ISACA CRISC® - Quiz Questions with Answers

Domain 1: Governance

1.

Who is the primary individual ultimately responsible and accountable for how risk is addressed?

- **Risk owner**
- Risk analyst
- Risk manager
- Control steward

Correct answer: Risk owner

The risk owner has the bottom-line accountability for the enterprise risk program. This individual works with other stakeholders and experts to implement the program.

The risk analyst analyses, evaluates, and assesses threats.

The risk manager is responsible for ensuring that risk management functions are being carried out.

The control steward is responsible for routine management and maintenance of controls.

2.

Under what circumstances might an organization choose **NOT** to be compliant with certain laws and regulations?

If the cost of compliance is greater than the consequences

If only a small percent of their business comes from those countries

If the cost of compliance brings the risk appetite lower

If the cost of compliance nullifies the requirements of compliance

---

Correct answer: If the cost of compliance is greater than the consequences

Compliance is a risk decision. Every organization has a risk appetite that is set by senior management. Depending on the penalties, an organization may willingly choose not to invest in compliance because the cost of doing so far outweighs the penalties. However, it's important to note that choosing not to comply with laws and regulations can pose legal, financial, reputational, and operational risks to the organization, and such decisions should be made carefully and with full consideration of the potential consequences.

The statement that the cost of compliance has any effect on risk appetite is nonsensical. Risk appetite is the amount of risk that an entity is willing to accept in pursuit of its mission. It is necessary to manage risk within the appetite, and that could include being in compliance, or not. Attempting to circumvent compliance requirements through lobbying may be unethical and potentially illegal. Being in compliance with laws and regulations does not nullify the requirement of compliance; it fulfills the requirement of compliance.

3.

Which risk management policy sets the guidelines for protecting corporate information and includes underlying infrastructure and supporting systems?

Information security policy

Privacy policy

Risk appetite/tolerance policy

Risk mitigation policy

Correct answer: Information security policy

An information security policy addresses the protection of all corporate data. Because data is stored on infrastructure and flows through the network from system to system, the school of information security policy also includes the underlying supporting infrastructure and systems.

Privacy policies focus primarily on the protection of personal data.

Risk appetite/tolerance policies define the organization's acceptance level of risk, not the specific controls to mitigate it.

Risk mitigation policies outline strategies to reduce risk, but do not encompass the overall protection of information systems.

4.

Asset valuation is the process by which the risk management program calculates the value an asset provides. The outcome of this calculation can be expressed either quantitively or qualitatively.

Which risk scenario is concerned with the value an asset brings to an organization's credibility?

Damage to reputation

Breach of contract

Violation of privacy

Legal noncompliance

Correct answer: Damage to reputation

Damage to reputation impacts an organization's brand. A strong brand is a competitive advantage that has a significant financial impact. When valuing assets that are used to develop and maintain an organization's brand, the risk management program would be concerned about potential damage to reputation.

While a breach of contract can certainly have financial and reputational consequences, it is primarily concerned with the failure to meet the terms agreed upon in a legal contract rather than the organization's credibility.

Violation of privacy pertains to the failure in protecting personal or sensitive information per legal or regulatory standards.

Legal noncompliance involves failing to adhere to laws and regulations governing the organization's operations.

5.

What is an example of an organizational measure that adjusts policies, processes, or procedures to reduce risk to an acceptable level?

Data retention

Encryption

File monitoring

Firewalls

Correct answer: Data retention

Data retention is a policy that determines how long an organization will keep and store its data. The longer data is stored, the larger the data volume is. This creates a situation where there could be a large amount of confidential information being stored. If there is a data breach, this would create a high risk to the organization.

Encryption, file monitoring, and firewalls are considered technical controls rather than organizational measures.

6.

If an organization wants to mandate the way their staff complies with risk policies, what can they use or refer to in order to accomplish this?

Standards

Best practices

Guidelines

Regulations

Correct answer: Standards

A risk standard is a mandatory requirement, code of practice, or specification that is established and recognized by an external standards organization. External standards organizations are typically specific to an industry and have the background and credibility to create standards that organizations should follow.

Best practices are recommendations based on industry experience that suggest the most efficient way to achieve a goal but are not mandatory.

Guidelines provide general advice or recommendations on how to perform a task but are usually not enforceable.

Regulations are laws or rules set by a governing body that organizations must comply with.

7.

Governance frameworks establish accountability to protect which aspect of an organization?

Assets

Employees

Policies

Board of Directors

Correct answer: Assets

Assets are the tangible and non-tangible resources that an organization uses to conduct operations. Governance and accountability ensure that these assets are accounted for and leveraged according to business guidelines.

Governance frameworks might have policies that affect employee behavior, although the primary focus of governance is not directly on protecting employees but on overseeing overall management.

Governance frameworks include policies, but they do not primarily exist to protect the policies themselves. They establish policies to protect the organization's assets.

Governance frameworks ensure that the Board of Directors fulfills its duties, but they do not exist primarily to protect the Board itself.

8.

Who is responsible for setting the risk appetite of an organization?

Senior management

Middle management

Risk manager

Subject matter experts

Correct answer: Senior management

Setting the risk appetite of an organization is part of the strategic planning process. Therefore, senior management is responsible for this task.

Middle management is responsible for managing risks within their areas of responsibility according to the risk appetite set by senior management, but they do not typically set the risk appetite.

The risk manager is responsible for overseeing the risk management process, ensuring that risks are identified, assessed, and managed, but they do not typically set the risk appetite.

A subject matter expert provides specialized knowledge on specific risks but does not set the overall risk appetite for the organization.

9.

What is the **MAIN** focus of a high-level risk policy versus a functional risk policy?

To determine the approach of the enterprise toward risk management

To establish specific risk category classifications

To set guidelines related to the acceptable use of organizational resources

To outline detailed steps necessary to carry out the day-to-day risk management activities

---

Correct answer: To determine the approach of the enterprise toward risk management

High-level risk policies establish overarching principles, objectives, and strategic direction for risk management across the organization. They outline the enterprise's overall risk appetite, tolerance, and desired risk management culture. These policies provide guidance on how risk should be identified, assessed, mitigated, and monitored at a broad organizational level.

Specific risk category classifications is more detailed and typically found in functional risk policies.

Acceptable use of resources to risk management is usually covered in separate policies, like IT usage or security policies.

Day-to-day risk management activities are outlined in operational procedures and guidelines, not high-level policies.

10.

During a risk management business process review, it is important to classify processes by criticality. What additional information do you need to gather for each process?

Process responsibility and accountability

Process duration

Process cost

Process transfer time

Correct answer: Process responsibility and accountability

In addition to understanding what risk management processes are implemented, it is equally important to identify who is establishing those processes and who is executing them. The reason for gathering this additional level of information is to ensure that the right people (subject matter expertise and role of the organization) are assigned to the processes.

The important element to think about here is that the question is asking about risk management review. The process duration, cost, and possible transfer time are less critical or subtopics that can be discussed but would be discussed with the person who is responsible and the person who is accountable.

11.

What process needs to be in place to ensure that risk management is aligned with the enterprise's goals and objectives?

Governance

Management

Monitoring

Regulation

Correct answer: Governance

Governance is the process of overseeing the direction and execution of activities and/or a program. Governance is essential to risk management execution to ensure that it is following the enterprise's overall goals.

Management refers to the daily operations and execution of tasks, such as risk management.

Monitoring is the process of continually tracking and evaluating risk management activities.

Regulation refers to external rules and laws that organizations must comply with.

12.

A company has entered into a long-term contract with a major supplier for the purchase of a critical component. The supplier is facing financial difficulties, and there is a risk that they may be unable to fulfill their obligations under the contract.

What type of risk is the company facing?

Credit

Market

Operational

Compliance

Correct answer: Credit

A credit risk is the risk of financial loss due to the failure of a counterparty to meet their contractual obligations. In this scenario, the company is facing the risk that the supplier may default on their contract and not deliver the critical component.

Market risk involves exposure to changes in market conditions like price fluctuations, which is unrelated to the supplier's financial issues.

Operational risk pertains to risks arising from internal processes or systems, not the failure of a third-party supplier.

Compliance risk relates to the company failing to adhere to laws or regulations, which is not the core issue here.

13.

An insurance company is undergoing a major restructuring that involves consolidating multiple business units and implementing new technologies. The risk management team wants to ensure that risk management becomes a fundamental part of the organization's decision-making processes and that all employees are aware of their role in managing risks.

What is the primary risk governance objective of the risk management team in this situation?

