subcontracting. In the case of subcontracting service receivers generally do not have control of the fourth party. The subcontracting process has to be thoroughly reviewed when the process involves sharing critical data.

(2) Risk practitioners are reviewing the process of outsourcing arrangements. Which of the following is the most important factor?

A. availability of policies and procedure to handle security exception

B. availability of security related clauses in outsourcing agreement
C. adherence to international standard for data processing by service provider
D. availability of information security team at service provider

Answer: B. availability of security related clauses in outsourcing agreement
Explanation: Risk practitioners should also ensure that security requirements of the organization are addressed in the outsourcing contract to make the service provider bound to comply with specific security requirements. Other options are not as important as availability of security related clauses in outsourcing agreements.

(3) Which of the following is the most important clause in any outsourcing contract?

A. inclusion of right to audit clause in outsourcing agreement
B. inclusion of provision to access compliance of the service provider in outsourcing agreement
C. inclusion of incident management process in outsourcing agreement
D. inclusion of encryption process in outsourcing agreement

Answer: B. inclusion of provision to access compliance of the service provider in outsourcing agreement
Explanation: Periodic audit is the most effective method to ensure that service provider is complying with the security requirements of the service receiver. Service level agreement should include clauses with respect to the right to audit the system and processes of the service provider. The service provider may not allow the service receiver to audit them directly. In such a case, there should be a provision to access the compliance by an independent auditor. If such provision is not included in the agreement, then the service receiver has no way to ensure compliance or proper handling of their data.

(4) Which of the following is the most important factor to decide outsourcing of a process to another country?

A. high cost of telecommunication setup
B. privacy law preventing cross border flow of information
C. time zone differences
D. software development complications

Answer: B. privacy law preventing cross border flow of information
Explanation: It is very important to ensure the applicable data privacy laws are adhered to. Some privacy laws prohibit the cross-border flow of personally identifiable information. Other options are not as significant as adherence to privacy laws.

(5) In case of an outsourced process, who will be responsible for violation of any regulatory requirement by a service provider?

A. service provider as it owns the data
B. service receiver as it processes the data
C. both service provider and service receiver
D. service receiver as it violated the contract

Answer: A. service provider as it owns the data
Explanation: Service receiver retains the responsibility for ensuring compliance with regulatory requirements. Service receiver is the deemed to be owner of the data and responsible for the safe

custody of the data. If the service provider fails to safeguard the data, authority will generally hold the organization responsible for non-compliance and take appropriate action including penalties.

(6) Most effective method to mitigate the risk associated with outsourcing function is:

A. conducting audit to verify compliance with contractual requirements
B. conducting annual awareness training to staffs of service provider
C. conducting financial due diligence of service provider
D. obtaining compliance certificate from service provider

Answer: A. conducting audit to verify compliance with contractual requirements
Explanation: Periodic audit is the most effective method to ensure that service provider is complying with the security requirements of the service receiver.

(7) Application has been developed by a third party service provider. Most effective method to ensure that no back door codes are implemented is:

A. by monitoring the network traffic
B. by conducting penetration testing
C. by conducting internal audit
D. by conducting security code review for entire application

Answer: D. by conducting security code review for entire application
Explanation: Best security measure when a third party is engaged in application development is to conduct a security code review for the entire application to detect all the malware including back doors.

(8) When a hardware is not certified by a manufacturer or a vendor, it represents:

A. low risk
B. unknown risk
C. no risk
D. high risk

Answer: B. unknown risk
Explanation: When a hardware is not certified by a manufacturer or a vendor, it represents the unknown risk.

3.10.2 Data and Database Management

Data Input Validation

Risk practitioners should ensure that appropriate protection is available for confidentiality, integrity and availability of the data. Protection should be ensured during input, processing and output stages. Validation check should be built in during the data input stage so that only permitted data gets inputted in the system. To ensure that input data do not contain embedded commands or other content that might adversely affect automated processing systems, such as structured query language (SQL) code. Input validation includes:

- Range check to allow only predefined range of data value
- Format check to allow only specified data format
- Special character check to prevent script commands

- Size check to prevent buffer overflows [too many data] or incomplete data [not enough data])
- Likelihood and reasonableness check to prevent unlikely data

Whitelisting & Blacklisting

Validation can be built either whitelisting or blacklisting of data. In the whitelist approach, only specific data is allowed and rest others are prevented. In the blacklist approach, except for blacklisted data, everything is allowed. Whitelisting is more preferable when data is static or infrequently changing values. It is advisable to use a common library for whitelisting as it ensures a consistent approach though the organization with multiple applications.

Blacklisting is more preferable when the range of input data values is much broader and only few known data elements are to be restricted.

Data Authorization

Risk practitioners should ensure that there is adequate control over user authorization and authentication for access to sensitive data. Access to be granted on the basis of need to know basis only and principle of least privilege is followed. Authorization from the data owner should be mandatory to provide access to the users.

Periodic User Access Review

User access review should be conducted at frequent intervals and there should be a defined process of immediate deactivation of access for terminated or transferred employees.

Storage of Sensitive Data

Sensitive data should be stored in isolation i.e. on separate network and server by way network segmentation. Firewall should be installed to ensure role based access control.

Sensitive data should be encrypted during storage as well as transmission. Encapsulated data packets with authentication headers helps to safeguard the confidentiality against man-in-the-middle attack or interception of the data by other means. Encapsulation of the data packet helps to protect the data from unauthorised access in the network. Encapsulation is used to hide the values or state of a structured data by creating successive layers of control.

Data Encryption

Most effective method for protecting the data stored on a USB or a mobile device is to encrypt the data.

In case an organization plans to implement a data leak prevention (DLP), it is most important to first analyze the business case. Business case would help to determine the overall cost and benefit of the DLP solution and indicate feasibility of the solution.

Data Retention

Data should be retained in a hygienic condition as long as required by business or regulation requirements.

Database Security

Risk practitioners should ensure that appropriate safeguards are available for database security. Following are some of the important requirements:

- Sensitive data in the database should be encrypted
- Restricted access rights for the user
- Communication protocols for the database should be secured
- Administrator access should be restricted and monitored
- Effective and efficient database index for quick retrieval
- Database backup
- Referential integrity
- Input validation
- Effective data schema designs

Data Redundancy and Data Normalization

Data redundancy arises when the same data is stored at different places in a database. This causes problems in data updation or data deletion or data modification or otherwise managing the data.

Data normalization is the process of reducing redundant data and thereby making databases more structured. Data normalization reduces the risk of redundancy.

Acceptable Usage Policy (AUP)

Employees and contract staff should be made aware of acceptable usage policy. Written acknowledgement should be obtained from them with respect to adherence to AUP. If users are allowed to use their personal device, organizations should have approved BYOD policy. BYOD can be effective only if users are aware about the acceptable and unacceptable practices related to BYOD. Proper training of the users is of utmost important.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answer
What is the most effective method for protecting the data stored on a USB?	To encrypt the data
What is the most effective method for protecting the data stored in a mobile device?	To encrypt the data
Who should provide authorization for access to the data?	Data owner
What is the most important requirement before implementing a DLP solution?	To analyze business case and consider cost and benefit of the DLP solution
What is the best method to protect the confidentiality of data being transmitted over a network?	● Encapsulating the data packets ● Encryption
On what basis data retention period is defined?	Business or regulation requirements
BYOD policy can be effective only if	User are aware about acceptable and unacceptable practices

Data normalization process addresses the risk of	Data redundancy
Process to determine whether unauthorized modifications were made to production programs	Compliance testing helps to verify that the change management process is being followed and there are no unauthorized changes

Self-Assessment Questions

(1) Risk practitioners observed that a new printer stores all the printing data in its hard disk. Risk practitioner should:

A. recommend for security assessment for new equipment;
B. recommend to configure printers to automatically wipe all the data on disks after each print job;
C. recommend to replace the printer with another one which do not have built in hard disk drive;
D. recommend to wipe out the data when decommissioning the printer;

Answer: A. recommend for security assessment for new equipment
Explanation: First step is to conduct the security assessment for the newly installed printer. Security assessment will help to identify and evaluate various inherent risks of the new printer. Once all the risks are identified, appropriate controls can be placed.

(2) Most effective method to prevent the data leakage is:

A. acceptable usage policies
B. backup policies
C. incident management policy
D. database integrity check

Answer: A. acceptable usage policies
Explanation: Acceptable usage policies define the best practices with respect to usage of information assets. Adherence to AUP, helps to protect the information assets. Other options do not directly support in preventing the data leakage.

(3) Most effective method to protect the data on a USB drive is:

A. creating employee awareness
B. read only data in USB device
C. encrypting the USB device
D. restricted use of USB device

Answer: C. encrypting the USB device
Explanation: Encryption provides the most effective protection of data on mobile devices. Encryption converts the data in the USB in an unreadable form. It can be read only by the person possessing the encryption key. Other options are good control but they are not as effective as encryption of the USB device.

(4) Most effective method to protect the data on a mobile computing device is:

A. to conduct data integrity check
B. to encrypt the data stored in the mobile
C. to enable screen saver for device
D. to enable biometric access control

Answer: B. to encrypt the data stored in the mobile
Explanation: Encryption provides the most effective protection of data on mobile devices. Encryption converts the data in an unreadable form. It can be read only by the person possessing the encryption key. Other options are good control but they are not as effective as encryption of the data.

(5) Access to the database should be formally approved by:

A. database administrator
B. risk practitioner
C. data owner
D. data custodian

Answer: C. data owner
Explanation: Risk practitioners should ensure that there is adequate control over user authorization and authentication for access of sensitive data. Access to be granted on the basis of need to know basis only and principle of least privilege is followed. Authorization from the data owner should be mandatory to provide access to the users.

(6) Most important requirement for incorporating a DLP is:

A. benchmarking DLP with peers
B. evaluating various alternative DLP solutions
C. updating DLP solution in risk register
D.A business case for DLP to protect the data

Answer: D.A business case for DLP to protect the data
Explanation: In case an organization plans to implement a data leak prevention (DLP), it is recommended to analyze the business case which details the cost and benefit of the solution. If a business case indicates the feasibility of the solution, then other options to be further evaluated.

(7) Data transmitted on a network can be best protected by:

A. encapsulation of data packets with authentication header
B. applying hash to all messages sent on network
C. hardening of all network devices
D. use of fibre optic cables for networking

Answer: A. encapsulation of data packets with authentication header
Explanation: Encapsulation of the data packet helps to protect the data from unauthorised access in the network. Encapsulation is used to hide the values or state of a structured data by creating successive layers of control.

(8) Most important factor for developing a record retention policy is:

A. data storage capability
B. data storage budget
C. business and regulatory requirement
D. frequency and mode of storage

Answer: C. business and regulatory requirement
Explanation: Data should be retained in a hygienic condition as long as required by business or regulation requirements.

(9) Most important approach for making the BYOD policy effective is:

A. policy is user friendly
B. users are trained on best practices for BYOD usage
C. policy is made available on intranet
D. only approved devices are allowed for BYOD usage

Answer: B. users are trained on best practices for BYOD usage
Explanation: Most effective method to ensure that users comply with BYOD policies and procedures is educating the users on acceptable and unacceptable practices. Other options are not as effective as user training.

(10) A risk practitioner is reviewing the record retention policy. Most important factor to consider is:

A. business requirement
B. international standard
C. storage availability
D. industry benchmarking

Answer: A. business requirement
Explanation: Data should be retained in a hygienic condition as long as required by business or regulation requirements.

(11) When a database normalization is disabled, which of the following is the major risk?

A. confidentiality Risk
B. availability risk
C. redundancy risk
D. access risk

Answer: C. redundancy risk
Explanation: Normalization is a process of reducing duplicate data and thus reducing data redundancy. Redundancy is considered as negative in the database environment as it requires more effort and storage for handling the data. Denormalizing increases the data redundancy.

3.10.3 Segregation of Duties, Cross training and Job Rotation

Segregation of duties is the process of assigning responsibility for different functions of a job to separate individuals so as to prevent or detect the irregularities and fraud. For example, for entering a transaction one employee initiates the transaction and the other person records the transaction i.e. a single person cannot execute a complete transaction.

SoD also includes two people to participate in a task simultaneously which is also known as dual control. Though SoD does not guarantee security as both the employee may collude to commit the fraud or or other irregularities.

Addressing violation of segregation of duties

Implementing a role based access is a preventive method to address the risk of violation of segregation of duties. When an employee has restricted access, he will not be able to perform any job which is not assigned to him.

SoD is a best way to ensure that developers do not make any unauthorized changes in the production environment. He should not have access to the production environment.

Compensating control in absence of segregation of duties

In small organizations, it may not be feasible to segregate each function. In such cases appropriate compensating controls like audit and log reviews should be enabled.

Cross-training and Job Rotation

Many organizations have the process of cross training in which people on the same team are trained in one another's roles. However, one risk with cross training is that a single employee can bypass the control if he is aware of all the related processes.

Job rotation and mandatory vacation plays a dual role of improving employee's productivity as well as helps to detect fraud or other irregularities.

Mandatory job rotation also reduces the risk of collusion between two employees as two employees will not be allowed to work together over an extended period of time.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
How to address the risk of violation of segregation of duties?	To implement a role based access
Best way to ensure that developer do not make any unauthorized changes in production environment	● Segregation of duties between developer and production staff. ● Developers should not have access to the production environment.
What should be compensating control in case segregation of duties cannot be implemented?	● Review of logs ● Audit
Risk of collusion between two employees can be addressed by	Mandatory job rotation

Self-Assessment Questions

(1) Most effective method to prevent violation of segregation of duties is:

A. capturing transaction logs
B. implementing two factor authentication
C. implementing role based access
D. monitoring access logs

Answer: C. implementing role based access
Explanation: Implementing a role based access is a preventive method to address the risk of violation of segregation of duties. When an employee has restricted access, he will not be able to perform any job which is not assigned to him.

(2) Best way to ensure that developers should not have access to production environment is:

A. implementation of segregation of duties between developer and operation staffs
B. restricting the access of executable code by developer
C. implementing change management process for all changes other than emergency changes
D. implementing system development life cycle (SDLC)

Answer: A. implementation of segregation of duties between developer and operation staffs
Explanation: Implementing a role based access is a preventive method to address the risk of violation of segregation of duties. When an employee has restricted access, he will not be able to perform any job which is not assigned to him. SoD is a best way to ensure that developers do not make any unauthorized changes in the production environment. He should not have access to the production environment.

(3) A small organization cannot afford segregation of duties due to resource constraint. Best compensating control in lieu of segregation of duties is:

A. capturing and review of logs
B. user awareness training
C. authentication based access
D. review of user access rights

Answer: A. capturing and review of logs
Explanation: In small organizations, it may not be feasible to segregate each function. In such cases appropriate compensating controls like audit and log reviews should be enabled.

(4) Most effective method to prevent the risk of collusion is:

A. discretionary access control
B. mandatory access control
C. mandatory job rotation
D. need to know access

Answer: C. mandatory job rotation
Explanation: Mandatory job rotation also reduces the risk of collusion between two employees as two employees will not be allowed to work together over an extended period of time.

3.10.4 Business Continuity Plan and Business Impact Analysis

Following are the important aspect from a BCP and BIA perspective:

Objectives of Business Impact Analysis

Following are the primary objective of business impact analysis:

- To determine the critical processes of the organization that should be prioritized for effective prevention or response.
- To determine the impact of disruption on the organization over a period of time.
- To raise the awareness amongst the employees with respect to business continuity requirements of the organization.

Relationship between BCP and Risk Assessment

- Business continuity and disaster recovery process should be aligned with risk assessment of the organization. Any change in the risk environment should also be considered to determine the effect of change on a business continuity plan.
- Business Impact assessment (BIA) can be a common tool utilized by the BCP team as well as the risk assessment team.

Involvement of Stakeholders in BCP

Success of a business continuity plan depends upon the involvement of respective business owners and collaborative development and updation of the plan. BCP should be written and updated by representatives of all the functional units.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
What is the primary objective of Business Impact Analysis?	● To determine the impact of disruption to the organization over a period of time. ● To determine the critical processes of the organization that should be prioritized for effective prevention or response.
BCP should be written and updated by	Representative of all the functional units

Self-Assessment Questions

(1) Most important advantage of Business Impact Analysis (BIA) is:

A. that it does not require to be updated
B. that it promotes continuity awareness in the organization
C. that it replaces the risk assessment process
D. that is does not require support from business process owner

Answer: B. that it promotes continuity awareness in the organization
Explanation: Main objective of the BIA is to determine the critical processes of the organization that should be prioritized for effective prevention or response. BIA is useful in raising the awareness with respect to business continuity requirements of the organization.

(2) Business Impact Analysis (BIA) is primary used for:

A. estimating the budget for normal resumption of service after a disruption
B. evaluating the impact of a disruption on the organization's ability to operate over a period of time
C. conducting risk assessment
D. evaluating the preparedness of business continuity team

Answer: B. evaluating the impact of to an organization's ability to operate over time a disruption
Explanation: Main objective of the BIA is to determine the critical processes of the organization that should be prioritized for effective prevention or response. Business Impact Analysis (BIA) is primarily used to determine and evaluate the impact of a disruption on the organization's ability to operate over a period of time.

(3) Most important department to be involved in preparation and maintenance of Business Impact Analysis (BIA) is:

A. information security function
B. risk management function
C. representative from all relevant function
D. senior management

Answer: C. representative from all relevant function
Explanation: Success of a business continuity plan depends upon the involvement of respective business owners and collaborative development and updation of the plan. BCP should be written and updated by representatives of all the functional units.

(4) Most important aspect of a business continuity management is:

A. to ensure appropriate back up arrangement
B. to determine the budget for business disruption
C. to prioritize the applications on the basis of criticality
D. to replace the risk assessment

Answer: C. to prioritize the applications on the basis of criticality
Explanation: Most important aspect of a business continuity management is to prioritize the applications on the basis of criticality.

(5) In a business continuity management, processes are prioritized for recovery on the basis of:

A. business impact analysis
B. threat analysis
C. vulnerability analysis
D. risk assessment

Answer: A. business impact analysis
Explanation: Business Impact analysis is used to determine the criticality of the processes and assets that is to be prioritized for recovery during a disruption.

3.10.5 Security Architecture

It is important for a risk practitioner to evaluate the system architecture in terms of appropriateness of controls and other forms of risk response. System architecture should be robust enough to provide assurance against malicious activity.

Security architecture provides overview and relationship between systems and hence it is very useful in complex security deployment.

Primary purpose for developing a security architecture is to align the security strategy between the functional areas of the organization and external parties.

Platforms and Operating Systems

- Organizations should purchase the IT equipment from trusted vendors to avoid the risk of infected devices. Also, new devices should be tested thoroughly before implementation. This helps to address the risk of hardware infected with back doors and security vulnerabilities during the manufacturing or delivery process.

- If a hardware is not certified by the vendor or the manufacturer, there remains an unknown risk.
- Vendors provided default accounts and passwords should be disabled or changed.
- Strong authentication is required for privilege accounts such as administration.
- Organization should ensure use of licensed operating software and regular updation of patch and configuration.
- Operating software should be hardened to disable all the unused services.

Patch Management

Patch management policy should be available. Patch should be tested before deployment. In exceptional cases, pre-testing of patches may not be feasible due to business emergency, in such cases organization should have a rollback plan to roll back the patches from the system in case of adverse impact of patch deployment.

Applications

- Adoption of secure coding practices is necessary to address the flaws or bugs in the coding of the application.
- Application should have proper design, coding and testing to address the vulnerabilities.
- Organizations should study the common vulnerabilities published by the Open Web Application Security Project (www.owasp.org) and should address these vulnerabilities.
- Applications can be made secured by adopting following practices:
    - Sensitive data should be masked
    - Restricted access for the users
    - Input controls such as range checks, reasonableness checks etc.
    - Reconciliation and balancing for proper processing of transaction
    - Use of digital certificates for authentication
    - Encryption of stored as well as in transit data
    - Secure coding practices
    - Use of middleware to isolate direct access and manage data input/output
    - Network isolation and secure communications channels
- Absence of validation checks for data input fields is a major vulnerability. It provides an opportunity for attackers to exploit the system by way of SQL injection attack. Attackers can submit a part of a structured query language statement to gain access to the application and database. They can deface or even disable the web applications.
- Organization to evaluate the risk associated with legacy systems and should be controlled by use of middleware, network isolation and secure communication channels.
- Error messages should not be displayed in such a way that they might provide information to an attacker that can be used to modify the attack. Error messages should have different code that can be understood by the IT department only for rectification.
- Use of multiple factors of authentication for critical systems such as biometric access and a password.

- User accounts should be automatically locked out after a number of failed login attempts.
- When an application is developed from a third party, it is always recommended to conduct a security code review for the entire application to detect all the malware including back doors.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answer
Most important aspect before installing new equipment	Conduct risk assessment of new equipment
Most useful in managing complex security deployments	Security Architecture
Primary purpose for developing a security architecture	To align the security strategy between the functional areas of the organization and external parties
What is the most important aspect prior to releasing a patch into production?	Testing of the patch
What is the best method to minimize the risk of interoperability issues of untested patch deployment?	Organization should have a rollback plan to roll back the patches from the system in case of adverse impact of patch deployment.
What is the risk if validation checks are missing for data input fields?	Absence of validation checks for data input fields is a major vulnerability. It provides an opportunity for attackers to exploit the system by way of SQL injection attack. Attackers can submit a part of a structured query language statement to gain access to the application and database. They can deface or even disable the web applications

.

Self-Assessment Questions

(1) Most important element to manage the complex security deployments is:

A. support from management
B. industry recognized process and standards
C. development of policy
D. security architecture

Answer: D. security architecture
Explanation: It is important for a risk practitioner to evaluate the security architecture in terms of appropriateness of controls and other forms of risk response. Security architecture provides overview and relationship between systems and hence it is very useful in complex security deployment.

(2) Risk practitioners noted that in a BYOD environment employees are simultaneously operating business applications as well as their social media accounts. Best course of action will be:

A. to implement a virtualized desktop on each mobile device
B. to develop BYOD usage policy
C. to create user awareness
D. to restrict the social media accounts inside the DMZ area

Answer: A. to implement a virtualized desktop on each mobile device
Explanation: Implementing a virtualized desktop provides better control in terms of data security. It will be difficult to copy or extract the data from virtualized desktop to personal device. Other options are not as effective as virtualized desktops.

(3) Primary objective of developing a security architecture is:

A. to align security strategies within all functional areas of the organization and external partners
B. to create a repository of all IT assets and resources
C. to protect the organization from external attacks
D. to determine the different technology implemented by the organization

Answer: A. to align security strategies within all functional areas of the organization and external partners
Explanation: Primary purpose for developing a security architecture is to align the security strategy between the functional areas of the organization and external parties.
Platforms and Operating Systems

(4) Most important aspect of a patch management is:

A. simultaneous application of patch in all the system
B. patch to be procured from recognized vendor
C. testing of patch before deployment
D. approval from management

Answer: C. testing of patch before deployment
Explanation: Most important aspect of a patch management is to test the patch before deployment. Other options are not as critical as testing of patches.

(5) Interoperability issues due to untested patch release can be best mitigated by:

A. testing the patch on sample systems
B. approval from security team
C. having reliable rollback plan
D. procuring patch from a recognized vendor

Answer: C. having reliable rollback plan
Explanation: Patch should be tested before deployment. In exceptional cases, pre-testing of patches may not be feasible due to business emergency, in such cases the organization should have a rollback plan to roll back the patches from the system in case of adverse impact of patch deployment.

(6) Which of the following vulnerabilities allows attackers access to data through a web application?

A. Validation checks are missing in data input fields.
B. Password history rule not implemented.
C. Application logs are not monitored at frequent intervals.
D. Two factor authentication not implemented.

Answer: (A)Validation checks are missing in data input fields.
Explanation. In absence of validation checks in data input fields, attackers are able to exploit other weaknesses in the system. For example, through SQL injection attacks, hackers can illegally retrieve application data. Other options may make applications vulnerable but these can be countered in other ways.

(7) Application has been developed by a third party service provider. Most effective method to ensure that no back door codes are implemented is:

A. by monitoring the network traffic
B. by conducting penetration testing
C. by conducting internal audit
D. by conducting security code review for entire application

Answer: D. by conducting security code review for entire application
Explanation: When an application is developed from a third party, it is always recommended to conduct a security code review for the entire application to detect all the malware including back doors. Other options are not as effective as security code review.

(8) When a hardware is not certified by a manufacturer or a vendor, it represents:

A. low risk
B. unknown risk
C. no risk
D. high risk

Answer: B. unknown risk
Explanation: Organization should purchase the IT equipment from trusted vendors to avoid the risk of infected devices. Also, new devices should be tested thoroughly before implementation. This helps to address the risk of hardware infected with back doors and security vulnerabilities during the manufacturing or delivery process. If a hardware is not certified by the vendor or the manufacturer, there remains an unknown risk.

3.10.6 Cryptography

Cryptography is defined as the art or science of secret writing with the use of techniques such as encryption. Encryption is the process of converting data into unreadable code so it cannot be accessed or read by unauthorized people. This unreadable data can again be converted into readable form by process of decryption. Different types of algorithms are available for encryption and decryption.

Symmetric Encryption vis a vis Asymmetric Encryption

Encryption can be of two types i.e. symmetric encryption and asymmetric encryption. The table below will help us to understand the difference between two terms.

Symmetric Encryption	Asymmetric Encryption

Single key is used to encrypt and decrypt the messages	Two keys are used. One for encryption and other for decryption.
Key is said to be symmetric because the encryption key is the same as the decryption key.	Message encrypted by private key can be decrypted only by corresponding public key
	Similarly, message encrypted by public key can be decrypted only by corresponding private key
Comparatively, faster computation and processing.	Comparatively, slower computation and processing.
Comparatively, symmetric encryption process is cheaper	Comparatively, a symmetric encryption process is costlier.
Major disadvantage of symmetric encryption is sharing of key with another party.	No such challenge is faced in asymmetric encryption as two separate keys are used.

Encryption Keys

In an asymmetric environment, total four keys are available with different functions. Following table indicates who possessed different keys:

Type of Key	Availability
Sender’s Private Key	Key is available only with the sender.
Sender’s Public Key	Key is available in the public domain. Public keys can be accessed by anyone.
Receiver’s Private Key	Key is available only with the receiver.
Receiver’s Public Key	Key is available in the public domain. Public keys can be accessed by anyone.

Use of keys for different objectives

Above Keys are used to achieve following objectives:

- Confidentiality
- Authentication & Non-repudiation

- Integrity

Confidentiality

In an asymmetric encryption, two keys are used. One for encryption and other for decryption. Messages encrypted by one key can be decrypted by another key. These two keys are known as private keys and public keys. Private key is available only with the owner of the key and a public key is available in the public domain.

Message can be encrypted by following means:

- Receiver’s public key
- Receiver’s private key
- Sender’s public key
- Sender’s private key

Receiver’s Public Key
If a message is encrypted by using the public key of the receiver, then only the receiver can decrypt the same as he is the only one having access to his private key. This will ensure message confidentiality as only the owner of a private key can read the message.

Receiver’s Private Key
Sender will not be in possession of the receiver's private key and hence this option is not feasible.

Sender’s Public Key
If a message is encrypted by using the public key of the sender, then it can be decrypted only by using the private key of the sender. Receiver will not be in possession of the sender's private key and hence this option is not feasible.

Sender’s Private Key
If a message is encrypted by using the private key of the sender, then anyone with a public key can encrypt the same. Public key is available in the public domain and hence anyone can encrypt the message. This will not ensure confidentiality of the message.

Hence message confidentiality, receiver’s public key is used to encrypt the message and receiver’s private key is used to decrypt the message.

Authentication

Authentication is ensured by verifying and validating some unique features of the sender. In normal course, we validate a document by verifying the signature of the sender. This signature is unique for everyone. Similarly, for digital transactions a private key is unique for each owner. Only the owner is in possession of his unique private key and no one else. Each private key has a corresponding public key. Third person can authenticate the identity of the owner with the use of a public key. When the objective is to authenticate the sender of the message, the sender's private key is used to encrypt the hash of the message. Receiver will try to decrypt the same with use of the sender's public key and if successfully decrypted, it indicates that the message is genuine and the sender is authenticated.

Hence for authentication of the message, sender’s private key is used to encrypt the message and sender’s public key is used to decrypt the message.

Non - Repudiation

Non-repudiation refers to a situation wherein the sender cannot take back his responsibility for the digital message or transaction. Non-repudiation establishes once the sender is authenticated. Hence for non-repudiation, the same concept of authentication will apply.

Hence for non-repudiation of the message, sender’s private key is used to encrypt the message and sender’s public key is used to decrypt the message.

Integrity

Integrity refers to correctness, completeness and accuracy of the message/data. To achieve objective of integrity following steps are followed:

- Sender will create a hash of the message.
- This hash is encrypted using the sender's private key.
- Message along with an encrypted hash is sent to the receiver.
- Receiver will do two things. First he will decrypt the hash value using the sender's private key and second he will again calculate the hash of the message received.
- Receiver will compare both the hash and if both hash values are the same, the message is considered as correct, complete and accurate.

Summary

Following table will help us to understand use of different keys to achieve each of above objective:

<table>
<tr><td>Objective</td><td>Use of Keys</td><td>What to encrypt</td></tr>
<tr><td>Confidentiality</td><td>receiver’s public key</td><td>full message</td></tr>
<tr><td>Authentication/Non-repudiation</td><td>sender’s private key</td><td>hash of the message</td></tr>
<tr><td>Integrity</td><td>sender’s private key</td><td>hash of the message</td></tr>
<tr><td rowspan="2">Confidentiality & authentication/non-repudiation</td><td colspan="2">For confidentiality – use of receiver’s public key to encrypt full message</td></tr>
<tr><td colspan="2">For authentication (non-repudiation) – use of sender’s private key to encrypt hash of the message</td></tr>
<tr><td rowspan="2">Confidentiality, Integrity & Authentication/non-repudiation</td><td colspan="2">For confidentiality – use of receiver’s public key to encrypt full message</td></tr>
<tr><td colspan="2">For integrity, authentication (non-repudiation) – use of sender’s private key to encrypt hash of the message</td></tr>
</table>

Hash of the Message

Some important features and functionality of hash value is as follow:

- Hash value is digital code of the message / content.
- It is arrived at by using a different algorithm.
- Hash value is also known as message digest.
- Hash value is unique for each message/content.
- A slight change in message/content will produce a different hash value.
- Hash value is used to ensure integrity of message/content.
- Hash value is used for creation of digital signature. Hash value when encrypted with the sender's private key, it becomes a digital signature. Digital signature is used to determine integrity of message and authentication of sender (i.e. non-repudiation)

Combining Symmetric and Asymmetric Methods

Most efficient use of PKI is to combine the best features of asymmetric as well as symmetric methods. Challenge of asymmetric encryption is an expensive and time consuming process. Though symmetric encryption is comparatively much faster, it possesses the challenge of sharing the symmetric key to other parties. To combine the benefit of both and address their challenges following process is recommended:

- Step 1: For faster and inexpensive computation, encrypt the entire message with the help of a symmetric key.
- Step 2: Encrypt the above symmetric key with the public key of receiver.
- Step 3: Send the encrypted message (step 1) and encrypted symmetric key (step 2) to the receiver.
- Step 4: Receiver will decrypt the symmetric key using his private key.
- Step 5: Receiver will use a symmetric key to decrypt the full message.

Thus when combined method is used:

- Use of symmetric key to encrypt full message
- Use of receiver's public key to encrypt the symmetric key

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
In asymmetric encryption, message confidentiality can be ensured by	Use of receiver's public key for encryption and use of receiver's private key for decryption
In asymmetric encryption, message authentication can be ensured by	Use of sender's private key to encrypt the message/hash and use of sender's public key to decrypt the message/hash
In asymmetric encryption, message non-repudiation can be ensured by	Use of sender's private key to encrypt the message/hash and use of sender's public

	key to decrypt the message/hash
In asymmetric encryption, message integrity can be ensured by	Use of sender’s private key to encrypt the hash and use of sender’s public key to decrypt the hash
Cost of cryptography increases by	Long asymmetric keys
How to combine symmetric and asymmetric methods for better results?	● Use of symmetric key to encrypt full message ● Use of receiver’s public key to encrypt the symmetric key

Self-Assessment Questions

(1) For asymmetric encryption, message confidentiality can be ensured by:

A. use of private key for encryption and use of public tor decryption
B. use of public key for encryption and use of private key for decryption
C. use of public key for encryption as well as decryption
D. use of private key for encryption as well as decryption

Answer: B. use of public key for encryption and use of private key for decryption
Explanation: In an asymmetric encryption, two keys are used. One for encryption and other for decryption. Messages encrypted by one key can be decrypted by another key. These two keys are known as private keys and public keys. Private key is available only with the owner of the key and a public key is available in the public domain. Let us evaluate each option:
A.use of private key for encryption and use of public tor decryption – if message is encrypted by the private key of the owner, anyone can decrypt the same using public key (as public key is easily available) and hence confidentiality of the message cannot be ensured.
B.use of public key for encryption and use of private key for decryption – if message is encrypted by using the public key, then only the person with private key can encrypt the same. This will ensure message confidentiality as only the owner of a private key can read the message.
Option C & D is not valid as in an asymmetric encryption two keys are required for encryption and decryption.