Integrating risk management into the enterprise

Making risk-aware business decisions

Establishing and maintaining a common risk view

Ensuring that risk management controls are implemented and operating correctly

---

Correct answer: Integrating risk management into the enterprise

The primary objective of the risk management team in this scenario is to integrate risk management into the enterprise. This means ensuring that risk management is considered at all levels of the organization and is embedded into the decision-making process.

Making risk-aware business decisions is an outcome of effective risk management but is not involved in integrating risk management into the enterprise.

Establishing and maintaining a common risk view is more of a side activity rather than embedding risk management into the organization.

Ensuring that risk management controls are implemented and operating correctly is primarily an operational aspect rather than integrating risk management into the organization.

14.

As it relates to risk management, there are three lines of defense. Which line of defense is concerned with the compliance function?

Second line

First line

Third line

All lines

Correct answer: Second line

The second line of defense is typically composed of risk management and compliance functions. The expectation of these functions is to ensure that the individual business functions are acting in compliance with the overall risk management program.

The first line of defense is operational management. Operational management includes implementing risk management policies and executing an effective internal control.

The third line of defense is the audit function. Auditing involves independent and objective review of the control environment.

15.

Which personnel role within the risk management function is tasked with ensuring that the risk management functions are carried out?

Risk manager

Risk analyst

Risk steward

Subject matter expert

Correct answer: Risk manager

The risk manager manages and understands the overall risk management functions that need to be accomplished within the enterprise. This individual is responsible for ensuring that the risk management functions are carried out by the people in the department.

A risk analyst is responsible for analyzing, evaluating, and assessing threats.

A risk steward is responsible for the routine management and maintenance of controls.

A subject matter expert provides insights into specific areas.

16.

As it relates to risk management three lines of defense, which line of defense is responsible for monitoring and reporting the enterprise's current risk profile exposure to appropriate stakeholders?

Second line

First line

Third line

Fourth line

Correct answer: Second line

The second line of defense includes the portion of the organization that is responsible for monitoring the overall risk profile, posture, and exposure. Based upon this ongoing monitoring, the second line of defense is communication with stakeholders and executives on the steps of the program.

ISACA has three lines of defense in their governance section of the CRISC manual. The first line is operational management, the second line is risk and compliance functions, and the third is audits. There is no fourth line in this logic.

17.

From an enterprise perspective, what term is used to describe "a challenge to achieving objectives"?

Risk

Governance

Threat

Vulnerability

Correct answer: Risk

Risk is a known challenge to achieving a stated outcome. In and of itself, it is not deemed to be positive or negative until analysis is complete.

Governance refers to the frameworks, policies, and processes that guide and control an organization's operations and decision-making.

A threat is a potential event that could exploit vulnerabilities and cause harm to an organization.

A vulnerability is a weakness in a system that can be exploited by threats.

18.

A company is conducting a comprehensive review of its risk management practices. They want to understand the overall level of risk the organization is currently exposed to, including the types of risks, their likelihood, and potential impact.

What are they trying to define?

Risk profile

Risk appetite

Risk posture

Risk capacity

Correct answer: Risk profile

A risk profile is a comprehensive assessment of an organization's risk exposure, including the types of risks, their likelihood, and potential impact. It helps an organization understand its risk exposure and make informed decisions.

Risk appetite is the level of risk an organization is willing to accept.

Risk posture is the current state of an organization's risk management practices.

Risk capacity is the maximum amount of risk an organization can absorb without facing financial distress.

19.

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

What type of asset represents all the equipment, devices, and systems components that are the critical foundation for an organization to deliver sustained performance?

Technology

Software

Data

Network

Correct answer: Technology

Technology is a broad asset that includes hardware and software. This includes equipment that is critical to running the business but is not computer-related. For technology to be most effective, it must be maintained, patched and upgraded, refreshed, and well-documented. Not staying on top of these requirements introduces risk.

Software does not include the physical component.

Data represents information but is not tied to equipment or devices.

Network involves the infrastructure for communications but is a subset of technology.

20.

A large corporation has been hit by major attacks. They have determined that they need to add a new tool to their network, a Database Activity Monitor, as one of their actions to combat this new attack type they have experienced.

Which step in the risk management lifecycle are they in?

Risk response and mitigation

Risk identification

Risk assessment

Risk monitoring and reporting

Correct answer: Risk response and mitigation

Once a risk has been assessed and categorized, its potential impact can be understood in more detail. At this point, risk response and mitigation activities are put in place to reduce the impact of the risk to the enterprise. This is where there are four options: risk avoidance, risk acceptance, risk transfer, and risk reduction. Adding a tool to the network is a type of risk reduction.

Risk identification is the step in which risks are recognized or identified. The risk assessment step involves evaluating the risks' likelihood and potential impact on the organization and prioritizing them based on their severity. The risk monitoring step in the risk management lifecycle involves continuously observing and analyzing the risk landscape to identify new risks and evaluate the effectiveness of implemented risk mitigation strategies.

21.

Your organization wants to examine its effectiveness and efficiency in responding to risk.

What type of review should you recommend?

Business process review

Risk tolerance review

Risk taxonomy review

Risk communication review

Correct answer: Business process review

A business process review examines in detail all the steps that an organization is taking when dealing with risks. This includes the entire end-to-end process, starting with risk identification all the way through addressing the risk and monitoring the results.

A risk tolerance review focuses on assessing the level of risk an organization is willing to accept.

A risk taxonomy review involves categorizing and classifying risks to ensure a common understanding across the organization.

A risk communication review examines how risk-related information is communicated within the organization.

22.

If an organization is global, how can the risk program be structured to handle the laws and regulations of the various jurisdictions they operate in from a single point of accountability?

Centralized global program

Decentralized regional program

Outsourced risk management program

Decentralized global program

Correct answer: Centralized global program

To drive consistency and set the expectation that risk must be managed across the enterprise, the best practice for global organizations is to centralize the risk management program at the enterprise level. Global policies can be implemented for each jurisdiction and specific regional guidelines can be incorporated.

A decentralized regional program can suffer from a lack of a central vision for risk management.

An outsourced risk management program could stray too far from the organization's central plan.

A decentralized global program would give each branch its own authority to define its program.

23.

Which personnel role in the risk management function has detailed knowledge of specific risk areas in an organization?

Subject matter expert

Risk manager

Risk analyst

Risk executive

Correct answer: Subject matter expert

A subject matter expert has focus and knowledge and insight into specific areas within an organization. They understand and can identify threats and risks. They are a very valuable resource to other members of the risk management function.

A risk manager is responsible for ensuring risk functions are carried out.

A risk analyst is responsible for analyzing, evaluating, and assessing threats.

A risk owner is accountable for making risk-based decisions.

24.

A risk practitioner has been working through the process of assessing and managing risk. What is the correct order of the IT risk management life cycle?

IT risk identification, IT risk assessment, Risk response and mitigation, Risk and control monitoring and reporting

IT risk assessment, IT risk identification, Risk response and mitigation, Risk and control monitoring and reporting

IT risk identification, IT risk assessment, Risk and control monitoring and reporting, Risk response and mitigation

IT risk identification, Risk response and mitigation, IT risk assessment, Risk and control monitoring and reporting

---

Correct answer: IT risk identification, IT risk assessment, Risk response and mitigation, Risk and control monitoring and reporting

Risk management is the framework and set of ongoing activities that predicts challenges, analyzes them, and takes action to lower the chance of a risk taking place. If it does, risk management mitigates the impact.

The first step is to identify the potential IT risks the organization may face. Once risks are identified, an assessment can then be performed. This would include quantitative and qualitative methods. Once the potential cost or the amount of damage is identified, the risk can then be mitigated. The mitigation is the response to the potential risk. This includes the four options of risk avoidance, risk transfer, risk reduction, and then, risk acceptance. It is necessary to continue monitoring the IT environment. Threats and attackers can change on a daily basis.

25.

What is the function and role of business continuity?

Enable an enterprise to survive during an adverse event

Enable an enterprise to function after a merger

Enable an enterprise to return to normal IT operations after an incident

Enable an enterprise to revert to an earlier system after a failed upgrade

---

Correct answer: Enable an enterprise to survive during an adverse event

Business continuity is defined as the uninterrupted operations of an organization. The business continuity function is responsible for developing and testing plans to simulate business and external events that could interrupt business operations. For example, if a natural disaster occurs and takes out a data center, business continuity ensures that the business is able to continue normal operations out of an alternate facility.

Enabling an enterprise to function after a merger is an issue related to change management and integration planning.

Enabling an enterprise to return to normal operations after an incident is an issue related to disaster recovery.

Enabling an enterprise to revert to an earlier system after a failed upgrade is an issue related to change management.

26.

In simple terms, how is risk defined in ERM?