(2) In public key encryption, sender of the message is authenticated by:

A. use of receiver's private key to encrypt the hash of the message and use of receiver's public key to decrypt the same.
B. use of sender's public key to encrypt the hash of the message and use of sender's private key to decrypt the same.
C. use of sender's private key to encrypt the hash of the message and use of sender's public key to decrypt the same.
D. use of receiver’s public key to encrypt the hash of the message and use of receiver's private key to decrypt the same

Answer: C. use of sender's private key to encrypt the hash of the message and use of sender's public key to decrypt the same.

Explanation: Authentication is ensured by verifying and validating some unique features of the sender. In normal course, we validate a document by verifying the signature of the sender. This signature is unique for everyone. Similarly, for digital transactions a private key is unique for each owner. Only the owner is in possession of his unique private key and no one else. Each private key has a corresponding public key. Third person can authenticate the identity of the owner with the use of a public key. When the objective is to authenticate the sender of the message, the sender's private key is used to encrypt the hash of the message. Receiver will try to decrypt the same with use of the sender's public key and if successfully decrypted, it indicates that the message is genuine and the sender is authenticated.

(3) In public key encryption, content integrity of message is ensured by:

A. use of sender's private key to encrypt the hash of the message and use of sender's public key to decrypt the same.
B. use of sender's public key to encrypt the hash of the message and use of sender's private key to decrypt the same.
C. use of receiver's private key to encrypt the hash of the message and use of receiver's public key to decrypt the same.
D. use of receiver’s public key to encrypt the hash of the message and use of receiver's public key to decrypt the same

Answer: A. use of sender's private key to encrypt the hash of the message and use of sender's public key to decrypt the same.
Explanation: Hash value is unique code for a given message. Hash value is unique for each message. A slight change in message/content will produce a different hash value. Hash value is used to ensure integrity of message with details as follow:
Hash value to be encrypted using sender’s private key. Sender will send (i) messages and (ii) encrypted hash to the receiver.
On receiving the message, the receiver will (i) decrypt the received hash by using the public key of the sender and (ii) re-compute the hash of the message and if the two hashes are equal, then it proves that message integrity is not tampered with.

(4) In public key encryption how to ensure confidentiality of messages and also at the same time authenticate the sender of the message?

A. use of receiver's public key for encrypting hash of the message and thereafter use of sender's public key to encrypt the message
B. use of sender's private key for encrypting hash of the message and thereafter use of receiver’s private key to encrypt the message
C. use of receiver's public key for encrypting hash of the message and there after use of sender's private key to encrypt the message
D. use of sender's private key for encrypting hash of the message and there after use of receiver’s public key to encrypt the message

Answer: D. use of sender's private key for encrypting hash of the message and there after use of receiver’s public key to encrypt the message
Explanation: For Authentication, encrypt the hash of the message with the sender's private key. For confidentiality, encrypt the message with the receiver's public key.

(5) In public key encryption, message authenticity and confidentiality is best achieved by encrypting the message with use of:

A. receiver’s public key and use of sender's private key to encrypt hash of the message
B. receiver's private key and use of sender's public key to encrypt hash of the message
C. sender’s public key and use of receiver's private key to encrypt hash of the message
D. sender's private key and use of receiver’s public key to encrypt the hash of the message

Answer: A. receiver’s public key and use of sender's private key to encrypt hash of the message
Explanation: For confidentiality, encrypt the message with the receiver's public key. For Authentication, encrypt the hash of the message with the sender's private key.

(6) Which of the following provides assurance about email authenticity?

A. use of sender's public key to encrypt prehash code
B. use of sender's private key to encrypt prehash code
C. use of receiver's public key to encrypt prehash code
D. use of receiver's private key to encrypt prehash code

Answer: B. use of sender's private key to encrypt prehash code
Explanation: To provide assurance about email authenticity, the hash of the message should be encrypted with the sender's private key

(7) Use of sender's private key to encrypt message as well as message hash will ensure:

A. authenticity and privacy
B. confidentiality and integrity
C. authenticity and integrity
D. confidentiality and privacy

Answer: C. authenticity and integrity
Explanation: Use of sender’s private key to encrypt the message as well as message hash will ensure authenticity and integrity. It will not ensure confidentiality or privacy as anyone having a public key can decrypt the message.

(8) An organization sending invoices to clients through email wants to ensure the same has not been modified in transit. Which of the following will the organization achieve this objective?

A. use of the firm's private key to encrypt the hash of the invoice.
B. use of firm's public key to encrypt the hash of the invoice
C. use of client's private key to encrypt the hash of the invoice
D. use of client's private key to encrypt the invoice.

Answer: A. use of firm's private key to encrypt the hash of invoice
Explanation: Hash value is unique code for a given message. Hash value is unique for each message. A slight change in message/content will produce a different hash value. Firm can ensure integrity of invoice can implement following process:
Hash value of the invoice is to be encrypted using the sender's private key. Firm will send (i) invoice and (ii) encrypted hash of the invoice to the client.
On receiving the message, the client will (i) decrypt the received hash by using the public key of sender and (ii) re-compute the hash of the invoice and if the two hashes are equal, then it proves that message integrity is not tampered with.

(9) Organization uses public key infrastructure for its communication server where there is one private key for the server and associated public key is made available to the customer. This ensures:

A. customer's authenticity
B. website’s authenticity
C. non repudiation from customer
D. certifying authority's authenticity

Answer: B. website’s authenticity
Explanation: When a link is established between an organization's website and customer’s computer, the customer's computer validates the private key of the website with use of associated public key. This helps to determine the authenticity of the website.

(10) Cryptographic cost increases by:

A. applying long asymmetric key
B. applying symmetric encryption instead of asymmetric encryption
C. encryption of hash as compared to encryption of full message
D. applying short asymmetric key

Answer: A. applying long asymmetric key
Explanation: Cost of symmetric key (only one key is used) is lower as compared to asymmetric key (two keys are used). For encryption and decryption of long asymmetric keys more processing time and cost is required as compared to short asymmetric keys. A hash is shorter than the original message and hence expense will be lower for encrypting only hash.

(11) Efficient use of PKI is ensured by encrypting:

A. receiver’s private key
B. sender's private key
C. complete message
D. symmetric session key

Answer: D. symmetric session key
Explanation: Most efficient use of PKI is to combine the best features of asymmetric as well as symmetric methods. Challenge of asymmetric encryption is an expensive and time consuming process. Though symmetric encryption is comparatively much faster, it possesses the challenge of sharing the symmetric key to other parties. To combine the benefit of both and address their challenges following process is recommended:
Step 1: For faster and inexpensive computation, encrypt the entire message with the help of a symmetric key.
Step 2: Encrypt the above symmetric key with the public key of receiver.
Step 3: Send the encrypted message (step 1) and encrypted symmetric key (step 2) to the receiver.
Step 4: Receiver will decrypt the symmetric key using his private key.
Step 5: Receiver will use a symmetric key to decrypt the full message.

(12) Which of the following is the most effective process to ensure message integrity, confidentiality and non-repudiation?

A. use of sender’s private key to encrypt message digest, use of symmetric key to encrypt the message, use receiver's public key to encrypt the symmetric key
B. use of sender's private key to encrypt message digest, use of symmetric key to encrypt the message, use of receiver’s private key to encrypt the symmetric key
C. use of sender's private key to encrypt message digest, use of symmetric key to encrypt the message, use of sender's private key to encrypt the symmetric key

D. use of sender's private key to encrypt message digest, use of symmetric key to encrypt the message, use of sender's public key to encrypt the symmetric Key

Answer: A. use of sender's private key to encrypt message digest, use of symmetric key to encrypt the message, use receiver's public key to encrypt the symmetric key
Explanation:Integrity & Non-repudiation: sender's private key is used to encrypt the hash/message digest
Confidentiality: Most efficient use of PKI is to combine the best features of asymmetric as well as symmetric methods. Challenge of asymmetric encryption is an expensive and time consuming process. Though symmetric encryption is comparatively much faster, it possesses the challenge of sharing the symmetric key to other parties. To combine the benefit of both and address their challenges following process is recommended:
Step 1: For faster and inexpensive computation, encrypt the entire message with the help of a symmetric key.
Step 2: Encrypt the above symmetric key with the public key of receiver.
Step 3: Send the encrypted message (step 1) and encrypted symmetric key (step 2) to the receiver.
Step 4: Receiver will decrypt the symmetric key using his private key.
Step 5: Receiver will use a symmetric key to decrypt the full message.
Thus for confidentiality use of symmetric key to encrypt the message, use receiver's public key to encrypt the symmetric key.

3.10.7 Elements of Public Key Infrastructure

A public key infrastructure is a set of rules and procedures for creation, management, distribution, storage and use of digital certificate and public key encryption.

PKI Terminologies

CRISC aspirants should have basic understanding of following terms with respect to public key infrastructure

Digital Certificate: Digital certificate is an electronic document used to prove the ownership of a public key. Digital certificate includes information about the key, owner of the key and digital signature of the issuer of the digital certificate. It is also known as a public key certificate.

Certifying Authority (CA): A certification authority is an entity that issues digital certificates.

Registration Authority (RA): A registration authority is an entity that verifies user requests for digital signatures and recommends the certificate authority to issue it.

Certificate Revocation list (CRL): CRL is a list of digital certificates which have been revoked and terminated by certificate authority before their expiry date and these certificates should no longer be trusted.

Certification Practice Statement (CPS): A certification practice statement is a document which prescribes practice and process of issuing and managing digital certificates by certifying authority. It includes details like controls in place, method for validating applicants and usage of certificates.

Public Key Infrastructure: Public key infrastructure is a set of roles, policies and procedures for issuance, maintenance and revocation of public key certificates.

Process involved in PKI

Issuance of public key involves following process:

Step 1: Applicant applies for issuance of digital certificate to certifying Authority (CA).

Step 2: Certifying Authority (LA) delegates the verification process to Registration Authority (RA).

Step 3: Registration Authority (RA) verifies the correctness of information provided by the applicant.

Step 4: If information is correct, RA recommends CA for issuance of certificate

Step 5: Certifying Authority (LA) issues the certificate and manages the same through its life cycle. CA also maintains details of certificates that have been terminated or revoked before its expiry date. This list is known as certificate revocation list (CRL). CA also maintains a document called as Certification Practice Statement (CPS) containing standard operating procedure (SOP) for issuance and management of certificates.

Certifying Authority (CA) vis a vis Registration Authority(RA)

Following table provides differentiation between CA and RA:

Certification Authority	Registration Authority
CA is responsible for issuance and management of digital certificates	RA is being delegated with the function of verifying the correctness of information provided by applicants.
CA delegates some of the administrative functions such as verification of information provided by applicants.	After authentication of information, RA recommends CA for issuance of certificate
CA authenticates and validates the holder of certificate after issuance of certificate.	RA authenticates information of the applicant before issuance of certificate.

Functions of Registration Authority

A registration authority has following functions:

- To verify and validate information provided by the applicant.
- To verify that the applicant is in possession of a private key and that it matches with the public key requested for a certificate. This is known as proof of possession (POP).
- To distribute physical tokens containing private keys.
- To generate shared secret keys during initialization and certificate pick up phase of registration.

Key aspects from CISA exam perspective

Below table covers important aspect from CISA exam perspective:

CRISC Questions	Possible Answers
Authority that manages life cycle of digital certificate	Certifying Authority
Functions of Registration Authority	● To verify and validate information provided by the applicant. ● To verify that the applicant is in possession of a private key and that it matches with the public key requested for a certificate. This is known as proof of possession (POP). ● To distribute physical tokens containing private keys. ● To generate shared secret keys during initialization and certificate pick up phase of registration
Procedural aspect for dealing with a compromised private key is prescribed in	Certification Practice Statement

Self - Assessment Questions

(1) Which of the following functions manages the life cycle of a digital certificate?

A. Registration Authority (RA)
B. Certifying Authority (CA)
C. Public key authority
D. Private key authority

Answer: B. Certifying Authority (CA)
Explanation: A certification authority is an entity that issues digital certificates. CA is responsible for issuance and management of digital certificates

(2) Which of the following is the function of the Registration Authority (RA)?

A. to issue the digital certificate
B. to manage certificate throughout its life cycle
C. to document and maintain certificate practice statements
D. to validate the information of the applicants for certificate

Answer: D. to validate the information of the applicants for certificate
Explanation: A registration authority has following functions:

- To verify and validate information provided by the applicant.

- To verify that the applicant is in possession of a private key and that it matches with the public key requested for a certificate. This is known as proof of possession (POP).
- To distribute physical tokens containing private keys.
- To generate shared secret keys during initialization and certificate pick up phase of registration.

(3) Which of the following authorities manages the life cycle of a digital certificate to ensure the existence of security in digital signature?

A Certifying Authority (CA)
B. Registration Authority (RA)
C. Certification practice statement
D. Public key Authority

Answer: A Certifying Authority (CA)
Explanation: A certification authority is an entity that issues digital certificates. CA is responsible for issuance and management of digital certificates

(4) A certificate authority can delegate the process of:

A. certificate issuance
B. certificate life cycle management
C. establishing link between applicant and its public key
D. maintenance of certificate revocation list

Answer: C. establishing link between applicant and its public key
Explanation: CA delegates some of the administrative functions such as verification of information provided by applicants. RA is being delegated with the function of verifying the correctness of information provided by applicants. RA verifies that applicant is in possession of a private key and that it matches with the public key requested for the certificate. This is known as proof of possession (POP).

(5) Following is considered as weakness in a public key infrastructure process:

A. centralized location of certificate authority
B. transaction can be executed from any device.
C. user organization is also the owner of certificate authority
D. availability of multiple data center to manage the certificate

Answer: C. user organization is also the owner of certificate authority
Explanation: This indicates that there is conflict of interest as the user and owner of the certificate are the same. Independence of the certifying authority will be impaired in this scenario and this is considered a major weakness.

(6) Which of the following is the function of registration authority?

A. issuance of certificate
B. validation of information provided by applicant
C. to sign the certificate to achieve authentication and non-repudiation
D. to maintain certificate revocation list

Answer: B. validation of information provided by applicant
Explanation: A registration authority has following functions:

- To verify and validate information provided by the applicant.

- To verify that the applicant is in possession of a private key and that it matches with the public key requested for a certificate. This is known as proof of possession (POP).
- To distribute physical tokens containing private keys.
- To generate shared secret keys during initialization and certificate pick up phase of registration.

(7) Procedural aspect for dealing with a compromised private key is prescribed in:

A. certificate practice statement
B. certificate revocation list
C. certificate disclosure statement
D applicant disclosure form

Answer: A. certificate practice statement
Explanation: A certification practice statement is a document which prescribes practice and process of issuing and managing digital certificates by certifying authority. It includes details like controls in place, method for validating applicants and usage of certificates.

(8) Which of the following is a function of a certifying authority?

A. to ensure availability of a secured communication network based on certificates.
B. to validate the identity and authenticity of certificate owner
C. to ensure that both communicating parties are digitally certified
D. to host private keys of subscribers in public domain

Answer: B. to validate the identity and authenticity of certificate owner
Explanation: A registration authority has following functions:

- To verify and validate information provided by the applicant.
- To verify that the applicant is in possession of a private key and that it matches with the public key requested for a certificate. This is known as proof of possession (POP).
- To distribute physical tokens containing private keys.
- To generate shared secret keys during initialization and certificate pick up phase of registration.

3.10.8 Digital Signature

Digital Signature is a process wherein a digital code is attached to an electronically transmitted document to verify its contents and the sender's identity.

Steps for creating digital signature

Digital Signature is created in below two steps:

Step 1: Create Hash (Message digest) of the message.

Step 2: Encrypt the hash (as derived above) with the private key of the sender.

Steps description	Step Results
Step 1: Creating hash value (message digest) of given message.	4526dee03a36204cbb9887b3528fac4e
Step 2: Encryption of above hash (message digest)	4xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxe

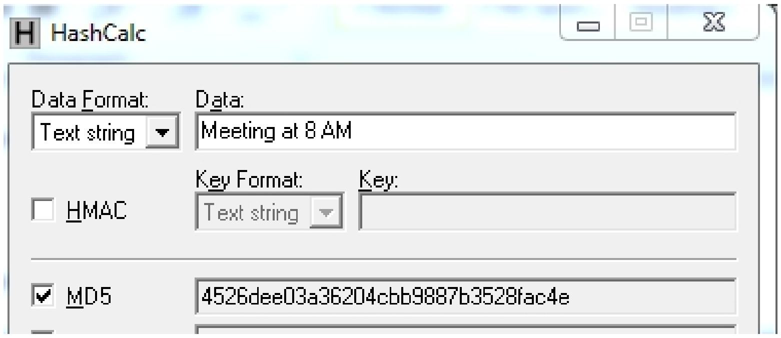
Digital Signature

What is hash or messages digest?

A hash function is a mathematical algorithm which gives a unique fixed string for any given message. It must be noted that the hash value will be unique for each message.

Message	Hash Value
Meeting at 8 AM	4526dee03a36204cbb9887b3528fac4e
Meeting at 8 PM	10ca8c76ec6b2b34a9a06505da298ed8

Software showing hash value of the message "Meeting at 8 AM"



Data Format: Text string

Data: Meeting at 8 AM

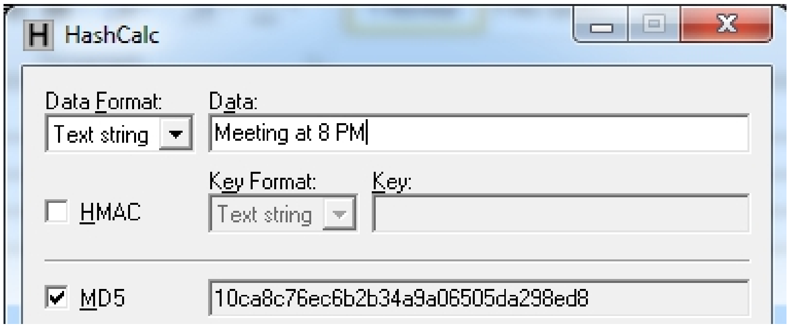
☐ HMAC

Key Format: Text string

Key:

☑ MD5 4526dee03a36204cbb9887b3528fac4e

Software showing hash value of the message "Meeting at 8 PM"



Data Format: Text string

Data: Meeting at 8 PM

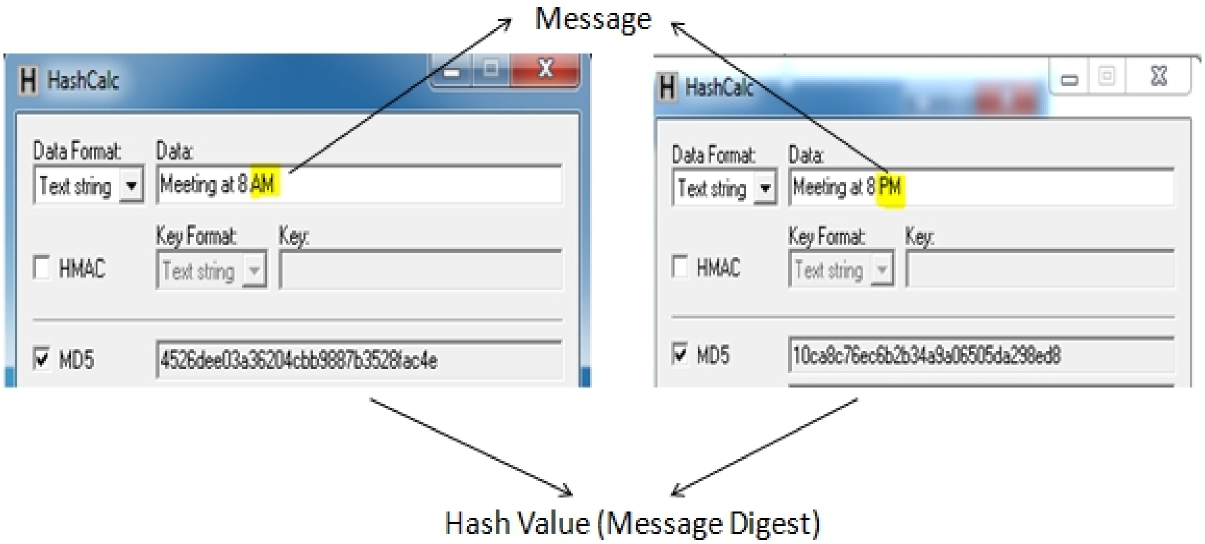
☐ HMAC

Key Format: Text string

Key:

☑ MD5 10ca8c76ec6b2b34a9a06505da298ed8

Hash value of the first message is for 8 AM and second is for 8 PM. If you note above, hash value has changed even if there is change in one alphabet.



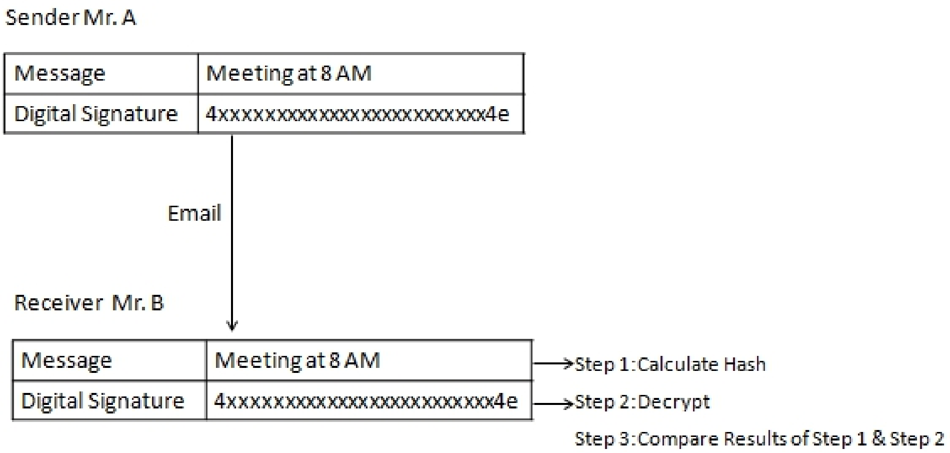
Data Format: Text string
Data: Meeting at 8 AM
☐ HMAC
Key Format: Text string
Key:
☑ MD5 4526dee03a36204cbb9887b3528fac4e

Data Format: Text string
Data: Meeting at 8 PM
☐ HMAC
Key Format: Text string
Key:
☑ MD5 10ca8c76ec6b2b34a9a06505da298ed8

Hash Value changes even with slightest change in message

Thus it helps in validating integrity of the message

Let us understand how message flows from sender A to recipient B:



Sender Mr. A

Message	Meeting at 8 AM
Digital Signature	4xxxxxxxxxxxxxxxxxxxxxxxxxx4e

Email

Receiver Mr. B

Message	Meeting at 8 AM
Digital Signature	4xxxxxxxxxxxxxxxxxxxxxxxxxx4e

Step 1:Calculate Hash
Step 2:Decrypt
Step 3:Compare Results of Step 1 & Step 2

Receiver Mr. will perform following steps:

(i)He will independently calculate the hash value of the message “Meeting at 8 AM”. Hash value comes to 4526dee03a36204cbb9887b3528fac4e.

(ii)Then he will decrypt the digital signature i.e. 4xxxxxxxxxxxxxxxxxxxxxxxxx4e using the public key of sender Mr. A. (This proves authentication and non-repudiation).

(iii)Now, he will compare the value derived under step (i) with the value derived under step (ii) If both tallies, it proves the integrity of the message.

Thus, Digital Signature ensures:

(1)Integrity (i.e. message has not been tampered)

(2)Authentication (i.e. message has been actually sent by sender)

(3)Non-repudiation (i.e. sender cannot later deny about sending the message)

But, digital signature does not provide:

× **Confidentiality**

It must be noted that digital signature does not provide confidentiality of the message.

Key aspects from CRISC exam perspective:

- In any given scenario, digital signature provide assurance with respect to integrity of the message (i.e. message is not altered), authentication of message (i.e. message is in fact sent by sender) and non-repudiation (i.e. sender cannot deny having sent the message in court of law).
- In any given scenario, digital signature encrypts the hash of the message (and not the message). Hence digital signature does not provide confidentiality or privacy.
- In any given scenario, for encryption of the hash of the message, the private key of the sender is to be used.
- In any given scenario, non-repudiation provides the strongest evidence that a specific transaction/action has occurred. No one can deny the transaction/action.

Self - Assessment Questions

(1)Hash function will address which of the concerns about electronic message:

A. Message confidentiality
B. Message integrity
C. Message availability.
D. Message compression

Answer: B. Message integrity
Explanation: Digital signature provides integrity, authentication and non-repudiation for electronic messages. It does not ensure message confidentiality. A digital signature includes an encrypted hash total of the message. This hash would no longer be accurate if the message was subsequently altered, thus indicating that the alteration had occurred. Hence, it helps to ensure message integrity. Digital signatures will not identify or prevent any of the other options.

(2) Digital signature will address which of the concerns about electronic message:

A. Authentication and integrity of data
B. Authentication and confidentiality of data
C. Confidentiality and integrity of data
D. Authentication and availability of data

Answer: A. Authentication and integrity of data
Explanation: Digital signature provides integrity, authentication and non-repudiation for electronic messages. It does not ensure message confidentiality or availability of data. Digital Signature is created in below two steps:
Step 1: Create Hash (Message digest) of the message.
Step 2: Encrypt the hash (as derived above) with the private key of the sender.

(3) A digital signature is created by the sender to prove message integrity by :

A. encrypting the message with the sender's private key. Upon receiving the data, the recipient can decrypt the data using the sender's public key.
B. encrypting the message with the recipient's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's public key.
C. initially using a hashing algorithm to produce a hash value or message digest from the entire message contents. Upon receiving the data, the recipient can independently create it.
D.encrypting the message with the sender's public key. Upon receiving the data, the recipient can decrypt the data using the recipient's private key.

Answer: C. initially using a hashing algorithm to produce a hash value or message digest from the entire message contents. Upon receiving the data, the recipient can independently create it.
Explanation: Digital Signature is created in below two steps:
Step 1: Create Hash (Message digest) of the message.
Step 2: Encrypt the hash (as derived above) with the private key of the sender.
Upon receiving the message, recipient will perform following functions:
Step 1: He will independently calculate the hash value of the message.
Step 2: Then he will decrypt the digital signature using the public key of the sender.
Step 3: Now, the recipient will compare the value derived under step (1) with the value derived under step (2). If both tallies, it proves integrity of the message.
Option A, B and D are incorrect because digital signature will not encrypt the message itself, however it encrypts the hash of the message.

(4)Digital signature addresses which of the following concerns about electronic messages?

A. Unauthorized archiving
B. Confidentiality
C. Unauthorized copying
D. Alteration

Answer: D. Alteration
Explanation: A digital signature includes an encrypted hash total of the size of the message as it was transmitted by its originator. This hash would no longer be accurate if the message was subsequently altered, thus indicating that the alteration had occurred. Digital signatures will not identify or prevent any of the other options. Digital signature will not address other concerns.

(5)Which of the following is used to address the risk of hash being compromised ?

A. Digital signatures
B. Message encryption
C. Email password
D. Disabling SSID broadcast.

Answer: A. Digital signature
Explanation:
Digital signature is created by encrypting hash of the message. Encrypted hash cannot be altered without knowing the public key of the sender.

(6)Digital signature provides which of the following?

A. Non-repudiation, confidentiality and integrity
B. Integrity, privacy and non-repudiation
C. Integrity, authentication and non-repudiation
D. Confidentiality , privacy and non-repudiation

Answer: C. Integrity, authentication and non-repudiation
Explanation:Digital signature provides integrity, authentication and non-repudiation for electronic messages. It does not ensure message confidentiality or availability of data.

(7) The MAIN reason for using digital signatures is to ensure data:

A. privacy.
B. integrity.
C. availability.
D. confidentiality

Answer: B. integrity.
Explanation: Digital signatures provide integrity because the hash of the message changes in case of any unauthorized changes in the data (file, mail, document, etc.) thus ensuring data integrity.

(8)Which of the following message services provides the strongest evidence that a specific action has occurred?

A. Proof of delivery
B. Non-repudiation
C. Proof of submission
D. Authorization

Answer: B. Non-repudiation

Explanation: Non-repudiation is the assurance that someone cannot deny something. Non-repudiation services provide evidence that a specific action occurred Typically, non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.. Digital signatures are used to provide non-repudiation.

(9) Which of the following ensures a sender's authenticity?

A. Encrypting the hash of the message with the sender's private key
B. Encrypting the message with the receiver's Public key
C. Encrypting the hash of the message with the sender's public
D. Encrypting the message with the receiver's private key

Answer: A. Encrypting the hash of the message with the sender's private key
Explanation: Sender encrypts the hash of the message using his private key. The receiver can decrypt the same with the public key of the sender, ensuring authenticity of the message. If the recipient is able to decrypt the message successfully with the public key of the sender, then it proves authentication i.e. the message is in fact sent from the sender. It ensures non-repudiation i.e. the sender cannot repudiate having sent the message.

(10) An organization states that digital signatures are used when receiving communications from customers. This is done by :

A. A hash of the data that is transmitted and encrypted with the organization’s private key
B. A hash of the data that is transmitted and encrypted with the customer's private key
C. A hash of the data that is transmitted and encrypted with the customer's public key
D. A hash of the data that is transmitted and encrypted with the organization’s public key

Answer : B. A hash of the data that is transmitted and encrypted with the customer's private key
Explanation: Digital Signature is created in below two steps:
Step 1: Create Hash (Message digest) of the message.
Step 2: Encrypt the hash (as derived above) with the private key of the sender.
In the above scenario, the sender is the customer. Hence hash to be encrypted by using customer’s (sender’s) private key.

(11) Digital signatures helps to:

A. help detect spam.
B. provide confidentiality.
C. add to the workload of gateway servers.
D. decreases available bandwidth.

Answer: A. help detect spam.
Explanation: Using strong signatures in email traffic, authentication and nonrepudiation can be assured and a sender can be tracked. The recipient can configure their e-mail server or client to automatically delete mails from specific senders
Digital signatures are only a few bytes in size and will not slash bandwidth. There will be no major impact to the workload of gateway servers.

(12)Basic difference between hashing & encryption is that hashing:

A. cannot be reversed.
B. can be reversed.

C. is concerned with integrity and security.
D. creates output of a bigger length than the original message.

Answer: A. cannot be reversed
Explanation: Let us understand outcome of hashing as well as encryption:
For the message “Meeting at 8 AM” hash value comes to 4526dee03a36204cbb9887b3528fac4e
For the message “Meeting at 8 AM” encryption results comes to “Mxxxxxx xx x xM”
Now, from hash value 4526dee03a36204cbb9887b3528fac4e we cannot derive the message but from “Mxxxxxx xx x xM” we can derive the original message by decryption.
Hashing works one way. By applying a hashing algorithm to a message, a message hash/digest is created. If the same hashing algorithm is applied to the message digest, it will not result in the original message. As such, hashing is irreversible, while encryption is reversible. This is the basic difference between hashing and encryption.

(13)An organization is sharing critical information to vendors through email. Organization can ensure that the recipients of emails (i.e. vendors) can authenticate the identity of the sender (i.e. employees) by:

A. employees digitally sign their email messages.
B. employees encrypting their email messages.
C. employees compressing their email messages.
D. password protecting all email messages.

Answer: A. employees digitally sign their email messages.
Explanation: By digitally signing all email messages, the receiver will be able to validate the authenticity of the sender. Encrypting all e-mail messages would not ensure the authenticity of the sender.

(14)Digital signature ensures that the sender cannot later deny generating and sending the message. This is known as:

A. Integrity.
B. authentication.
C. non-repudiation.
D. security.

Answer: C. non-repudiation.
Explanation: Non-repudiation ensures that the claimed sender cannot later deny generating and sending the message.

(15)In an e-commerce application, which of the following should be relied on to prove that the transactions were actually made?

A. Proof of delivery
B. Authentication
C. Encryption
D. Non-repudiation

Answer: D. Non-repudiation
Explanation: Non-repudiation ensures that a transaction is enforceable. Non-repudiation ensures that the claimed sender cannot later deny generating and sending the message.

(16)Mr. A has sent a message along with encrypted (by A's private key) hash of the message to Mr. B. This will ensure:

A. authenticity and integrity.
B. authenticity and confidentiality.
C. integrity and privacy.
D. privacy and non-repudiation.

Answer: A. authenticity and integrity.
Explanation: In the above case, the message is not encrypted (only hash is encrypted) and hence it will not ensure privacy or confidentiality. Encryption of the hash will ensure authenticity and integrity.