As a challenge to achieving objectives

As a magnitude of loss resulting from a threat exploiting a vulnerability

As a method to achieving objectives

As an imminent violation of computer security policies

Correct answer: As a challenge to achieving objectives

Risk represents uncertainty and unknowns. This is why risk creates a challenge to achieving objectives because the path to completion is not clear. Risk is not necessarily bad. It is defined as a challenge and an unknown, which can ultimately turn into an enabler.

Impact is a magnitude of loss resulting from a threat exploiting a vulnerability.

Governance is a method to achieving objectives.

An incident is a violation or imminent violation of computer security policies.

27.

Which of the following organizational attributes signifies a risk culture that is reactive?

Superficial incident investigation

Legal compliance

Regularly scheduled lessons learned

Active monitoring and reporting

Correct answer: Superficial incident investigation

Organizations that are reactive have minimal risk processes. They have not embraced risk management as the central part of their business operations or invested in it. Consequently, their approach to risk is high level and typically not proactive.

A compliance-driven culture focuses on legal compliance.

A proactive culture has regularly scheduled lessons learned.

A resilient culture has active monitoring and reporting.

28.

Which characteristic of an IT risk management program means that it can be reviewed by an independent third party?

Auditable

Justifiable

Complete

Enforced

Correct answer: Auditable

An auditable risk management program has thorough and transparent documentation. This allows auditors to understand how the program is constructed, examine how risk is managed in the organization, and evaluate the effectiveness of the overall program.

While it's important for risk management decisions to be justifiable, meaning they are based on sound reasoning and analysis, this does not necessarily imply that the program is reviewable by an independent third party.

While completeness is essential for the effectiveness of the risk management program, it does not directly relate to whether the program is reviewable by an independent third party.

Enforcing policies and procedures alone does not guarantee that the risk management program is reviewable by an independent third party.

29.

Using the RACI model, which role identifies the individual who is liable for the completion of a risk management task?

Accountable

Consulted

Informed

Responsible

Correct answer: Accountable

Individuals who are accountable are liable for the completion of the task. They oversee and manage individuals who are responsible for performing the task. However, ultimately, it is their accountability that ensures that the tasks are done well and according to specifications.

Consulted parties are those whose opinions are sought, typically subject matter experts.

Informed parties are those who are kept up-to-date on progress, often only on the completion of the task or deliverables, and with whom there is just one-way communication.

Responsible parties refer to the person or team members who actually do the work to achieve the task or deliverable but are not ultimately liable for it.

30.

Which personnel role in the risk management function has the authority and accountability for making risk-based decisions?

Risk owner

Risk analyst

Risk manager

Subject matter expert

Correct answer: Risk owner

The risk owner is the individual the enterprise has given the authority and accountability for making risk-based decisions. This individual also owns the loss that would be associated with a realized risk scenario.

A risk analyst is responsible for analyzing risks and providing insights to support decision-making, but they do not have the authority to make final decisions.

A risk manager oversees the overall risk management process, but may not have the authority to make final decisions.

A subject matter expert provides specialized knowledge and advice on particular aspects of risk, but they do not usually have the authority to make risk-based decisions.

31.

A pharmaceutical company has identified several potential security risks that could impact its operations. Now, the management team needs to decide which risks require immediate action, which can be tolerated, and which should be prioritized.

What phase of the information security risk management process is the company currently in?

Risk evaluation

Risk analysis

Risk treatment

Risk acceptance

Correct answer: Risk evaluation

The company is in the risk evaluation phase, where it determines the acceptability of the identified risks, prioritizes them, and decides on the appropriate course of action for each.

Risk analysis involves assessing the likelihood and impact of identified risks, which is a step that precedes risk evaluation.

Risk treatment refers to the process of implementing strategies to handle risks, such as mitigating, transferring, or avoiding them.

Risk acceptance is the decision to tolerate a risk without taking any further action.

32.

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

What type of asset contains detailed information about the buyers and revenue sources of an organization?

Customer lists

Industry catalogs

General ledger

Sales run books

Correct answer: Customer lists

Customer lists contain information about those who purchase products and services. This information is valuable because it typically includes buying preferences, purchase history, relationship management encounters, and sales campaign information. If this information fell into the hands of a competitor or was compromised in any way, it would be very detrimental.

Industry catalogs contain information about products or services offered within a particular industry but do not specifically provide information about an organization's buyers or revenue sources.

A general ledger is a financial record that contains all the financial transactions of an organization but does not directly contain details about buyers or customers.

Sales run books are guides or manuals that outline processes and strategies for sales teams but do not contain specific information about buyers or revenue sources.

33.

Why is it important to put a governance framework around risk management functions?

To align enterprise and risk strategy

To employ government regulators

To make sure there is not too much oversight

To drive the technology specifications

Correct answer: To align enterprise and risk strategy

Ultimately, risk management functions need to support the organization's goals and regulatory objectives. Aligning enterprise and risk strategy ensures that risk management activities are integrated into the organization's overall strategic objectives and decision-making processes. This alignment enables the organization to identify, assess, and manage risks in a manner that supports and enhances its long-term goals and objectives, contributing to improved performance and resilience.

Employing government regulators may be necessary in some industries to ensure compliance with regulations, but it is not the primary purpose of implementing a governance framework around risk management functions.

While avoiding excessive oversight is important to prevent bureaucracy and inefficiencies, it is not the primary goal of implementing a governance framework around risk management functions. The main purpose is to establish appropriate oversight mechanisms that ensure accountability, transparency, and effective risk management practices throughout the organization.

While technology specifications may be influenced by risk management considerations, driving technology specifications is not the primary purpose of a governance framework for risk management functions.

34.

An effective way to ensure compliance to an organization's ethics policy is to require employee attestation.

What is the best practice for when employee ethics attestation should take place?

Annually

At the exit interview

During onboarding training

Every 5 years

Correct answer: Annually

Attestation is the process of certifying something. Organizations have processes such as training, performance reviews, and data privacy that employees review annually. Adding ethics attestation to that annual cycle is an industry best practice.

Attestation at the exit interview does not help maintain ongoing compliance or reinforce ethical standards for current employees.

Attestation during onboarding does not ensure continued adherence as employees grow within the organization.

A five-year interval is too infrequent to effectively maintain ongoing awareness and compliance with the ethics policy.

35.

A food delivery company is working on a thorough review of its business processes. The team has made updates to their processes and now wants to assess the effectiveness of the updates and identify areas for improvement. They are now conducting interviews with employees and analyzing system usage data.

Which of the following **BEST** describes the step in the business process review cycle that they are in?

Feedback and evaluation

Schedule and implement changes

Document and evaluate current business processes

Customer feedback

Correct answer: Feedback and evaluation

The team's current focus on assessing the effectiveness of the updates they've made to their systems and gathering insights through employee interviews and system usage data is part of feedback and evaluation.

Scheduling and implementing changes has already been done in this situation since the team has made updates to their systems.

Identifying potential changes occurs before implementing changes.

Documenting and evaluating current business processes occurs at the beginning of the business process review.

36.

Which personnel role in the risk management function is responsible for the routine management and maintenance of controls?

Control steward

Control owner

Risk manager

Risk owner

Correct answer: Control steward

A control steward is responsible for the ongoing management and maintenance of controls. This individual gets their direction from the control owner and institutes changes at the direction of the control owner.

The control owner is accountable for the design and implementation of controls.

The risk manager is responsible for ensuring that risk management functions are carried out correctly.

The risk owner is responsible for analyzing, evaluating, assessing, and making decisions upon threats to the enterprise.

37.

What is the relationship between IT risk and business risk?

IT risk is a subset of business risk

Business risk is a subset of IT risk

There is no relationship; they are separate and distinct

They are the same

Correct answer: IT risk is a subset of business risk

IT exists to enable and accelerate business operations. Without a business structure, there is no need for IT. This means that any IT risk has a direct impact on the business and must be evaluated in the context of how the business is going to be affected.

Without a business structure, there is no need for IT, so it isn't accurate to say that business risk is a subset of IT risk.

There is a relationship because as IT dependence has grown, IT risk has become a critical part of business risk.

IT risk and business risk are not exactly the same because there are business risks that exist that have no relationship to IT risk.

38.

What is the term for "acceptable level of variation that management is willing to allow for a specific risk"?

Risk tolerance

Risk appetite

Risk aversion

Risk aggregation

Correct answer: Risk tolerance

Risk tolerance is the ability to handle volatility and losses. To maintain control of the overall organizational risk profile, risk variation is typically evaluated and tolerated at the individual policy or initiative level.