(17) Digital signatures require the:

A. signer to have a public key of sender and the receiver to have a private key of the sender.
B. signer to have a private key of the sender and the receiver to have a public key of the sender.
C. signer and receiver to have a public key.
D. signer and receiver to have a private key.

Answer: B. signer to have a private key of the sender and the receiver to have a public key of the sender.
Explanation: Digital Signature is created in below two steps:
Step 1: Create Hash (Message digest) of the message.
Step 2: Encrypt the hash (as derived above) with the private key of the sender.
At the recipient end, the hash is decrypted by using the public key of the sender.

(18)A digital signature contains a hash value (message digest) to:

A. ensure message integrity.
B. define the encryption algorithm.
C. confirm the identity of the originator.
D. compress the message.

Answer: A. ensure message integrity.
Explanation: The message digest is calculated and included in a digital signature to prove that the message has not been altered. It should be the same value as a recalculation performed upon receipt. Hence it helps to ensure message integrity.

3.10.9 Network Risks

Following are some of the important aspects related to network related risks:

- Objectives of network security are:
    - Integrity of in-transit data
    - Confidentiality of in-transit data
    - Availability of communication
- The IT department is responsible for managing the risk related to networks.
- Some of the controls to ensure integrity of transit data are use of parity bits, checksums, hashing and digital signatures.

- Encapsulating of IP security (IPsec) in authentication header (AH) mode ensures data confidentiality and data integrity.
- Web based traffic can be encrypted using transport layer security (TLS) for confidentiality. Secure Socket Layer (SSL) is still widely used but is now considered vulnerable to compromise.
- For remote access to a network system, a secure shell (SSH) is commonly used.
- Application level encryption is used to protect the application from other applications that are running on the recipient system.
- Network architecture is an important document to determine and design the network security.
- Devices handling sensitive data should have isolated network segments as an effective means of preventing unauthorized access to data in transit.
- Network configuration setting should be done by only authorized staff through a controlled change management process.
- Use of protocols such as Simple Network Management Protocol (SNMP) is not secured. Connection should be over a secure encrypted connection.
- Supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS) for controlling industrial machinery should have isolated network segments. As their operations are real-time, encryption may not be feasible as a solution.
- Network segmentation should be provided through use of firewalls, IDS, IPS, VLANS and gateways thus providing multiple hurdles for an attacker.
- Applications facing the public internet should be placed in a demilitarized zone (DMZ). DMZ acts as a buffer zone between a trusted and untrusted network. DMZ should be appropriately hardened and all the unused services should be disabled. Critical information and data should not be stored in a DMZ. A mail relay should normally be placed within a DMZ to shield the internal network.
- External security threats can be prevented by use of network address translation as they are having internal addresses that are non-routable.
- For communication with external trusted associated partners a private network should be used known as an extranet which connects internal networks on the basis of secure authentication.
- It is recommended to have different connections for different functions which allows for tailored security measures for every function.
- Organization should have appropriate arrangement for alternate routing, redundancy of cable and network devices, and load balancing.
- Objective of a network vulnerability is to identify the vulnerabilities associated with misconfigurations and missing updates.

Key aspects from CRISC exam perspective

CRISC Question	Possible Answer

Objective of a network vulnerability	To identify the vulnerabilities associated with misconfigurations and missing updates.

Self-Assessment Questions

(1)Data transmitted on a network can be best protected by:

A. encapsulation of data packets with authentication header
B. applying hash to all messages sent on network
C. hardening of all network devices
D. use of fibre optic cables for networking

Answer: A. encapsulation of data packets with authentication header
Explanation: Encapsulating of IP security (IPsec) in authentication header (AH) mode ensures data confidentiality and data integrity. Other options are not as effective as data encapsulation.

(2)Which of the following vulnerabilities allows attackers access to data through a web application?

A. Validation checks are missing in data input fields.
B. Password history rule not implemented.
C. Application logs are not monitored at frequent intervals.
D. Two factor authentication not implemented.

Answer: A. Validation checks are missing in data input fields.
Explanation. In absence of validation checks in data input fields, attackers are able to exploit other weaknesses in the system. For example, through SQL injection attacks, hackers can illegally retrieve application data. Other options may make applications vulnerable but these can be countered in other ways.

(3)Device that can be installed in a demilitarized zone is:

A. email server
B. firewall
C. authentication server
D. corporate database server

Answer: A. email server
Explanation: Email server or mail relay can be installed in a demilitarized zone to protect the internal network. External emails may contain malicious contents to compromise the internal network of the organization. Authentication server and corporate database server should not be placed in a demilitarized zone (DMZ). Firewalls may provide another segment for DMZ, but do not technically reside within the DMZ network segment.

(4)External security attack can be prevented by:

A. analysing system access log
B. conducting background verification of temporary staff
C. network address translation
D. internal audit

Answer: C. network address translation
Explanation: External security threats can be prevented by use of network address translation as they are having internal addresses that are non-routable. Other options are not as effective as network address translation.

(5)Objective of network vulnerability assessment is:

A. to identify spyware
B.to identify misconfiguration and missing updates
C.to identify preparedness of security team
D.to identify zero days' vulnerabilities

Answer: B.to identify misconfiguration and missing updates
Explanation: A network vulnerability assessment intends to identify known vulnerabilities that are based on common misconfigurations and missing updates. Network vulnerability assessment may not be best to address option A, C and D.

3.11.1 System Testing

Following are some of the important testing for SDLC:

Unit Testing

- Unit tests include tests of each separate program or module.
- Testing is generally conducted by developers themselves. It is conducted as and when a program or module is ready and it does not require to wait until completion of the total system.
- Unit testing is done through a white box approach wherein internal program logics are tested.

Integrated Testing

- Integrated test includes integration or connection between two or more system components.
- Purpose of the integration test is to validate accurate and correct information flow between the systems .

System Testing

- System testing tests the complete and full system capabilities.
- It covers end to end system specifications.
- It covers functionality test, recoverability test, security test, load test, volume test, stress test and performance test.

Final Acceptance Testing

- Final acceptance test consists of two tests i.e. QAT (quality assurance test) and UAT (user acceptance test)

Regression Testing

- Meaning of regression is to return to an earlier stage.
- Objective of a regression test is to confirm that a recent change has not introduced any new faults and other existing features are working correctly.
- It must be ensured that the same data (which was used in earlier tests) should be used for the regression test. This will help to confirm that there are no new errors or malfunctioning.

Sociability Testing

- Sociability means the quality of being able to merge with others.
- Objective of the sociability test is to ensure that the new system works as expected in existing infrastructure without any adverse impact on other existing systems. the application works as expected in the specified environment where other applications run concurrently.

Pilot Testing

- A pilot test is a small-scale preliminary study to understand and evaluate system functionality and other aspects.
- Pilot test is conducted for only few units or few locations to evaluate the feasibility.
- Objective of the pilot test is to determine the feasibility of the new system before full fledged implementation.

Parallel Testing

- Parallel test involves the testing of a new system and comparing the results of a new system with that of an old system.
- Objective of parallel testing is to ensure that the new system meets the requirements of the user.

White Box & Black Box Testing

White Box Testing

- In white box testing, program logic is verified.
- For conduct of white box testing, appropriate knowledge of programming language is a must.
- White box testing is generally conducted for unit testing

Black Box Testing

- In black box testing, emphasis is on functionality of the system.
- For conduct of black box testing, knowledge of programming language is not mandatory.
- Black box testing is generally conducted for user acceptance test and interface testing.

Alpha & Beta Testing

Alpha Testing

- Alpha testing is conducted by internal user
- Alpha test is conducted before beta test
- Alpha test may or may not include full functionality test

Beta Testing

- Beta test is conducted by external user
- Beta test is conducted after alpha test
- Beta test is generally conducted for full functionality

Key aspects from CRISC exam perspective

Below table covers important aspect from CRISC exam perspective:

CRISC Questions	Possible Answer
In which test, testing of architectural design is conducted?	Integration testing
In which test, testing for linked and connected modules is conducted?	Integration Testing
Failure of which test has the greatest impact?	Acceptance Testing
Which test is required to determine the ability of a new system to operate in the existing environment without any adverse impact on other systems?	Sociability Testing

Self-Assessment Questions

(1) To determine proper working of new system without adverse impact on other existing systems, most appropriate test is:

A. unit test
B. pilot test
C. sociability test
D. integration test

Answer: C. sociability test
Explanation: Objective of the sociability test is to determine whether a new system can operate effectively without adverse impact on other existing systems. Integration test is to verify connection and information between two or more systems. Pilot testing includes testing in different phases i.e. first at one location and then extended to other locations. Unit testing is the test of individual functions, modules or units.

(2) Which of the subsequent tests is presumably to be conducted when a system is in the development phase?

A. User acceptance test
B. stress test
C. Regression test
D. Unit test

Answer: D. Unit test
Explanation:Unit tests require individual program or module testing. The development team should ensure that each module or programs are reviewed during the event stage to ensure the code is running properly. Stress test, regression test and acceptance test will usually take place later, once the system has been built and ready for implementation.

(3) Which of the following approaches is applied during unit testing?

A. top-down
B. black box
C. bottom-up
D. white box

Answer: D. white box

Explanation: In any given case, the best technique for unit testing is white box approach (because both require internal logic testing). Unit testing requires individual program or module testing. The program logic is tested in white box testing. This is applicable to testing systems and to test interfaces. White box research looks at a module's internal structure. In the recorder, only functionality is tested. Program logics are not tested and are therefore not applicable to unit testing.

(4) Testing of two or more systems network for accurate data flow between them is:

A. unit testing
B. interface testing
C. sociability testing
D. regression testing

Answer: B. interface testing
Explanation: Interface testing may be a hardware or software test that evaluates the connection of two or more components that pass information from one area to another.

(5) For some instances system interface failures occur when corrections are re-submitted to previously observed errors. This might indicate absence of which of the subsequent kinds of testing?

A. Pilot testing
B. Integration testing
C. Parallel testing
D. Unit testing

Answer: B. Integration testing
Explanation: Integration testing / interface testing is completed to ensure correct and accurate data flow between two or more systems. Integration testing aims to ensure accuracy of the device interface's most critical components. To evaluate the results, pilot testing takes place first at a single location.

(6) What data should be used for regression testing when an organization is conducting regression testing for rectified bugs within the system?

A. Same data as utilized in previous test
B. Random data
C. Different data as utilized in previous test
D. Data produced by a test data generator

Answer: A. Same data as utilized in previous test
Explanation: Regression's dictionary meaning is' act of going back' or' return.' Regression testing ensures that adjustments or corrections have not created new errors during a system. Therefore, It is also ready to be achieved so that the information used for regression testing is the same because of the data used in previous tests.

(7) Which of the subsequent testing would be relevant when an organization needs to determine whether a replacement or modified system is capable of functioning in its target environment without affecting other existing systems?

A. Regression testing
B. Sociability testing
C. Interface/integration testing
D Pilot testing

Answer: B. Sociability testing
Explanation: Sociability testing is performed to ensure the new or changed system will operate without having an adverse effect on existing systems. The aim of sociability testing is to verify that a replacement or modified system can function within its target environment without adversely affecting existing systems.

(8) Which of the following characteristics of white box testing differentiates between white box testing and black box testing?

A. white-box testing involves an IS auditor.
B. white-box testing involves testing of the program's logical structure.
C. white-box testing involves a bottom-up approach.
D. white-box testing does not involve testing of the program's logical structure.

Answer: B. white-box testing involves testing of program’s logical structure.
Explanation: The software logic is tested in white-box testing when only functionality is tested in black-box testing. The program logic is not tested in black-box testing. White box testing includes the knowledge to be implemented / tested about the system internals or the module. Black box testing requires an awareness of the program's features. Neither test method has to include the IS auditor.

(9) Which of the following is the primary purpose for conducting parallel testing?

A. To ensure adherence to budget
B. To record the functionalities of the program.
C. To highlight errors in the program logic
D. Validate device functionality with user specifications.

Answer: D. Validate device functionality with user specifications.
Explanation: Parallel testing is the method of comparing Old and New system results. The objective of parallel testing is to ensure that the user requirements are met when implementing a new program. Unit testing is used to validate individual module or system program logic.

(10) What should be the IS auditor's major concern while reviewing the process of acceptance testing?

A. Test objectives not documented.
B. Expected test results not documented by user.
C. Test problem log not updated.
D. unsolved major issues.

Answer: D. unsolved major issues.
Explanation: All of the options include IS auditor reviewing acceptance testing procedure. Option D, i.e. major issues are still pending, but major concern. The IS auditor will then determine the effect on system functionality and usability of the unresolved issues.

(11) Failure in which stage can have the greatest adverse impact on cost and time budget?

A. Unit testing
B. Integration testing
C. System testing
D. Acceptance testing

Answer: D. Acceptance testing
Explanation: The first test step is unit testing. Step two is integrated testing. Third stage is system testing and the fourth stage is final acceptance. Acceptance testing is the final stage before installation of the app, and is available for use. The biggest impact will come if the program fails at the point of acceptance testing, as that could lead to delays and overruns. Unit, integration and device testing is conducted by developers at various development levels, and the effect of failure is comparatively less than acceptance testing.

(12) The primary purpose of a system test is to:

A. Testing efficiency of system built-in security controls.
B. Set appropriate system functionality documentation.
C. Evaluate the functioning of the system.
D. Identify and document New Program Benefits.

Answer: C. Evaluate the functioning of the system.

Explanation: System testing includes (i) Recovery testing (ii) Security testing (iii) Load testing (iv) Volume testing (v) Stress testing & (vi)Performance testing. The key reason a system is evaluated is to assess the reliability of the whole system.

(13) When creating data for testing the logic in a new system, which of the following is most critical?

A. quantity of the data.
B. data designed as per expected live processing.
C. sample of actual data
D. completing the test as per schedule.

Answer: B. data designed as per expected live processing.
Explanation: Data designed as per expected live processing gives accurate results. Quality is more important than quantity. Sample of actual data may not cover all the scenarios in the live environment.

3.11.2 System Migration & Changeover (Go-live) Techniques

Changeover (Go-live) Techniques

Following are three changeover techniques for moving data to new system:

Parallel Changeover

- In parallel changeover, both new systems and old systems are operated simultaneously.

.

- Objective of parallel changeover is to test the reliability and performance of a new system before discontinuing the old system.

.

- Parallel changeover reduced the risk of failed changeover.

.

- It allows the staff to get acquainted and trained on a new system.

.

- Main disadvantage of parallel changeover is the cost of running both the systems and ensuring data is consistent between the two systems.

Phased Changeover

- In phased changeover, new modules are implemented in a phased manner.
- This addresses the risk of complete system failure as new modules are tested and implemented in a gradual manner.
- Following are some of the challenges of phased changeover:
    - Requirement of distinct hardware, OS, database etc. to maintain two unique environments.
    - To ensure consistency of data between new and old modules.

Abrupt Changeover

- In an abrupt changeover, a new system is implemented and the old system is taken off immediately.
- It is the riskiest kind of changeover as a full system needs to be rolled back if changeover is failed.
- Abrupt changeover is feasible where rollback is relatively easy and there is minimum impact of business processes.

Challenges related to Data Migration

- Process of migration possesses high risk for data integrity and availability. Migration process should be thoroughly reviewed by the risk practitioner.
- Risk practitioner should consider following points while reviewing system migration process:

- To ensure correctness and completeness of the data transferred from old system to new system.
- To ensure that data integrity is being maintained and there is no transcription or transposition error by transfer of data.
- To ensure that appropriate backup is available for transferred data to address the risk of data corruption.
- To ensure that the field/record/index and other data schema is consistent between old system and new system.

Fall back (Rollback)

- Organization should have a structured fallback plan in place to address the risk of failure of system changeover or system migration.
- Objective of a fallback plan is to roll back and return to the prior system.
- Organization should have all required capability for roll back of the system before starting the changeover process

Key aspects from CRISC exam perspective

Below table covers important aspect from CRISC exam perspective:

CRISC Questions	Possible Answer
Who has responsibility for signing off on the accuracy and completeness of data migration of new system ?	Data owner/ User
Benefit of Parallel Cutover	Assurance that new system is working as per user requirement before discarding old system
Which system migration method has the greatest risk?	Direct cutover or Abrupt cutover
Which system migration method has the greatest redundancy?	Parallel Change
What is the greatest concern about the Direct Cutover Method?	Lack of backout plan

Self-Assessment Questions

(1) Who should approve completion and implementation of a new system application?