Risk appetite refers to the overall amount of risk an organization is willing to take on to achieve its objectives.

Risk aversion indicates a preference to avoid risk, usually implying a lower tolerance for risk.

Risk aggregation involves combining individual risks to understand their overall impact on the organization.

39.

Risk practitioners continually monitor a wide variety of risk indicators. All the following are examples of risk indicators **EXCEPT**:

Existing assets

New assets

Changes to business operations

Legal changes

Correct answer: Existing assets

Existing assets have already been accounted for in the risk program. If they are replaced, upgraded, or decommissioned, then the appropriate action would be taken by the risk practitioner.

When monitoring risk, one of the critical things to look for is changes. The three wrong answers are all changes to the environment, or could be. New assets may be identical to ones that the business already has and do not change the risk profile much, but, at the same time, they could be different from anything they already have.

When the operations of the business change, there are many possible things that could mean. Again, here, it could be very different from how the business has been operating.

Legal changes could be new laws, such as the fairly recent European Union General Data Protection Regulation (EU GDPR) or the California Consumer Privacy Act (CCPA).

40.

Which of the following characteristics is representative of a compliance-driven risk culture?

Periodic testing

Superficial incident investigations

Ad hoc training

Communication on a need-to-know basis

Correct answer: Periodic testing

A compliance risk culture is one that has legal and monetary consequences if risk is not managed in a comprehensive and disciplined manner. Examples of organizations that have a compliance risk culture are those in heavily regulated industries such as financial services, healthcare, or environmental.

Superficial incident investigations is characteristic of a vulnerable risk culture.

Ad hoc training and communication on a need-to-know basis are characteristic of a reactive risk culture.

41.

How should an enterprise address the risk of employees engaging in unethical activities?

By having senior management communicate the policy to all employees equally

By allowing employees to make ethical decisions on their own accord based on their previous experiences

By having a copy of an ethics manual posted in a common area where all employees can view it

By assigning an ethics manager in each department who can help each employee make the right choices at all times

---

Correct answer: By having senior management communicate the policy to all employees equally

Ethics is an important aspect of risk management. Clearly conveying the organization's ethical standards from the top down establishes a strong ethical foundation.

Employee autonomy is important, but providing clear guidelines through policy communication is essential.

Ethics manual accessibility is not as effective as direct communication from leadership.

An ethics manager can be a valuable resource, but the primary responsibility for setting ethical expectations lies with senior management.

42.

What is the purpose of a risk program management audit function?

Demonstrate that controls and proactive practices are in place

Demonstrate that a business can survive an adverse event

Demonstrate that the risk management programs are fully documented

Demonstrate that risk management teams are trained on industry compliance

---

Correct answer: Demonstrate that controls and proactive practices are in place

The audit function provides the organization, as well as external stakeholders and regulatory bodies, with assurances that the risk management program is effective. This is accomplished by conducting a comprehensive, objective review of the risk program that includes people, process, and technology.

A demonstration of the completeness of the documentation of the risk management program would not show just how complete the program is. Especially in comparison to the correct answer of demonstrating that the controls are in place.

Demonstrating the knowledge and skill level of the risk management team would be useful, but it does not show that the risk program management is actually being performed.

Testing the disaster recovery plan would provide information to management about their ability to survive an adverse event.

43.

What is the term for "the amount of risk that an entity is willing to accept in pursuit of its mission"?

Risk appetite

Risk tolerance

Risk capacity

Risk management

Correct answer: Risk appetite

The term risk appetite means the amount of risk an enterprise is willing to take before it puts actions in place to reduce the risk. Risk appetite can be higher or lower than risk capacity.

Risk tolerance is the acceptable level of variation that management is willing to allow for a specific risk.

Risk capacity is the maximum level of risk an organization can bear without jeopardizing its ability to achieve its objectives.

Risk management is the overall process of identifying, assessing, and controlling risks to an organization.

44.

A risk manager at an AI company is faced with a situation where they must decide whether to disclose a potential conflict of interest that could impact a project.

Which of the following **BEST** describes the principles that guide the risk manager's decision-making process in this scenario?

Professional ethics

Compliance

Risk appetite

Contractual requirements

Correct answer: Professional ethics

Professional ethics guidelines require the disclosure of conflicts of interest. That helps to ensure unbiased decision-making and integrity within the company.

Compliance refers to adhering to laws, regulations, and standards, but disclosing conflicts of interest is more closely related to ethical responsibility than regulations.

Contractual requirements may contain provisions for handling conflicts, but this situation is driven more by ethical principles.

Risk appetite refers to the level of risk an organization is willing to accept, which is unrelated to the ethical decision of disclosing conflicts of interest.

45.

What is the main purpose of risk policies?

Provide direction regarding acceptable and unacceptable behaviors as it relates to risk

Provide direction regarding acceptable and unacceptable technologies that can be implemented

Provide direction regarding acceptable and unacceptable training that employees should take

Provide direction regarding acceptable and unacceptable risk investments

---

Correct answer: Provide direction regarding acceptable and unacceptable behaviors as it relates to risk

Risk policies are designed to outline specific expectations and behaviors for all operations of the business. Typically, these policies are part of employee training and require an annual refresh to ensure that every employee understands their accountability to the organization's risk practices.

Providing direction regarding acceptable and unacceptable technologies that can be implemented may be influenced by risk policies, but the main focus of risk policies is on behaviors and practices related to risk management.

Providing direction regarding acceptable and unacceptable training that employees should take is usually outlined in training or development policies.

Providing direction regarding acceptable and unacceptable risk investments would be guided by investment policies or strategies.

46.

When projects fail, they bring business, financial, and technical risk to an organization. Which of the following is **NOT** an example of why a project may be considered a failure?

Instituting change requests

Surpassing the allotted budget

Not meeting scheduling deadlines

Not meeting customer expectations

Correct answer: Instituting change requests

A project is considered to be a failure when it does not meet its baseline objectives. This includes budget, schedule, and end-user outcomes. During the course of project delivery, a change request to any of these parameters can be approved by the accountable stakeholder. If the project team delivers against the new objectives, then it would be considered a success.

A change request is a normal process that occurs in information security, information technology, projects, etc. A change request could be a reason for success, depending on the change and the effects of that change.

47.

What is the name of the model used to outline the roles and responsibilities of various stakeholders in an organization and to clearly show the relationships and interactions between the stakeholders?

RACI

Three Lines of Defense

COSO

ISO 31000

Correct answer: RACI

The RACI model helps clarify who is responsible for what within an organization for specific projects, processes, or tasks. The letters in RACI mean the following:

- ***R** = Responsible, which is those who do the work.*
- ***A** = Accountable, which are those who are answerable for the end result.*
- ***C** = Consulted, which are those whose opinions or subject matter expertise is sought out.*
- ***I** = Informed, which are those who are kept up to date.*

The Three Lines of Defense model delineates the roles and responsibilities in risk management into three distinct areas.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO) model is for enterprise risk management.

The ISO 31000 standard provides guidelines for managing risk faced by organizations. It consists of principles, a framework, and a process for managing risk.

48.

An organizational asset is something of either tangible or intangible value that is worth protecting. Data is one of an organization's most important assets. However, protecting all of it all the time using the same approach can be cost-prohibitive.

When using a security categorization process, what is the appropriate **FIRST** step to take to safeguard data?

Identify information type

Select provisional impact levels

Adjust information impact levels

Assign system security category

Correct answer: Identify information type

Not all data is created equal in terms of value. To ensure the proper handling, use, and safeguarding of data in the most cost-effective way, the enterprise should clearly categorize the data. The first step in this is to identify the information type.

Selecting provisional impact levels is the second step in security categorization.

Adjusting information impact levels occurs after reviewing provisional impact levels.

Assigning a system security category is the last step in the process.

49.

What does governance attempt to balance in an organization to meet stakeholder needs and deliver value?

Performance and conformance

Growth and acquisition

Innovation and differentiation

Services and stability

Correct answer: Performance and conformance

Performance has to do with the delivery of business results. Conformance is defined as the process of following guidelines and rules such as regulatory and compliance. Organizations are required to deliver both, and governance is the framework that helps them accomplish that.

Growth and acquisition is a strategic archetype focusing on growing revenues.

Innovation and differentiation is a strategy archetype that focuses on offering new services or products to clients.

Services and stability is a strategy archetype that focuses on stable client-oriented services.

50.

Which of the following consequences of an organization's noncompliance with the laws and regulations of the jurisdictions in which they operate is the MOST harmful?

Loss of license

Fines

Increased audits

Employee dissatisfaction

Correct answer: Loss of license

Penalties come in various forms. Losing a license to operate is often the most harmful consequence because it directly impacts the organization's ability to conduct business.

Fines are often one-time financial penalties that, while burdensome, might not cripple an organization and are less severe than losing the ability to operate entirely.

Increased audits can be a nuisance and lead to additional scrutiny, but they do not impact the organization's ability to operate.

Employee dissatisfaction can affect morale, productivity, and turnover rates, but it is usually an internal issue that can be managed over time.

51.

An electronics company is implementing a new risk governance framework to enhance its risk management practices. The success of this initiative heavily depends on having strong support from the top levels of the organization to ensure adequate resources, commitment, and alignment with the company's strategic goals.

Which of the following **BEST** describes the critical element that is needed to ensure the success of the risk governance framework?

Executive sponsorship

Policy

Lines of defense

Best practices

Correct answer: Executive sponsorship

Executive sponsorship refers to strong support and commitment from top management. It is the critical element that ensures the success of the risk governance framework.

Policies are important for establishing guidelines but do not specifically refer to top-level support.

Lines of defense relates to the roles in managing risks but doesn't address the importance of executive backing for successful implementation.

Best practices refer to recommended procedures, but they do not emphasize the role of executive leadership in ensuring success.

52.

Which role in the risk program is **BEST** positioned to act in an advisory capacity?

Risk practitioner

Risk auditor

Risk owner

Risk executive

Correct answer: Risk practitioner

The risk practitioner is involved in all aspects of the risk program from development to execution. This broad scope of responsibility gives the individual a unique and comprehensive perspective of the program from end to end.

A risk auditor typically focuses on evaluating and assessing the effectiveness of the risk management program and controls, often from an independent or internal audit perspective.

A risk owner is responsible for managing specific risks within the organization and ensuring that appropriate controls and mitigation strategies are in place.

A risk executive is involved in high-level oversight and strategic direction of the risk management program.

53.

In accordance with the RACI model, which role in the risk management process carries out the risk management activities and efforts?

Responsible

Informed

Accountable

Consulted

Correct answer: Responsible

A person who is responsible for a given task or function is designated by the organization as the person who will be executing the tasks. As such, this individual is also responsible for the successful outcome of these activities.

An informed individual is someone who is given updates on risk management efforts.

An accountable individual ensures that risk management efforts are carried out.

A consulted individual provides support for the risk management process.

54.

What is a characteristic of a "Don't Care" organizational risk culture?

Apathy

Minimal required training

Communication on a need-to-know basis

Active monitoring and reporting

Correct answer: Apathy

Apathy occurs when individuals in an organization do not acknowledge or simply do not care about the impact of risk to the organization. This creates an environment in which the organization can be vulnerable to risk.

Minimal required training is used with a "compliance culture" risk culture.

Communication on a need-to-know basis is used with a "Blame Culture" risk culture.

Active monitoring and reporting is used with a "Way of Life" risk culture.

55.

Your organization is planning a move to the public cloud. What factor of the risk management profile will this impact?

New technology

Changes to business procedures

New regulations

Actions of competitors

Correct answer: New technology

A move to the public cloud involves re-platforming and migrating to a new technology stack. This includes all hardware, software, and network components.

While changes to business procedures might be required, the primary impact in this context is the adoption of new technology.

Moving to the cloud might require compliance with different regulations, but the main factor in this scenario is the introduction of the new technology itself.

***T**he effectiveness of risk-awareness programs is more about the ongoing education and training within the organization, rather than directly being impacted by a move to the cloud.*

56.

What is one reason for communicating the current risk management capability of an enterprise?

For predicting how well the enterprise is managing risk and reducing exposure

For setting the overall expectations about the risk management program

For describing the root cause of loss events

For showing options to mitigate risks

Correct answer: For predicting how well the enterprise is managing risk and reducing exposure

Risk communication is an essential part of the risk management process. Communicating the risk management capability has many uses, including predicting how well the enterprise is managing risk and reducing exposure and being a key indicator for good risk management.

Setting the overall expectations about the risk management program is related to communicating expectations from risk management.

Describing the root cause of loss events and showing options to mitigate risks is related to information flows regarding status of IT risks.

57.

Your organization is considering a stock buyout of a competitor. What factor of the risk management profile will this impact?

Mergers or acquisitions

Divestiture

New technology

Customer expectations

Correct answer: Mergers or acquisitions

The buyout of a competitor will result in a newly acquired entity. This entity will either be merged or integrated into existing operations. In either case, the enterprise risk profile will need to be revisited.

Divestiture is the opposite of an acquisition.

New technologies is one aspect that should be considered in a merger.

Customer expectations is an external factor that needs to be considered.

58.

Which role in the risk management process is notified of the progress of risk management efforts as appropriate?

Informed

Consulted

Responsible

Accountable

Correct answer: Informed

Individuals whose role is to be informed are generally senior management or the Board of Directors. While they do not have direct input or involvement in the delivery of risk management activities, it is very important that they are informed of what actions have taken place in the end result.

The consulted role is individuals who provide input, advice, feedback, or approvals.

The responsible role is individuals tasked with completing the actual tasks.

The accountable role is the single person liable for the completion of tasks.

59.

At what corporate level of culture as it relates to risk would clear lines of accountability be a common characteristic?

Proactive

Resilient

Compliant

Reactive

Correct answer: Proactive

Clear lines of accountability show that individuals in an organization are assigned to and step up to managing risk. They understand their role and invest their time in delivering against the organization's risk management framework. Once a company is here, they have achieved a proactive level.

At a reactive level, accountability and responsibility are not defined. At compliant, responsibilities are assigned. At resilient, the lines of accountability and responsibility are communicated and understood throughout the enterprise.

60.

How are threats and vulnerabilities related?

Threats refer to whether something was attempted, while vulnerabilities refer to whether the target of the attempt was susceptible to what was tried

Threats refer to specific techniques used to compromise a system, while vulnerabilities refer to the potential impact of an incident

Threats refer to procedures to handle security breaches, while vulnerabilities refer to planning for recovering from disasters

Threats refer to safeguards against financial losses, while vulnerabilities refer to managing risks by third-party solutions

---

Correct answer: Threats refer to whether something was attempted, while vulnerabilities refer to whether the target of the attempt was susceptible to what was tried

Traditionally, the probability of a risk occurring was a combination of threats and vulnerabilities. Threats are the potential dangers such as attackers or natural disasters, while vulnerabilities are weaknesses in a system.

Exploits refer to specific techniques used to compromise a system, while risk assessments can refer to the potential impact of an incident.

Incident response refers to procedures to handle security breaches, while disaster recovery refers to planning for recovering from disasters.

Fraud prevention refers to safeguards against financial losses, while supply chain security involves managing risks by third-party solutions.

61.

Risk practitioners are continually alert to changes in the organizational supply chain due to the potential for increased risk.

Which of the following is **NOT** a component of a supply chain?

Equipment maintenance logs

Raw materials

Transportation and logistics

Manufacturing facilities

Correct answer: Equipment maintenance logs

A supply chain consists of internal and external entities that contribute to sourcing, creating, and delivering products to the customer. If disrupted, there is a direct impact to the organization's ability to continue operations, thereby increasing risk.

Raw materials are essential components of the supply chain as they are the basic inputs used in the manufacturing process.

Transportation and logistics involves the movement and management of goods within the supply chain, including the delivery of raw materials and finished products.

Manufacturing facilities are locations where raw materials are transformed into finished products, making them a key part of the supply chain.

62.

What is the first line of defense in an ERM program?

Organizational management

Risk and compliance functions

Audits

Enterprise consensus

Correct answer: Organizational management

The three lines of defense ensure that risk management is implemented across the entirety of an organization's lines of business. The first line is operational management, which involves daily operational activities.

Risk and compliance functions are in the second line of defense.

Audits are the third line of defense.

Enterprise consensus is not one of the lines of defense.

63.

Not all organizational assets have equal value, so they don't require the same level of risk management.

Which of the following is a contributing factor to calculating an asset's value?

Financial penalties for noncompliance

Availability of asset documentation

Application of security incident and event management

Quality of employee security training

Correct answer: Financial penalties for noncompliance

Asset evaluation is the process by which the risk management program determines the relative importance of assets in the context of operational impact. Contributing factors include such things as financial penalties for noncompliance, impact on business practices, and damage to reputation.

Availability of asset documentation relates to business process reviews.

Application of security incident and event management relates to technical controls to reduce risk.

Quality of employee security training relates to operational measures to reduce risk.

64.

What is the term for "the objective amount of loss an enterprise can accept without its continued existence being called into question"?