A. board members
B. user management
C. quality assurance team
D. project steering committee

Answer: B. user management

Explanations. It is the user management who assumes ownership of the project and should provide sign off for completion and implementation of the system as per agreed deliverables.

(2) Which of the following is the greatest benefit of parallel changeover?

A. It provides significant cost saving
B. It provides assurance the new system meets the requirement before old system is discontinued
C. It provides hands on training to employees for use of new system before old system is discontinued
D. It provides opportunity to integrate new and old system

Answer: B. It provides assurance the new system meets the requirement before old system is discontinued
Explanation: In parallel changeover, both new and old systems are operated parallel for some time. This
helps to minimize the risk of consequences of defect of the new system.

(3) Which of the following is the prime objective of parallel testing?

A. To determine cost effectiveness of system
B. To ensure the new system meets the user requirement
C. To enhance system capabilities
D. To evaluate results of unit testing

Answer: B. To ensure the new system meets the user requirement
Explanation: Objective of parallel testing is to ensure that user requirements are met. Parallel testing involves comparing the results of the new system with the old system to determine correct processing of new system.

(4) Which of the following is the greatest risk in a system migration procedure?

A. new system will be rolled out in phased manner
B. quality plan not available for system migration
C. users are involved in acceptance testing
D. use of prototyping approach to confirm user requirement

Answer: B. quality plan not available for system migration
Explanations. It is very important to have a quality plan for any project. Quality plans should be comprehensive and should address the issue of data integrity during migration. Other options cannot be considered as risk.

(5) Which of the following is the greatest concern for a system migration project?

A. planned migration window is too short for completing all task
B. abrupt changeover is planned, immediately disposing legacy system
C. employees have been handed over new system without adequate training
D. printing functionality of new system tested after changeover

Answer: B. abrupt changeover is planned, immediately disposing legacy system
Explanation: Changeover should be phased wise or parallel to address the risk of implementation of a new system. Disposing the old system will complicate the fall back strategy. Abrupt change over has its own risk and consequences. Other options are not as significant as abrupt changeover without a backup plan.

(6) Which of the following changeovers assumes greatest risk?

A. parallel
B. pilot
C. phased
D. direct cutover

Answer: D. direct cutover
Explanation: In direct cutover, a new system is implemented from a cut-off date and the older system is completely discontinued once the new system is implemented. This process is also known as abrupt changeover. This is considered as the riskiest approach with no scope of rollback in case a new system fails.

(7) Which of the following changes assumes greatest redundancy?

A parallel
B. pilot
C. phased
D. direct cutover

Answer: A parallel
Explanation: In this method, both new and old systems are operated parallel for some time. Once the users are confident about the new system, the old system may be discontinued. This helps to minimize the risk of consequences of defect of the new system. Major challenge in this method is the requirement of more resources to maintain both the systems.
It provides assurance that the new system meets the requirement before the old system is discontinued. Parallel changeover provides greatest redundancy.

(8) Prime responsibility for signing off on the accuracy and completeness of data migration of a new system?

A. Steering committee
B. IS Auditor
C. Data owner
D. Project Manager

Answer: C. Data owner
Explanation: Data owner assumes the responsibility for reviewing the completeness and accuracy of data migration and providing sign-off for the same.

(9) Which of the following is the greatest concern for an immediate cutover to the new system?

A. lack of back out plan
B. user acceptance testing not properly documented
C. project deadline is extended
D. users are not trained properly to utilize new system

Answer: A. lack of back out plan
Explanation: In an immediate cutover scenario, absence of a backout plan is a major concern as it takes considerable time, effort and cost to restore the old systems. It is advisable to have a parallel or phased changeover strategy. Other options are not as critical as lack of backup plan.

(10) Which of the following is the PRIMARY purpose for conducting parallel testing when an organization implementing a new system adopted parallel testing?

A. The budget includes ensuring cost.
B. To record the functionalities of the program.
C. To highlight errors in the program logic
D. Validate device functionality with user specifications.

Answer: D. Validate device functionality with user specifications.
Explanation: Parallel testing is the method of comparing Old and New system results. The objective of parallel testing is to ensure that the user requirements are met when implementing a new program. Unit testing is used to validate individual module or system program logic.

3.11.3 Post implementation Review

- Objective of a post implementation review is to determine the efficiency and effectiveness of the system and to ensure that the system is capable to support the business requirements.
- Following aspects are reviewed during a post implementation review:
    - Whether the system meets the user requirement?
    - Whether controls are appropriately defined and deployed?
    - Whether return on investment (ROI) is effective?
    - Whether the risk of the new system is within the acceptable limit?
- Lessons learnt during the implementation should be documented and to be considered for future projects.
- Review should be jointly conducted by the project development team, end users and risk practitioner.
- Post implementation review should be conducted after sufficient time period to determine the effectiveness, efficiency and adequacy of the project.

Project Closeout

Closing a project is a formal process to determine the positive and negative points for the implemented project and how to address the same as next project management. Following are important steps for closing a project:

1. If any issues are outstanding, specific individuals should be made accountable for follow up and closure.
2. Document relevant risk related to the project and to update the risk register.
3. Project documentation should be properly archived for future reference.
4. Conduct of post implementation review
5. To take final sign-off from the end user with respect to deliverables.

Key aspects from CRISC exam perspective

Below table covers important aspect from CRISC exam perspective:

CRISC Questions	Possible Answers
What are the prime objectives of post implementation review?	● To determine the extent to which project met its objective and addressed the requirements originally defined. ● To determine cost benefit analysis and return on investment ● To determine lessons learned from the project for improvement of future projects
What should be the area of focus for a risk practitioner during a post implementation review?	To determine adequacy and effectiveness of security controls

Self-Assessment Questions

(1) Who should approve completion and implementation of a new system application?

A. board members
B. user management
C. quality assurance team
D. project steering committee

Answer: B. user management
Explanations. It is the user management who assumes ownership of the project and should provide sign off for completion and implementation of the system as per agreed deliverables.

(2) Post implementation review includes:

A. interface testing
B. analysis on return on investment
C. review of audit trails
D. review of enterprise architecture diagrams

Answer: B. analysis on return on investment
Explanation. One of the purposes of conducting a post implementation review is to do cost benefit analysis or return on investment to determine that original business case requirements are met.

(3) Risk practitioner's primary focus during post implementation review is:

A. to determine appropriate documentation of user feedback
B. to determine whether return on investment is being measured
C. to determine operating effectiveness of controls built in the system
D to review change management procedure.

Answer: C. to determine operating effectiveness of controls built in the system
Explanation: From IS audit perspective, IS auditor's prime focus should be on determining the adequacy and effectiveness of controls built in the system. Other options are important but a more significant area of focus should be the effectiveness of controls built in the system.

(4) Risk practitioners are conducting post implementation review of an ERM system. He is most likely to review:

A. access control setting
B. procedure for unit testing
C. procedure for system testing
D. detailed design documentation

Answer: A. access control setting
Explanation: Risk practitioners are most likely to review whether security parameters have been appropriately mapped in the new system. One of the parameters is to review access control configuration. Post implementation review is done after user acceptance testing and hence the auditor may not like going into details of unit testing, system testing or design documentation.

(5) Post implementation review should cover:

A. assessment of downtime risk
B. identification of lessons learnt to improve future projects
C. verification of controls built in the system
D. deletion of test data

Answer: B. identification of lessons learnt to improve future projects

Explanation. One of the reasons for conducting a post implementation review is to identify the lessons learned and use them for improvement of future projects.

(6) Post implementation review is conducted primarily to:

A. Ensure that the project meets the intended business requirements.
B. determine adequacy of information security
C. determine compliance with regulatory requirements
D. evaluate project expenses against the budget

Answer: A. Ensure that the project meets the intended business requirements.
Explanation Post implementation review is conducted primarily to ensure that the project is implemented in accordance with business requirements. Other options are not the primary objective.

(7) Which of the following is the main objective of post implementation review?

A. documentation of lessons learned
B. identification of future enhancements
C. to determine timely delivery of project
D.to determine whether project objectives are met

Answer: D. to determine whether project objectives are met
Explanation: Main objective of performing a post implementation review is to determine the project's overall success and impact on business. If project objectives are successfully achieved, then it indicates success of the project. Although other options are important, it is more important to determine whether project objectives are met.

3.12 Impact of Emerging Technologies on Design and Implementation of Controls

Organizations should have well defined and documented processes of use and new emerging technologies. Unauthorized use of new technology possesses a great risk for the organization.
Risk practitioners should make use of discovery scanners to detect unauthorized use of new technology or devices that have not yet been reviewed and approved for use.

3.13 Control Ownership

- Risk register should include the owner of each risk who is accountable for managing that risk. Risk owner should be a senior official who can make decisions for managing the risk.
- Mapping of each risk to relevant business processes is the best basis for establishing the risk ownership. Risk ownership should be documented in a risk register. A risk register contains the details of each risk like likelihood, potential impact, priority, status of mitigation and risk owner.
- There should be frequent communication between risk practitioners and risk owners with respect to risk responses and control effectiveness.
- Risk owners should ensure that residual risk is within the acceptable limit of the organization.
- Results of continuous monitoring should be communicated to the risk owner as they own the risk and are responsible for appropriate risk response.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
What is the best basis for establishing risk ownership?	To map risk to relevant business process
Risk ownership should be documented in	Risk Register
Whom should the results of continuous monitoring be best communicated?	Risk Owner

Self-Assessment Questions

(1) Risk ownership should be best established on the basis of:

A. linking overlapping departments
B. analysing the risk response budget
C. IT department
D. mapping identified risk to specific process owner

Answer: D. mapping identified risk to specific process owner
Explanation: Best way to establish the ownership of a risk is to map that risk to the relevant process owner.

(2) Risk ownership and risk mitigation details should be best documented in:

A. business continuity plan

B. BIA document
C. risk register
D. business case

Answer: C. risk register
Explanation: Risk register is the inventory of all the existing risks of the organization. For each risk, details like likelihood, potential impact, priority, status of mitigation and owner should be documented. Other options do not contain details of risk mitigation and ownership.

(3) Results of control monitoring should be best communicated to:

A. risk owner
B. audit department
C. IT department
D. security manager

Answer: A. risk owner
Explanation: Results of the risk monitoring should be discussed and communicated with the risk owner as they own the risk and are accountable for maintaining the risk within acceptable level. Though as a best practice, results should be communicated to other support functions but primarily it should be made available to the risk owner.

3.14 Risk Management Procedures and Documentation

Risk management is mostly achieved by combining administrative, technical and physical controls. Role of a risk practitioner is very critical to ensure that controls are adequate and operating as designed. Risk practitioner should ensure that following control management procedure is followed:

- Proper implementation of the control
- Availability of documented procedures to support the operations
- Availability of change management procedure for configuration
- Training of the staff to review the controls
- Allocate ownership of each control to senior official

Chapter 4 Risk and Control Monitoring and Reporting

Once the risk response is implemented in the form of controls, it is very important to continuously monitor the effectiveness and efficiency of control. Results of the risk monitoring should be reported to management to help them determine the effectiveness of the risk management program. This chapter covers following topics:

4.1 Key Risk Indicators
4.2 Key Performance Indicators
4.3 Data collection and extraction tools and techniques
4.4 Monitoring Controls
4.5 Control Assessment Types
4.6 Result of Control Assessment
4.7 Changes to IT Risk Profile

4.1 Key Risk Indicators

- Risk indicator is a measure used by an organization to determine the level of current risk for an activity. This helps the organization to monitor the risk level and receives an alert when a risk level approaches an unacceptable level.
- Thus, the objective of key risk indicators is to flag the exception as and when it occurs. This provides an opportunity for the organization to respond to the risk before damage is done.
- Examples of key risk indicators are:
  - Number of unauthorized software detected in audit.
  - Hours of system downtime
  - Number of systems without antivirus
- Let us take one example of system downtime. Risk indicator can be set as follow:

Description	Risk Indicator
System downtime less than 5 hours	Acceptable
System downtime between 5 to 10 hours	Close Monitoring
System downtime more than 10 hours	Unacceptable

- Number of workstations vis-à-vis the count of employees can be considered as a key risk indicator for configuration management. High amount of excess inventory as compared to actual employees indicates poor configuration as the same is not mapped correctly with actual business requirements. Similarly, a high level of shortage of workstation also indicates poor configuration mapping.

Advantage of KRI

Following are the advantages of KRIs:

- It helps to validate the risk appetite and risk tolerance level of the organization.
- It helps to identify the risk in an objective way.
- It helps in quantification of the risk
- It helps in continuous risk monitoring
- It helps in triggering risk mitigation action
- It helps in monitoring and managing regulatory compliance

KRI Selection

- Selection of the right kind of KRI is utmost important for the success of a risk management program.
- Following are the some of the characteristics of a good metrics also termed as SMART:
  - **Specific**: KRI should be clear, concise and easily understandable
  - **Measurable**: KRI should be able to quantified and there should not be any subjectivity
  - **Attainable**: KRI should be something realistic
  - **Relevant:** KRI should be relevant to the goals and objective of the organization
  - **Time**: KRI should be achievable in a given time frame
- Risk indicator should include and cover:
  - Lag indicators i.e. occurrence of risk events
  - Lead indicators i.e. preventive controls
  - Trends over a period of time
- For the effectiveness of KRI, the organization must ensure that data used to measure the KRI is complete, correct and accurate.
- KRI threshold should be aligned with risk appetite and risk tolerance of the organization. KRIs need to be evaluated on a regular basis to verify that each KRI remains properly related to the risk appetite and tolerance levels of the organization.

Design of Key Risk Indicator (KRI)

Following are some of the key aspect for design of KRI in order of their priority:

- KRI should be linked to specific risk
- KRI should be capable to predict a risk event
- KRI should be complete and accurate
- KRI should be easily measurable and comparable

Linking to a specific risk is the most important criterion when selecting a KRI.

To ensure the KRI are effective and linked to specific risk, a risk manager must understand the end-to-end operational flow of the business processes. This will help to understand various aspects of the business such as detailed processes, data flows, decision-making processes, risk appetite and tolerance. On the basis of this information, risk practitioners can design relevant and specific KRI along with measurement criteria.

Identification of Key Risk Indicators (KRI)

Key risk indicators are generally identified during the risk response stage (i.e. before the risk monitoring stage). During the risk response stage, controls for mitigation of the risks are selected and implemented. Once the controls are implemented, some KRI is to be identified and developed. These KRIs will help to determine the effectiveness of the control. If KRI is within the threshold, it indicates that controls are effective. In case KRI crosses the threshold, then additional controls may be required.

Responsibility of monitoring of Key Risk indicators (KRI)

KRI should be measured and monitored by an independent team to ensure unbiasedness. If the same is measured by line managers, the same should be reviewed by independent authority. It is equally important that his efforts are reviewed and validated by a senior official. Most effective method to validate the efforts of a line manager is to review the reported results by an independent person. This helps to determine the efficiency and effectiveness of line managers in monitoring the key risk indicators.

Reporting of KRI results

- When KRI reaches its threshold, it should be first reported to the business process owner who owns the risk and determines the risk response. Process owners should evaluate the effectiveness of existing control and to determine whether additional controls are required.

- Results of key risk indicators are to be placed to senior management at periodic intervals. KRIs are the most useful data for management to determine current state of risk.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
Who should measure and monitor the KRI? ·	Independent team to ensure unbiasedness. (If the same is measured by line managers, the same should be reviewed by independent authority.)
During which stage KRI is generally identified?	Risk Response stage
Best monitoring capability to identify whether controls that are in place remain effective in mitigating their intended risk?	Measuring key risk indicators
Which is the most important factor to be considered while implementing a KRI?	KRI is linked with specific risks
Which is the most useful data for communicating to management about the current state of risk?	Measurement of key risk indicator

Which is the best method for proper design of an effective KRI?	Understand the end-to-end operational flow of the business
Who should be alerted first for KRI reaching the thresholds?	Business Process Owner

Self-Assessment Questions

(1) Most effective method to validate the efforts of line manager to monitor the key risk indicators (KRI) is:

A. independent review of reported results
B. provide risk management training to line manager
C. risk management team should design the KRI
D. KRI should always be quantifiable

Answer: A. independent review of reported results
Explanation: Line manager is responsible to monitor the key risk indicator. However, it is equally important that his efforts are reviewed and validated by a senior official. Most effective method to validate the efforts of a line manager is to review the reported results by an independent person. This helps to determine the efficiency and effectiveness of line managers in monitoring the key risk indicators.

(2) Key risk indicator (KRI) is mostly identified at which of the following stages?