Risk capacity

Risk tolerance

Risk downside

Risk uncertainty

Correct answer: Risk capacity

Risk capacity is the amount of risk an organization can take in pursuit of its business goals. It is a predetermined amount of risk that is expected as part of ongoing operations. It is subject to a maximum amount because exceeding that amount would jeopardize the organization's existence. An example would be that if a company determines that it can absorb a $10 million loss without threatening its survival, then $10 million represents its risk capacity.

Risk downside refers to the potential negative impact or losses associated with a risk event. While it deals with the adverse effects of risks, it doesn't specifically define the maximum acceptable loss that an organization can handle.

Risk tolerance is the amount of risk that an entity is willing to accept beyond their risk appetite. Risk uncertainty refers to the unpredictability associated with a particular risk event.

65.

What is an example of a financial industry that has incorporated ethics into its professional certification?

Accounting

General contracting

Retail

Billing and collections

Correct answer: Accounting

Certified Professional Accountants (CPAs) have published codes of ethics that are directly tied to their CPA certification. The CPA certification can be revoked if they are found to have violated ethics guidelines.

General contracting, retail, and billing/collections do not include ethics in professional certification.

66.

Which of the following statements describes an acceptable corporate risk governance structure?

A board of directors is accountable for governance and entrusts senior management with the responsibility of managing day-to-day operations

The board of directors implements operations while senior management evaluates risk management processes

The board of directors delegates risk governance to junior management and handles day-to-day operations themselves

A board of directors is responsible for day-to-day operations, while senior management is accountable for governance

---

Correct answer: A board of directors is accountable for governance and entrusts senior management with the responsibility of managing day-to-day operations

Corporate governance typically involves the board of directors overseeing and being accountable for the governance of the organization, which includes establishing overall policies and risk management strategies. Senior management is tasked with implementing these strategies and managing the day-to-day operations of the company, ensuring that the organization's goals are met within the governance framework.

The board oversees but does not implement operations, and senior management is responsible for risk management within those operations.

The board should not handle day-to-day operations, and risk governance is typically the responsibility of both the board and senior management, not junior management.

The board does not handle daily operations, and senior management is not typically accountable for governance.

67.

If an enterprise outsources part of its operations to a third party, who is ultimately accountable for compliance with laws and regulations?

The enterprise

The outsourcer

The negotiating agent

Both enterprise and outsourcer

Correct answer: The enterprise

The enterprise is the legal entity in the business that bears the responsibility for compliance with laws and regulations; outsourcing does not change that. The company that is taking on some of the functionality for the primary enterprise will likely have requirements in the contract that require it to either aid the enterprise in being in compliance, or they will have some of their own compliance requirements. However, the question says "ultimately" accountable. That is the enterprise. If they chose a company to outsource some of their operations to, and that company has a breach of the data due to their own practices, the enterprise chose poorly. Further, the enterprise owns the data and is responsible for protecting it.

If there was a negotiating agent, they may have some responsibility for legal compliance, but they, too, are not "ultimately" accountable.

68.

A risk manager is assessing the processes that are in place within her department. She is working to ensure the conductive control environment at the moment.

Which line of risk management defense does this fit into?

First line

Second line

Third line

All lines

Correct answer: First line

The first line of defense is implemented by the business unit, component, or business function responsible for a specific scope of operations. The business unit is responsible for implementing and monitoring the risk activities that apply to their function. This includes ensuring the conductive control environment within a business unit.

The second line of defense is risk and compliance functions. This includes establishing a business-aligned risk management framework.

The third line of defense is audit. This is where conformance to the program is assessed.

69.

Using the RACI model, which role in the risk management process is tapped for their expertise or opinion when developing or executing the risk management process?

Consulted

Responsible

Accountable

Informed

Correct answer: Consulted

Individuals who are consulted are often experts or process owners who have a great deal of knowledge and experience in risk management. The individuals who are responsible or accountable in their roles can leverage this expertise to ensure that they have developed and are executing sound, effective processes.

The responsible role carries out risk management efforts.

The accountable role ensures that risk management efforts are able to be carried out effectively.

The informed role includes stakeholders who are informed about risk management efforts at times.

70.

Which organizational risk culture manages risk as "the way we do business"?

Risk-driven

Proactive

Compliant

Reactive

Correct answer: Risk-driven

A risk-driven culture has risk management at the forefront of its policies and procedures. This means a high degree of accountability, active monitoring and reporting, and continuous improvement.

A culture that has a reactive approach simply accepts that incidents happen. A culture that is administrator-driven works to prevent a similar incident as the one that just happened. A compliance-driven culture works to prevent incidents before they occur. A business-driven culture works to continuously improve the risk systems.

A proactive culture is one that pursues continuous improvement of its systems. It is definitely a business-driven environment.

71.

A software development company is reviewing its risk management governance framework to ensure all aspects of its operations comply with legal and regulatory standards. During this review, the company identifies several obligations that must be met as part of agreements with clients and partners. These obligations are critical to maintaining business relationships and avoiding legal disputes.

Which of the following **BEST** describes these obligations?

Contractual requirements

Professional ethics

Regulatory requirements

Risk management frameworks

Correct answer: Contractual requirements

Contractual requirements are the specific obligations outlined in agreements with clients and partners, essential for maintaining strong business relationships and preventing legal issues. The risk management team must ensure that these requirements align with the organization's risk management policies and procedures.

Professional ethics involve moral principles that guide behavior in a professional setting, but they do not directly relate to the specific obligations in contractual agreements.

Regulatory requirements refer to the laws and regulations a company must comply with.

Risk management frameworks outline the processes for identifying and managing risks but do not define the obligations set forth in client and partner agreements.

72.

What is the downside of ethics policies that are unenforced or applied selectively?

Inconsistency can increase risk to the organization

Inconsistency can decrease risk to the organization

Inconsistency can lead to more internal audits

Inconsistency fosters employee creativity when it comes to ethical decisions

---

Correct answer: Inconsistency can increase risk to the organization

Ethics policies that are unenforced or applied selectively are ineffective at directing behavior. This creates opportunities and windows for activities to take place that are against the organization's values.

Applying ethics policies inconsistently opens the door to unethical behavior and thus increases organizational risk.

Inconsistency does not directly lead to more internal audits, although more audits may occur if systems are shown to be vulnerable over time.

Selective enforcement can lead to confusion and unethical practices rather than fostering positive ethical creativity.

73.

A corporation has put effort into selecting specific controls. What is the purpose of these controls?

Mitigate specific risks

Overcome adverse business events

Demonstrate program management oversight

Demonstrate compliance with a regulation

Correct answer: Mitigate specific risks

Controls are methods for monitoring and addressing risks. These controls are put in place to act as agents and gatekeepers that are continually assessing and managing organizational risk to neutralize or reduce the impact.

A Business Continuity Plan or Disaster Recovery Plan would be a control that would aid a company in overcoming adverse events. However, the question is more generic, which means this answer does not match the questions as well as "mitigate specific risks."

It is possible that a control could be implemented incorrectly, which means that controls do not demonstrate compliance or management oversight.

74.

Which characteristic of an IT risk management program means that it follows policies, laws, and regulations?

Compliance

Justifiable

Enforced

Up-to-date

Correct answer: Compliance

Many enterprises are in regulated industries, such as financial services or healthcare. In addition to regular business operations, they also have to follow regulatory guidelines that are put forth by industry organizations or the government. This means their risk management programs must also be aligned with these compliance guidelines.

Justifiable refers to a risk management program that is based on sound reasoning.

Enforced refers to a risk management program that is consistent and required.

Up-to-date refers to a risk management program that keeps up with changes.

75.

A healthcare company is implementing a new IT risk management framework. One of the key objectives is to ensure that all risk management activities can be reviewed and verified by internal and external assessors. This is crucial for maintaining transparency and accountability in the risk management process.

Which of the following **BEST** describes the characteristic that they are aiming for?

Auditable

Justifiable

Enforced

Compliant

Correct answer: Auditable

An auditable activity can be reviewed, verified, and assessed by internal and external parties, ensuring transparency and accountability. An auditable process provides a clear trail of evidence showing that risk management procedures have been followed and are effective.

Justifiable means actions can be explained or defended; it doesn't necessarily imply detailed review and verification

Enforced refers to ensuring that rules or policies are implemented and followed, but it doesn't cover the ability to review and verify those activities later on.

Compliant refers to following rules, regulations, or standards, but compliance doesn’t ensure verification and review of compliance.

76.

Why are organizations' service/business processes considered to be an asset with value worth protecting?