A. risk response stage
B. risk monitoring stage
C. control testing stage
D. risk analysis stage

Answer: A. risk response stage
Explanation: Key risk indicators are generally identified during the risk response stage (i.e. before the risk monitoring stage). During the risk response stage, controls for mitigation of the risks are selected and implemented. Once the controls are implemented, some KRI is to be identified and developed. These KRIs will help to determine the effectiveness of the control. If KRI is within the threshold, it indicates that controls are effective. In case KRI crosses the threshold, then it indicates that existing control is not adequate and additional controls may be required.

(3) Number of workstation can be a key risk indicator for:

A. data management
B. configuration management
C. change management
D. operations management

Answer: B. configuration management
Explanation: Number of workstation vis-à-vis count of employees can be considered as a key risk indicator for configuration management. High amount of excess inventory as compared to actual employees indicates poor configuration as the same is not mapped correctly with actual business requirements. Similarly, a high level of shortage of workstation also indicates poor configuration mapping.

(4) Which of the following best indicates that controls are effective to mitigate the risks?

A. experience of risk practitioner
B. key risk indicator
C. key performance indicator
D. business impact analysis

Answer: B. key risk indicator
Explanation: Key risk indicator best indicates that controls are effective to mitigate the risk. KRI helps to determine the effectiveness of the control. If KRI is within the threshold, it indicates that controls are effective. In case KRI crosses the threshold, then it indicates that existing control is not adequate and additional controls may be required.

(5) Most important aspect while designing a key risk indicator (KRI) is:

A. KRI is linked to specific risk
B. KRI is easy to measure
C. KRI is easy to interpret
D. KRI is easy to quantify

Answer: A. KRI is linked to specific risk
Explanation: Linking to a specific risk is the most important criterion when selecting a KRI. If KRI is not addressing a specific risk, then it will not serve any purpose. Following are some of the key aspect for design of KRI in order of their priority:
1. KRI should be linked to specific risk
2. KRI should be capable to predict a risk event
3. KRI should be complete and accurate
4. KRI should be easily measurable and comparable

(6) Most useful data for communicating to senior management about status of enterprise risk is:

A. results of control self-assessment
B. audit reports
C. risk scenarios
D. results of key risk indicators

Answer: D. results of key risk indicators
Explanation: Results of key risk indicators are to be placed to senior management at periodic intervals. KRIs are the most useful data for management to determine current state of risk.

(7) Most effective aspect for design of key risk indicator (KRI) is:

A. KRI is accurate and complete
B. KRI has capability to predict a risk event
C. KRI is quantifiable
D. KRI is interpretable

Answer: B. KRI has capability to predict a risk event
Explanation: Following are some of the key aspect for design of KRI in order of their priority:
1. KRI should be linked to specific risk
2. KRI should be capable to predict a risk event
3. KRI should be complete and accurate

4. KRI should be easily measurable and comparable

(8) Key risk indicator metric is said to be most reliable when:

A. it provide results within threshold
B. it provide results at predefined interval
C. it flags exception every time they occur
D. it provide quantifiable results

Answer: C. it flags exception every time they occur
Explanation: Risk indicator is a measure used by organization to determine the level of current risk for an activity. This helps the organization to monitor the risk level and receives an alert when a risk level approaches an unacceptable level. Thus the objective of key risk indicators is to flag the exception as and when they occur. This provides an opportunity for the organization to respond to the risk before damage is done.

(9) Which of the following best assists in the proper design of an effective key risk indicator (KRI)?

A. designing the frequency of reporting
B. designing measurement criteria for the risk
C. reviewing the security budget for each risk
D. documenting detailed flow of operational process

Answer: D. documenting detailed flow of operational process
Explanation: To ensure the KRI are effective and linked to specific risk, a risk manager must understand the end-to-end operational flow of the business processes. This will help to understand various aspects of the business such as detailed processes, data flows, decision-making processes, risk appetite and tolerance. On the basis of this information, risk practitioners can design relevant and specific KRI along with measurement criteria.

(10) A risk practitioner noted that a specific KRI related to the critical system reached its threshold. It should be first reported to:

A. process owner
B. IT dept.
C. security team
D. senior management

Answer: A. process owner
Explanation: When KRI reaches its threshold, it should be first reported to the business process owner who owns the risk and determines the risk response. Process owners should evaluate the effectiveness of existing control and to determine whether additional controls are required.

4.2 Key Performance Indicators

- Performance indicators operate in the same way as risk indicators with only difference is the risk indicator is to measure and monitor the risk whereas performance indicator is to measure and monitor the performance. Performance indicators measure how well a process is doing in terms of its goals and objectives.

- For example, a KPI may indicate that an error rate of 10 percent is within limit however anything above 10 percent requires escalation with some form of response.
- Following are the characteristics of a good KPI metrics:
  - KPI should have a feature of SMART i.e. smart, measurable, achievable, reliable and timeliness.
  - KPI should provide value to the business.
  - KPI should be linked to a specific business goal.
  - KPI should be measurable and comparable over a period of time.
- With the use of key performance indicators, organizations can measure and monitor a performance change indication.
- Key Performance Indicators and Key Risk Indicators are mostly used in combination with one another to measure performance and mitigate risk.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answer
What is the primary objective of key performance indicators ?	To determine how well a process is doing in terms of its goals and objectives.

Self-Assessment Questions

(1) A risk practitioner has set a threshold of 15% error for a critical process. Which of the following provides a warning when the error rate reaches the threshold?

A. key performance indicator
B. fault tree analysis
C. functional point analysis
D. Delphi method

Answer: A. key performance indicator
Explanation: Performance indicator measures how well a process is doing in terms of its goals and objectives. For example, a KPI may indicate that an error rate of 10 percent is within limit however anything above 10 percent requires escalation with some form of response. A fault tree analysis is used to identify the sources of a risk, but not the measurement of risk. Function Point Analysis is used to measure the size of software. Delphi method is a qualitative risk assessment technique.

4.3 Data collection and extraction tools and techniques

Variety of data sources is required to measure and monitor the risk. Following are some of the important source of data collection:

- Risk assessment reports
- Project related documents like UAT, post implementation reviews etc.
- Incident management database
- IT helpdesk database
- Audit reports

- Security assessment reports
- Event and activity logs

Logs

- Analysis of the log data is very important to determine the level of security violations. It helps in forensic investigations. It helps to take corrective action by strengthening controls wherever required.

- Determining the level of log capturing is very crucial. If a high level of data is captured for log monitoring, it may impact system speed. On the other hand, if some important events are not captured then it may be difficult to notice significant individual events.

- For forensic purposes, time synchronization of log entries is of utmost importance to correlate multiple events.

- Risk practitioners should ensure that logs should be allowed as read only mode. It should not be allowed to be altered or deleted. System administrators with responsibility for systems or applications should generally not have the ability to alter or delete logs made against their own scopes of responsibility.

- Objective of capturing a log is to do follow up investigation for suspected attempts. Results of investigation help in taking various preventive and corrective action. Mere capturing the logs or generating the reports will not serve the ultimate purpose. Hence most useful metrics for measuring the success of log monitoring is to determine percentage or number of suspected attempts investigated. If organizations do not investigate and keep only capturing the log, the ultimate objective of log capturing is not achieved. The most useful metric is one that measures the degree to which complete follow-through has taken place.

Security Information and Event Management

Capturing of the log will not be meaningful unless it is analyzed to gain some insight. Manual review of the log is not feasible in a complex environment. Security information and event management (SIEM) system collects the data from various sources and analyzes the same for possible security events.

The SIEM system has capability to detect the attacks by signature or behavior (heuristics) based analysis. SIEM has capability for granular assessment. SIEM can highlight the developing trends and can alert the risk practitioner for immediate response.

SIEM is the most effective method to determine the aggregate risk from different sources.

Integrated Test Facilities (ITF)

- In ITF, fictitious entities are created in a live environment. As the live environment is used, there is no need to create separate test processes. However, careful planning is necessary and test data must be isolated from production data.

- This technique allows the auditor to open a dummy account.

- Auditors can enter dummy or test transactions and verify the processing and results of these transactions for correctness.

- Processed results and expected results are compared to verify that systems are operating correctly.

- Example: A dummy asset of $ 100000/- is entered into the system to verify whether the same is being capitalized under the correct head and depreciation is calculated properly as per correct rate. Subsequently this dummy transaction is removed after verification of system controls.

External Sources of Information

Risk practitioner can also use external sources to gain additional insight such as:

- Computer emergency response team (CERT) advisories
- Media reports
- Report from security agencies and other concerned bodies
- Report from regulatory bodies

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answer
What is the most important metric to determine effectiveness of log monitoring?	Number of attacks investigated
Which system determines the aggregated risk from several sources?	Security information and event management (SIEM) system

Self-Assessment Questions

(1) Most useful metrics for measuring the monitoring of logs is:

A. percentage of penetration attempts investigated
B. number of logs captured
C. number of log reports generated
D. number of staffs engaged in review of logs

Answer: A. percentage of penetration attempts investigated
Explanation: Objective of capturing a log is to do follow up investigation for suspected attempts. Investigation helps to take various preventive and corrective action. Mere capturing the logs or generating the reports will not serve the ultimate purpose. Hence most useful metrics for measuring the success of log monitoring is to determine the percentage of suspected attempts investigated. If organizations do not investigate and keep only capturing the log, the ultimate objective of log capturing is not achieved.

(2) Most effective method to determine the aggregate risk from different sources is:

A. intrusion detection system
B. business impact analysis
C. security information and event management (SIEM) systems
D. gap analysis

Answer: C. security information and event management (SIEM) systems
Explanation: Most effective method to determine the aggregate risk from different sources is SIEM. Security information and event management (SIEM) system collects the data from various sources and analyzes the same for possible security events. The SIEM system has capability to detect the

attacks by signature or behavior (heuristics) based analysis. SIEM has capability for granular assessment. SIEM can highlight the developing trends and can alert the risk practitioner for immediate response.

(3) Integrated test facility (ITF) has advantage over other automated audit tools because of its following characteristics:

A. Creation of dummies/fictitious entities is not required as testing is done on actual master files.
B. ITF does not require setting up separate test environment/test processes.
C. ITF is a continuous audit tool and validates the ongoing operation of the system.
D. ITF eliminates the need to prepare test data.

Answer: B. ITF does not require setting up separate test environment/test processes.
Explanation: Fictitious entity is created in LIVE environment. As the live environment is used, there is no need to create separate test processes. However, careful planning is necessary and test data must be isolated from production data.

(4) Characteristics that BEST describes an integrated test facility:

A. Technique to verify system processing.
B. Technique to verify system integration.
C. Technique to generate test data.
D. Technique to validate the ongoing operation of the system.

Answer: A. Technique to verify system processing.
Explanation: In ITF, fictitious entities are created in a LIVE environment. Auditors can enter dummy or test transactions and verify the processing and results of these transactions for correctness. Processed results and expected results are compared to verify that systems are operating correctly. ITF does not verify system integration nor is it used to generate test data. ITF does not validate the ongoing operation of the system.

(5) Characteristics that BEST describes an integrated test facility:

A. Actual transactions are validated on an ongoing basis.
B. enables the IS auditors to generate test data.
C. pre-determined results are compared with processing output to ascertain correctness of system processing.
D. enables the IS auditors to analyse a large range of information.

Answer: C. pre-determined results are compared with processing output to ascertain correctness of system processing.
Explanation: In ITF technique, the auditor can enter dummy or test transactions and verify the processing and results of these transactions for correctness. Processed results and expected results are compared to verify that systems are operating correctly. Other options are not correct in view of ITF characteristics.

4.4 Monitoring Controls

- Implemented controls must be aligned with IT security and policies and should be reviewed at frequent intervals to determine its effectiveness, efficiency and adequacy.
- For monitoring the controls, relevant data should be gathered from various sources in a timely and accurate manner.

- Once the data is validated, analysis can be performed against specific control objectives.
- If results of the monitoring indicate an area of noncompliance or unacceptable performance, the risk practitioner should discuss with the risk owner (mostly business process owner) and recommend review of existing controls in terms of effectiveness and if require, implementation of additional controls.
- Control monitoring can be done either through independent reviewer or self- assessment by process owners.
- Following are some of the control monitoring sources:
  - Security operation centre (SOC) and network operations centre (NOC)
  - Tools and software for continuous control monitoring
  - Periodic control testing
  - Control self-assessment
- It is important to monitor the KRIs at periodic intervals as the risk profile changes over the time. Periodic monitoring helps to address the new risk and control the existing risks. For example, a product defect upto 10% is acceptable and KRI is set accordingly. However, over a period of time this 10% is considered too high owning to change in market scenario and KRI needs to be revised to set defect ratio upto only 2%.
- Risk profile provides overall risk status that the organization is exposed to. Risk profile is to be kept updated with new and emerging risk so as to ascertain organization's current risk status.
- Whenever a monitoring process identifies a security exception, the first step for a risk practitioner is to validate the exception to rule out any false positives.
- Role of a risk practitioner in the control monitoring process is to assist in planning, reporting and scheduling tests.

Continuous Monitoring System

Continuous monitoring is the process and technology used to monitor critical areas on an ongoing basis. There are various tools and techniques available for continuous monitoring. It must be noted that continuous monitoring involves cost and hence organization generally uses continuous monitoring technique for high risk areas whether impact and frequency of occurrence is high.

KRI Thresholds

Thresholds identified for monitoring and reporting of KRI is a key aspect in the monitoring process. It indicates whether controls are providing their intended value. Without appropriate thresholds, the organization may not be able to determine the effectiveness of the control.

KRI should have capability to identify the effectiveness of the controls. KRI should be able to identify when controls are no longer providing their intended value. This helps to take appropriate action on a timely basis. Without this information, an organization may be under the impression that ineffective controls are still effective and do not need to be reworked.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers

What is the first step of developing a risk monitoring program?	To conduct a capability assessment
What is the next best step once risk is accepted?	To implement monitoring technique
Risk monitoring is closely associated with	Risk reporting
What is the primary reason for monitoring key risk indicators at periodic intervals?	Risk profile changes with time
Overall risk status of the organization can be ascertained by	Risk profile of the organization
What is the first step when a security exception is noted?	To validate the exception to rule out the false positive
Continuous monitoring is more preferable for	Incidents that have high impact and high frequency
What is the most important aspect while developing a metric to monitor the control effectiveness?	Various thresholds
What is the role of a risk practitioner in the control monitoring process?	To assist in planning, reporting and scheduling tests.

Self-Assessment Questions

(1) An organization started operating in the country where identity theft is widespread. Best course of the action for the organization is to:

A. set up monitoring techniques to detect and react to fraud
B. make customer liable for fraud amount
C. make customer aware about possibility of fraud
D. outsource the process to a well-established service provider

Answer: A. set up monitoring techniques to detect and react to fraud
Explanation: Best course of action for the organization in the given situation is to set up monitoring techniques to detect and react to potential frauds. It is not possible to make customers liable for the fraud. Making customers aware about fraud is a good option but not as effective as setting up monitoring techniques. For outsourcing the process, a business case needs to reviewed and accordingly decisions should be taken. However, the most effective method will be setting up monitoring techniques to detect and react to fraud.

(2) First step of developing a risk monitoring program is:

A. to develop key risk indicator to monitor the results
B. to appoint a dedicated risk manager
C. to conduct a capability assessment
D. to gather data for calculating the key risk indicator

Answer: C. to conduct a capability assessment

Explanation: Conducting a capability assessment helps to determine the capability and preparedness of the organization to develop a risk management program. It helps to determine the maturity level of the organization managing the risk. Risk monitoring framework depends on the maturity of the organization. Other options are subsequent steps for developing a risk monitoring program.

(3) Risk monitoring is closely associated with:

A. risk analysis
B. risk reporting
C. risk mitigation
D. risk transfer

Answer: B. risk reporting
Explanation: Results of risk monitoring should be reported for appropriate action. Risk monitoring is closely associated with risk reporting.

(4) Prime objective of monitoring key risk indicator (KRI) is:

A. to minimize the cost of response
B. to minimize the error rate of key risk indicator
C. to monitor the change in risk profile
D. to improve risk assessment process

Answer: C. to monitor the change in risk profile
Explanation: It is important to monitor the KRIs at periodic intervals as the risk profile changes over the time. Periodic monitoring helps to address the new risk and control the existing risks. Risk profile provides overall risk status that the organization is exposed to. Risk profile is to be kept updated with new and emerging risk so as to ascertain organization's current risk status. For example, a product defect upto 10% is acceptable and KRI is set accordingly. However, over a period of time this 10% is considered too high owning to change in market scenario and KRI needs to be revised to set defect ratio upto only 2%. Other options are not the primary objective.