Service/business processes provide a competitive advantage

Service/business processes require fewer employees

Service/business processes require minimal upfront investment

Service/business processes provide exclusive rights to generate revenue through licensing

---

Correct answer: Service/business processes provide a competitive advantage

Best-of-breed service/business processes deliver optimum outcomes to an organization's clients. These processes are developed and documented to provide a customer experience that is differentiated from other organizations. If these service/business processes were compromised, it would represent a risk to an organization's brand, customer satisfaction, and, ultimately, its profitability.

A process may require fewer employees in comparison to what it would like for that company if it did not have that process in place, but that is not the main reason that it needs to be protected. Again, the competitive advantage is more important.

Business processes actually require more upfront investment, not a minimal investment.

Intellectual property can provide exclusive rights to generate revenue through licensing.

77.

Which characteristic of an IT risk management program means that it is carried through from end to end?

Complete

Justifiable

Auditable

Monitored

Correct answer: Complete

A complete IT risk management program executes its activities from risk awareness to analysis, action, and continuous learning. Omitting or skimming over any of the steps would reduce the effectiveness of the program.

Justifiable refers to the program being based on logical, well-founded reasoning.

Auditable refers to the program being designed so it can be reviewed by an independent third party.

Monitored refers to a program being subject to review and accountability.

78.

Which individual in an organization is responsible for establishing risk processes, practices, activities, and role definition related to risk management capabilities?

Risk practitioner

Risk owner

Internal auditor

Data custodian

Correct answer: Risk practitioner

The risk practitioner is responsible for the end-to-end setup of the risk management program. This involves all aspects of people, processes, and role definition.

The risk owner is responsible for managing specific risks within their area of responsibility but does not typically establish the overall risk management processes.

An internal auditor reviews and assesses the effectiveness of the organization's risk management processes and controls but does not establish them.

A data custodian is responsible for the safe custody, transport, and storage of the data and the implementation of business rules. They do not typically establish risk management processes.

79.

What is the name of the department or business function that typically houses the enterprise risk team?

Risk management

Finance

Strategy and planning

Executive leadership

Correct answer: Risk management

Enterprise risk management is a department or business function within an organization that is fully dedicated to defining, monitoring, and managing risks within an organization. It is important that this function is separate from other departments so that they can act independently and objectively to maintain the overall enterprise risk portfolio.

The finance department houses teams such as accounting and procurement.

The strategy and planning department houses teams such as business development and market analysis.

The executive leadership houses teams that perform decision-making and resource allocation.

80.

Risk tolerances and appetites change over time. Which of the following is a factor or initiative that would require an enterprise to reassess its risk portfolio and reconfirm its risk appetite?

Changes in business strategy

Refreshes in existing technology

Up-leveling the employee training program

Opening one new warehouse

Correct answer: Changes in business strategy

A change in strategy impacts the business components that make up risk tolerance and appetite: resources, market forces, operational processes, and financial considerations. Therefore, a reassessment would be required.

Risk appetite is the amount of risk management is willing to accept, in general. Risk tolerance is how much risk they are willing to accept that exceeds the appetite under specific circumstances. If the business strategy changed, it would impact management's view on both appetite and tolerance.

Refreshing technology is very unlikely to impact management's view on risk appetite and tolerance. The same can be said for employee training programs or opening a new warehouse.

81.

Why is an understanding of organizational culture important to managing risk?

Because organizational culture drives behavior

Because organizational culture creates a misalignment between stated risk appetite and actual behavior

Because organizational culture does not promote risk management

Because organizational culture is the same in all departments

---

Correct answer: Because organizational culture drives behavior

Individuals within an organization will act according to their environment. Culture of risk is defined as the set of shared values and beliefs that governs attitudes toward risk-taking, care, and risk integrity and determines how openly risks and losses are reported and discussed. It is important to have a culture that supports the active monitoring and management of risk.

Organizational culture should attempt to align an organization's stated risk appetite and actual behavior.

Organizational culture's significance lies in how it shapes behaviors and attitudes toward risk-taking and risk management practices.

Organizational structure may vary between different departments in an organization.

82.

What risk category in ISACA's Risk IT Framework 2nd Edition deals with pollution or disturbances of protected areas?

Environmental

Compliance

Market

Operational

Correct answer: Environmental

The category of environmental risk deals with issues such as pollution and environmental sustainability. Environmental risk encompasses potential harm or damage to the environment resulting from human activities. This includes pollution, deforestation, habitat destruction, and the disturbance of protected natural areas like national parks, wildlife reserves, and marine sanctuaries. The government, for example, has policies on environmental justice, public plans, and conservation.

Compliance risks deal with regulatory requirements from governments, such as GDPR.

Market risk refers to the potential financial losses due to changes in market conditions, such as fluctuations in stock prices, interest rates, or currency exchange rates.

Operational risk is the potential for losses due to failures in internal processes, systems, human factors, or external events.

83.

An organizational asset is something of either tangible or intangible value that is worth protecting. What type of asset represents the credibility of an organization in the marketplace?

Brand

Intellectual property

People

Cash and investments

Correct answer: Brand

An organization's brand represents customer and marketplace perception of many dimensions. These include the reputation of their products and services, customer service, or corporate social responsibility. A strong brand heavily contributes to an organization's profitability and sustained success. If this asset were compromised in any way, it would be very detrimental.

Intellectual property distinguishes one company from another. For example, a drug formula. The drug formula is of great value to the customer who needs that drug, but it does not actually show credibility.

Cash and investments is a possible result of the company being considered credible, having many customers and many sales. It is the result, not the credibility.

People are critical to a business. If the right people are hired and given the right processes, the company can see great results. A person who works at Apple, for example, who is wearing one of their T-shirts and is seen in the store is trusted by the customer. However, it is the shirt with the Apple logo that brings confidence first and foremost.

84.

Which of the following represents a potential professional ethics conflict of interest?

Hiring an unqualified relative

Researching how to set up your own company while employed

Posting to social media about your company

Providing false or misleading information to a supervisor

Correct answer: Hiring an unqualified relative

Organizations hire for specific roles and responsibilities. While hiring members of the same family does not always represent an ethics situation, a hiring manager who hires an unqualified relative presents a conflict of interest.

Researching how to set up your own company while employed could be a conflict of interest if it leads to competing with your current employer, but, by itself, it is not necessarily a conflict of interest.

Posting to social media about your company could pose a risk to confidentiality or reputation but isn't necessarily a conflict of interest.

Providing false or misleading information to a supervisor is unethical, but not a conflict of interest.

85.

Not all risk originates from technology systems or data or cybersecurity platforms. Risk also comes from lines of business.

Which of the following is an example of a business-originated risk?

Economic cycles

Government legislation

Acts of nature

Data breaches

Correct answer: Economic cycles

Economic cycles take place as a result of market activity or seasonality, which can be regional or global. This is normal. For example, many retail organizations experience regular economic cycles and have built those cycles into their risk management programs.

Government legislation is not a business-originated risk. If a business is not complying with legislation, the fault is with the business.

Acts of nature come from the planet, not people, not the business.

Data breaches are an IT-related risk due to inadequate controls.

86.

Key employees are organizational assets that are worth protecting. What type of control can be used to ensure that an organization is protected in case a key individual leaves or retires?

Cross-training

Badging

MFA

Security guards

Correct answer: Cross-training

Key employees in an organization typically have knowledge in a certain area or have specific expertise. This knowledge and expertise usually has a significant and direct impact on the success of the organization, so cross-training other employees to do their role can protect the organization if that employee leaves.

Badging and security guards are physical security controls.

Multi-factor authentication (MFA) is a control for securing the authentication process.

87.

What is the best practice for a global organization to incorporate country-specific guidelines and regulations in a risk management program and maintain centralized accountability?

Regional addendum

Multiple global programs

Outsource regional program

Decentralized risk program

Correct answer: Regional addendum

From country to country, there are typically common risk policies to be followed. A control suite is built in the risk management program to handle regulations. A best practice is to augment the risk management program with specific addendums by country so that the detailed guidelines and regulations for that jurisdiction are also followed.

***M**ultiple global programs can lead to inconsistencies and duplication.*

Outsourcing regional risk management programs might lead to a lack of control and alignment with the organization's overall risk management strategy.

A decentralized approach might address local requirements effectively but could make it challenging to maintain a unified risk management strategy.

88.

Which of the following is **NOT** one of the 4 strategic COBIT archetypes for enterprises to align their risk governance processes?

Market homogeneity

Innovation/differentiation

Cost leadership

Client service

Correct answer: Market homogeneity

Market homogeneity means that an enterprise is similar to all others in its industry. This is counter to the COBIT archetypes of innovation and differentiation,

Innovation/differentiation, cost leadership, and client service are all included as strategic archetypes for enterprises.

89.

Which individual in an organization has the responsibility for delivering day-to-day risk management functions?

Risk practitioner

Risk owner

Risk manager

Risk analyst

Correct answer: Risk practitioner

The risk practitioner is responsible for the day-to-day implementation of the risk management program. This individual works closely with other stakeholders to develop, integrate, implement, and monitor the risk management operations.

A risk owner is accountable for specific risks and is responsible for ensuring that effective risk management practices are applied to those risks.

A risk manager generally oversees the overall risk management function, develops risk management strategies, and ensures that policies and procedures are followed.

A risk analyst provides insights and recommendations but is not usually responsible for the daily execution of risk management activities.

90.

What is the **MOST** important factor that determines the risk level appetite of an organization?

Risk-taking culture

Employee background

Industry vertical

Financial repercussions

Correct answer: Risk-taking culture

The culture of an organization determines its outlook and values. A conservative organization may have a conservative risk perspective versus an organization with a more bold and risk-taking culture.

Employee background can influence risk appetite but is not the main factor.

Different industries have different levels of risk they normally take, but that varies by company.

Financial repercussions can affect risk appetites, but not as much as company culture.

91.

As it relates to organizational strategy, what is the sole purpose for the existence of an enterprise?

To achieve the defined vision

To capture maximum market share

To innovate and deliver products

Providing stable and client-oriented service

Correct answer: To achieve the defined vision

The vision of an enterprise defines its intended future state. This future state includes financial gain as well as operational effectiveness. The defined vision represents the long-term aspirations, goals, and direction of the enterprise. It serves as a guiding principle that articulates what the organization aims to accomplish and the impact it seeks to make in its industry or market. Achieving the defined vision ensures that the enterprise remains focused, aligned, and committed to its overarching objectives, driving its strategic decisions, investments, and actions.

While capturing maximum market share is an important aspect of organizational operations and success, it is ultimately a means to achieving the broader vision and purpose of the enterprise.

COBIT proposes the strategic archetype of innovation and differentiation to define the corporate strategy. It is not the purpose of the organization. A second strategic archetype is client service/stability which has the enterprise focused on providing stable and client-oriented service.

92.

As it relates to risk management's lines of defense, which line of defense is responsible for conducting risk audits?

Third line

Second line

First line

Fourth line

Correct answer: Third line

The third line of defense consists of conducting the audit and assessing the performance of the risk management program against the enterprise goals. This line of defense also reviews the design and effectiveness of the program and makes appropriate recommendations for change.

The first line of defense relates to operational management.

The second line of defense relates to risk and compliance functions.

There is no recognized fourth line of defense.

93.

A risk practitioner is managing a project to develop a new software application. During the planning phase, they identified several potential security risks that could impact the project. To mitigate these risks, they are choosing specific measures that will help protect the project from these threats.

What type of risk management procedure are they engaged in?

Control selection

Risk assessment

Establishing KPIs

Risk monitoring

Correct answer: Control selection

Control selection involves choosing specific measures to mitigate identified risks, which is the appropriate action in this scenario.

Risk assessment is the process of identifying and evaluating risks, which has already been done in the scenario.

Establishing KPIs involves setting key performance indicators to measure project performance, not directly related to mitigating security risks.

Risk monitoring involves tracking identified risks over time, which is important but not the immediate action needed to address the risks.

94.

What statement **BEST** explains how professional ethics impact risk?

Poor ethical standards can lead to fraud or theft.

Professional ethics have no bearing on risk.

Risk owners are accountable for employee professional ethics.

High professional ethics do not reduce risk at all.

Correct answer: Poor ethical standards can lead to fraud or theft.

Organizations that have a low standard of ethics can create a culture of lower standards. This leads to a reduced sense of awareness during business operations of potentially risky activities and creates incidents.

Professional ethics are closely tied to risk management because they can prevent misconduct.

While risk owners are responsible for managing and mitigating risks within their area of control, they are not directly accountable for the ethical behavior of all employees.

High professional ethics can reduce risk by fostering a culture of integrity and accountability.

95.

Which risk management procedure determines the audience and the level of risk information communicated across the enterprise?

Risk reporting

Risk escalation

Risk evaluation

Risk identification

Correct answer: Risk reporting

The risk reporting procedure establishes the steps associated with the amount and frequency of risk information that is communicated. This procedure includes communication that has to take place when a risk is identified, when the risk evaluation is completed, when the risk is being addressed, and any escalations.

The risk assessment procedure should detail how risks are analyzed and compared to the enterprise's goals and objectives. The procedure of risk identification should detail what is expected as steps to identify threats and the associated risk to an enterprise. The procedure for risk evaluation details how risk should be evaluated in relationship to the business context; e.g., how this risk impacts the business.

96.

A social media company has developed a new app that incorporates a unique algorithm for data analysis. The company wants to protect this algorithm from unauthorized use or disclosure.

What type of asset is the company trying to protect?

Trade secret

Patent

Trademark

Copyright

Correct answer: Trade secret

A trade secret is confidential information that gives a company a competitive advantage. In this case, the unique algorithm would be considered a trade secret.

Copyright protects original works of authorship, such as books, music, and software.

A trademark protects a brand name, logo, or slogan.

A patent protects inventions and processes, but the patent process can be time-consuming and expensive.

97.

Which risk governance objective requires the consideration of the full range of opportunities and consequences of decisions and their impact on the enterprise?

Making risk-aware business decisions

Implementing risk management controls correctly

Integrating risk management into enterprise processes

Establishing a common risk view

Correct answer: Making risk-aware business decisions

To make sound business decisions with risk in mind, all options, opportunities, and upside/downside must be considered. This balanced approach enables decision-makers to achieve the best holistic solution and maintain the risk governance guidelines of the organization.

A common risk view requires regular reporting and ongoing reviews of risk. Integrating risk management into the whole of the enterprise requires both a top-down and a bottom-up approach to enterprise risk. Implementing risk management controls correctly requires oversight and due diligence to ensure risks are being mitigated well across the enterprise.

98.

Which two standards organizations have published guidelines for information security risk assessment and management?

ISO and IEC

HIPAA and COBIT

SOX and ISO

NIST and PCI

Correct answer: ISO and IEC

ISO and IEC have individually and collectively published requirements for security risk assessment and management techniques. As an example, ISO/IEC 27001 is a comprehensive set of guidelines for how to establish, implement, and maintain an information security system. The standard is used internationally and has been in existence since 2013.

NIST and PCI are focused on specific areas rather than a broad approach to information security risk management.

SOX and HIPAA are primarily compliance frameworks, not comprehensive risk management standards.

99.

Which risk management policy sets specific guidelines to protect personally identifiable information to follow statutory regulations?

Privacy policy

Information security policy

Risk appetite policy

Enterprise risk policy

Correct answer: Privacy policy

A privacy policy focuses specifically on identifying information that can be used individually or combined collectively to identify a person. Several industries have regulatory guidelines against making personally identifiable information public. Organizations that do not follow these guidelines with a strict privacy policy can be subject to serious fines and consequences.

An information security policy includes guidelines to protect information assets and can encompass PII protection, but it is broader in scope and covers overall information security measures, not just privacy and statutory compliance.

A risk appetite policy defines the level of risk an organization is willing to accept. It does not specifically address the protection of PII or compliance with statutory regulations.

An enterprise risk policy provides a broad framework for managing various types of risks across the organization but does not specifically focus on PII protection or statutory compliance.

100.

Which of the following statements is in the ISACA Code of Professional Ethics?

Perform duties with objectivity, due diligence, and professional care

Serve as a central clearinghouse for distributing private and confidential information

To maintain up-to-date knowledge in building codes and safety laws

Only hire professionals who have CRISC certification

Correct answer: Perform duties with objectivity, due diligence, and professional care

ISACA has a comprehensive Code of Professional Ethics. All risk practitioners who have earned the CRISC certification must be aligned to the Code. The ISACA code of ethics includes the following:

1. *Support the implementation of and encourage compliance with appropriate standards, procedures, and controls for information systems.*
2. *Perform their duties with objectivity, due diligence, and professional care, in accordance with professional standards and best practices.*
3. *Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not discrediting their profession or the Association.*
4. *Maintain privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.*
5. *Maintain competency in their respective fields and agree to undertake only those activities which they can reasonably expect to complete with professional competence.*
6. *Inform appropriate parties of the results of work performed, including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.*
7. *Support the professional education of stakeholders in enhancing their understanding of information systems security and control.*

ISACA's code of professional ethics does not mention being a clearinghouse for distributing private and confidential information, retaking the CRISC certification every six months, or only hiring professionals who have a CRISC certification.