(5) Overall risk status of the organization is determined by:

A. risk analysis
B. risk response
C. risk appetite
D. risk profile

Answer: D. risk profile
Explanation: Risk profile provides overall risk status that the organization is exposed to. Risk profile is to be kept updated with new and emerging risk so as to ascertain organization's current risk status. Other options do not provide overall status of risk.

(6) Continuous monitoring is best option when:

A. there is high impact and high probability of event
B. there is low impact and low probability of event
C. there is mandate from regulation about strong information security requirements
D. primary business of the organization is e-commerce

Answer: A. there is high impact and high probability of event

Explanation: Continuous monitoring is the process and technology used to monitor critical areas on an ongoing basis. There are various tools and techniques available for continuous monitoring. It must be noted that continuous monitoring involves cost and hence organization generally uses continuous monitoring technique for high risk areas whether impact and frequency of occurrence is high.

(7) Most important aspect to identify and monitor the control life cycle is:

A. capability of threshold to identify when control fails to provide intended value
B. capability to customize the report as per senior management requirement
C. capability to provide description of methods and practices to develop metrics
D. capability to store and maintain the metrics

Answer: A. capability of threshold to identify when control fails to provide intended value
Explanation: Thresholds of the KRI should be able to indicate whether controls are providing their intended value. Without appropriate thresholds, the organization may not be able to determine the effectiveness of the control. KRI should have capability to identify the effectiveness of the controls. KRI should be able to identify when controls are no longer providing their intended value. This helps to take appropriate action on a timely basis. Without this information, an organization may be under the impression that ineffective controls are still effective and do not need to be reworked. Other options are not as significant as the ability of KRI to identify when control fails to provide the intended value.

(8) Prime role of risk practitioner is control monitoring process is:

A. to operate and maintain controls
B. to approve policy and procedure for control monitoring
C. to guide internal audit team for control monitoring
D. to assist in planning, reporting and scheduling tests of IS controls

Answer: D. to assist in planning, reporting and scheduling tests of IS controls
Explanation: Role of a risk practitioner in control monitoring process is to assist in planning, reporting and scheduling tests. Risk practitioners are not required to operate and maintain controls. Senior management is responsible for approving policy and procedure for control monitoring. Guiding internal audit teams is not the prime role of a risk practitioner.

4.5 Control Assessment Types

Risk practitioners must ensure that data analyzed for control monitoring should be complete, correct and accurate. It is important to review the data source. Data gathered directly by a risk practitioner is more reliable than data provided by a third party.

IS Audit

Role of an internal audit is to monitor, evaluate and determine the effectiveness of internal control and report the same to management and the board of directors. Recommendation from the IS auditor provides value addition for control enhancement and brings risk to the attention of management.

Risk practitioners can rely on the audit report by an independent auditor to determine the effectiveness and adequacy of the control environment. Alignment of risk management program and audit program is of utmost importance for the overall risk management program of the organization.

Periodic audit is the most effective way to ensure that third-party service providers comply with organization’s information security policy and other contractual terms and conditions.

Vulnerability Assessment

- A Vulnerability assessment is the process of identification of weakness in the system and to address the same before it is exposed or compromised by an intruder.
- Vulnerabilities can be in the form of misconfiguration or missing updates. Objective of VA is to identify these misconfigurations and missing updates.
- Identified vulnerabilities should be notified to the respective system owners for taking corrective action. System owners are responsible to ensure availability of effective and adequate control for safeguarding the system.
- A risk practitioner conducting a vulnerability assessment is required to have sufficient knowledge of the existing security environment and architecture. He should have working experience of different tools and technologies for conduct of vulnerability assessment.
- Automated tools are the best way to assess the vulnerabilities however risk practitioners should be aware about limitations of tools and always look for ways and means to identify the new and emerging risks.

Penetration Testing

- Objective of a penetration testing is to validate the findings of the vulnerability assessment. In penetration testing, the tester makes an attempt to exploit the vulnerability. If the attempt is successful, the vulnerability is real and must be addressed at the earliest. Otherwise, vulnerability may be a false positive and may not require any mitigation. This is known as white hat penetration approach wherein the tester is made aware of the vulnerabilities.
- In black hat approach, the tester is generally given no information about the control environment and he is required to gain unauthorized access to systems with the use of hacking tools and techniques.
    - To safeguard against the system failure and data compromise it is utmost important that:
    - Tester should have sufficient experience in this field
    - Scope and objective of the test should be clear and well understood by testing team
    - Test should be conducted only with management approval
    - Test should be conducted using a defined methodology and under proper oversight
- Penetration testing should be conducted at periodic intervals and also when there is major change in the systems infrastructure. Change in the infrastructure may introduce new exposures.
- Penetration testing is the best way to ensure that network security is effective and adequate.

Third-party Assurance

- Third party assurance can be in the form of certification or attestation for compliance to industry recognized standards.

- Some of the widely accepted and recognized standards and frameworks are:
    - ISO 27001
    - PCIDSS
    - COBIT 5
    - SSAE 16
- Compliance with these standards can help the organization to earn confidence of its shareholders, customers, service providers and other stakeholders.
- Certification or attestation is provided by an independent third party after evaluating the processes of the organization.
- Cloud service providers or other third party suppliers generally prefer to opt for third party assurance as it is very important to establish stakeholder confidence.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
What is the role of an Internal Audit Function?	Monitoring, evaluating, examining and reporting on controls.
What is the most effective way to ensure that third-party providers comply with organization's information security policy?	Periodic Audit
What is the prime objective of vulnerability assessment?	To identify misconfiguration and missing update
Identified vulnerabilities should be immediately notified to	System owner to take corrective action
What is the best time to perform a penetration test?	Penetration testing should be conducted at periodic intervals and also when there is major change in the systems infrastructure.
What is the most important pre-requirement before conducting a black box penetration test?	Scope and objective of the test should be clear and well understood by testing team
What is the best way to determine effectiveness of network security?	Penetration testing

Self-Assessment Questions

(1) Prime role of an internal auditor in an enterprise risk management program is:

A. to evaluate, examine and report on controls
B. to create risk awareness amongst the employees
C. to decide on risk response strategy
D. to operate overall risk management program

Answer: A. to evaluate, examine and report on controls
Explanation: Role of an internal audit is to monitor, evaluate and determine the effectiveness of internal control and report the same to management and the board of directors. Recommendation from the auditor provides value addition for control enhancement and brings risk to the attention of management.

(2) Most effective method to ensure that service provider complies with information security requirements of the organization is:

A. to provide security training to employees of the service provider
B. to conduct periodic audit of the service provider
C. to conduct external penetration test
D. to interact with management of service provider

Answer: B. to conduct periodic audit of the service provider
Explanation: Most effective method to ensure that service providers comply with information security requirements of the organization is to conduct periodic audits. Other options are not as effective as periodic audit.

(3) Best way to address the audit findings is to:

A. create a risk mitigation plan
B. create a business impact analysis
C. create an incident management plan
D. create an information security training program

Answer: A. create a risk mitigation plan
Explanation: Best way to address the audit findings is to create a risk mitigation plan. Objective of the risk mitigation plan is to take corrective action and close the audit finding.

(4) Risk associated with outsourcing can be best mitigated by:

A. conducting audit to verify compliance with agreement requirements
B. conducting annual awareness training for all employees of the service provider
C. retaining copies of outsourcing agreement till end of contract
D. analyzing the financial stability of the service provider

Answer: A. conducting audit to verify compliance with agreement requirements
Explanation: Risk associated with outsourcing can be best mitigated by conducting an audit to verify compliance with agreement requirements. Other options are not as effective as periodic audit.

(5) Prime objective of network vulnerability assessment is:

A. to identify misconfiguration and missing updates
B. to identify coding errors
C. to evaluate preparation of security team
D. to identify malware in the system

Answer: A. to identify misconfiguration and missing updates

Explanation: A vulnerability assessment is the process of identification of weakness in the system and to address the same before is exposed or compromised by an intruder. Vulnerabilities can be in the form of misconfiguration or missing updates. Objective of VA is to identify these misconfigurations and missing updates.

(6) Identified vulnerability should be immediately notified to:

A. system developer
B. system owner
C. data owner
D. risk practitioner

Answer: B. system owner
Explanation: Identified vulnerabilities should be notified to the respective system owners for taking corrective action. System owners are responsible to ensure availability of effective and adequate control for safeguarding the system.

(7) Penetration test should be best performed:

A. when there is a high staff turnover
B. when there is a major infrastructure changes
C. when there is change in risk management team
D. when there is high audit observation

Answer: B. when there is a major infrastructure changes
Explanation: Penetration testing should be conducted at periodic intervals and also when there is major change in the systems infrastructure. Change in the infrastructure may introduce new exposures.

(8) Best way to protect a corporate network from external attack is:

A. implementing an intrusion detection system
B. performing periodic penetration testing
C. enabling vendor provided configuration settings
D. defining a minimum-security baseline

Answer: B. performing periodic penetration testing
Explanation: Penetration testing is the best way to ensure that network security is effective and adequate. In penetration testing, the tester makes an attempt to exploit the vulnerability. If the attempt is successful, the vulnerability is real and must be addressed at the earliest. Penetration testing should be conducted at periodic intervals and also when there is major change in the systems infrastructure. Change in the infrastructure may introduce new exposures.

4.6 Result of Control Assessment

Effectiveness of the control monitoring program depends on following parameters:

- Accuracy of the data on the basis of which controls are evaluated
- Timely reporting on risk to management for taking corrective action
- Skill set of risk practitioner to properly evaluate the controls

Maturity Model Assessment and Improvement Techniques

- Risk management program should be a dynamic process and should evolve and improve on a continuous basis.
- Risk management programs should be improved on the basis of learnings from past events.
- Adoption of a capability maturity model (CMM) helps to indicate the maturity of the risk management process year over year.
- CMM helps an organization to understand its level of maturity by analyzing the operational effectiveness, efficiency and readiness. It provides insight into an organization's risk management capabilities.
- Maturity can be determined by analyzing the risk aware culture of the organization. Employees of a matured organization are aware about the risk of their processes and willing to resolve the same.
- With the help of the maturity model, the level of competence of the organization can be benchmarked and compared with the peers.
- Objective of adopting a maturity model is to strive for continuous improvement. This can be done by assessing the current maturity level of the business process and comparing the same with desired level. Gaps, if any, needs to be addressed to improve the process and maturity level.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
What kind of model provides insight into an organization's risk management capabilities?	Capacity maturity model (CMM)
Maturity of an organization’s risk management policy can be determined by	Risk culture and awareness of the organization
Organization can measure its risk management process against its peer by	Adoption of maturity model
Best reason to implement a maturity model	To enable continuous improvement
Best approach to determine whether existing security control is in accordance with desired level	To conduct maturity assessment/Gap Assessment

Self-Assessment Questions

Practice Questions - 4.6 Result of Control Assessment

https://criscexamstudy.blogspot.com/p/practice-questions-46-results-of.html

Flashcards - http://www.criscexamstudy.com/p/flashcards-46-result-of-control.html

(1) Enterprise's risk management capabilities can be determined by:

A. use of capability maturity model
B. determining the capability by conducting internal audit
C. self-assessing the capability
D. comparing capability with industry standards

Answer: A. use of capability maturity model
Explanation: Adoption of a capability maturity model (CMM) helps to indicate the maturity of the risk management process year over year. CMM helps an organization to understand its level of maturity by analyzing the operational effectiveness, efficiency and readiness. It provides insight into an organization's risk management capabilities. Other options are not as effective as the capability maturity model.

(2) High maturity of organization's risk management process can be determined by:

A. risk aware culture
B. high security budget
C. frequent internal audits
D. frequent penetration testing

Answer: A. risk aware culture
Explanation: Maturity can be determined by analyzing the risk aware culture of the organization. Employees of a matured organization are aware about the risk of their processes and willing to resolve the same.

(3) An organization wants to measure its risk management process against its peers. Organization should:

A. adopt the internal audit best practices
B. adopt the balance score card
C. adopt the maturity model
D. adopt appropriate risk assessment methodology

Answer: C. adopt the maturity model
Explanation: Adoption of a capability maturity model (CMM) helps to indicate the maturity of the risk management process year over year. CMM helps an organization to understand its level of maturity by analyzing the operational effectiveness, efficiency and readiness. It provides insight into an organization's risk management capabilities. With the help of the maturity model, the level of competence of the organization can be benchmarked and compared with the peers.

(4) Prime reason for adopting a maturity model for risk management is:

A. to reduce the security budget
B. to align business and IT objectives
C. to ensure effectiveness of security controls
D. to strive for continuous improvement

Answer: D. to strive for continuous improvement
Explanation: Objective of adopting a maturity model is to strive for continuous improvement. This can be done by assessing the current maturity level of the business process and comparing the same with desired level. Gaps, if any, needs to be addressed to improve the process and maturity level.

(5) Best method to determine whether existing security framework meets the organization needs is:

A. to conduct a control self-assessment
B. to compare security test results
C. to capture security logs
D. to conduct a process maturity assessment

Answer: D. to conduct a process maturity assessment
Explanation: Best method to determine whether an existing security framework meets the organization's needs is to conduct a process maturity assessment. This can be done by assessing the current maturity level of the business process and comparing the same with desired level. Gaps, if any, needs to be addressed to improve the process and maturity level. Other options are not as effective as process maturity assessment.

4.7 Changes to IT Risk Profile

- Risk practitioners should ensure that the risk profile of the organization should be evaluated at periodic intervals to determine the changes to the risk profile.
- Risk profile may change on account of following factors:
    - Implementation of new technologies
    - Changes in business processes
    - Changes in regulatory requirements
    - Changes in market demand and customer requirements
    - Changes in competitor's policy
- Risk profile of an organization may be affected by the cascading effects of minor changes.
- With change in risk profile, objectives and goals of the risk management process should be reviewed to ensure that they continue to be aligned with the goals and objectives of the organization.
- Changes in the organization's risk profile is to be updated in the risk register. Risk registers should be able to provide status of the organization's current risk profile.
- Primary reason to determine the changes is the risk profile is to evaluate whether additional response is required to reduce the risk.
- Risk profile of the organization changes over the time. Periodic monitoring of key risk indicators proactively identifies the changes in the risk profile. Once changes are identified, additional controls can be implemented to keep the risk within the appetite.

Key aspects from CRISC exam perspective

CRISC Questions	Possible Answers
Which is the best document to identify changes in an organization's risk profile?	Risk register
What are the primary reasons to determine the changes in the risk profile?	● To determine if additional response is required

	● To enable educated decision making
What is the primary reason for periodically monitoring key risk indicators?	Risk profile may have changed

Self-Assessment Questions

(1) Changes in organization’s risk profile can be identified by:

A. reviewing the internal audit report
B. reviewing the risk response analysis
C. reviewing the risk register
D. reviewing the risk classification

Answer: C. reviewing the risk register
Explanation: Risk practitioners should ensure that the risk profile of the organization should be evaluated at periodic intervals to determine the changes to risk profile. Changes in the organization’s risk profile is to be updated in the risk register. Risk registers should be able to provide status of the organization’s current risk profile. Other options will not be able to provide accurate details about changes in the organization’s risk profile.

(2) Main reason for reporting significant change in risk profile to senior management is:

A. to update management about current IT inventory
B. to update management about probability and impact of each risk
C. to update management about budget for security investment
D. to update management about current risk profile

Answer: D. to update management about current risk profile
Explanation: Risk profile of the organization changes over the time. Significant changes should be reported to senior management so that they can be aware of the current risk profile of the organization. This will help the senior management to determine whether additional response is required to reduce the risk.

(3) Prime reason for monitoring key risk indicator (KRI) on periodic basis is:

A. to ascertain whether cost of risk is to be minimized
B. to ascertain whether error is KRI is to be minimized
C. to ascertain whether risk profile have been changed
D. to ascertain whether internal audit is effective

Answer: C. to ascertain whether risk profile have been changed
Explanation: Risk profile of the organization changes over the time. Periodic monitoring of key risk indicators proactively identifies the changes in the risk profile. Once changes are identified, additional controls can be implemented to keep the risk within the appetite. Other options are not the prime reason for monitoring KRI on a periodic basis.

(4) Significant change in organization’s risk profile is reported to senior management:

A. to enable senior management monitor cost of control
B. to enable senior management take educated decisions
C. to enable senior management approve security budget
D. to enable senior management understand value of existing information assets

Answer: B. to enable senior management take educated decisions
Explanation: Risk profile of the organization changes over the time. Significant changes should be reported to senior management so that they can be aware of the current risk profile of the organization. This will help the senior management to determine whether additional response is required to reduce the risk.