QBank Quiz December 12, 2020

Test ID: 152923573

Question #1 of 150

Question ID: 1135941

Which enterprise architectural framework enables communication of information to personnel in a manner that is most useful to each group's responsibilities?

A) SABSA

B) TOGAF

C) Zachman

D) **NIST SP 800-53**

Explanation

Zachman is correct. It is a two dimensional framework that enables the analysis of the organization to be communicated in ways that are appropriate for each group. Analysis of the organization can be presented to different groups in different ways according to the groups' responsibilities.

The Sherwood Applied Business Security Architecture (SABSA) is an enterprise security architecture framework that is risk driven.

The Open Group Architecture Framework (TOGAF)l is an architectural framework that iteratively monitors and updates individual requirements.

NIST SP 800-53 is a control framework.

Objective:
Information Security Governance

Sub-Objective:
Define, communicate, and monitor information security responsibilities throughout the organization and lines of authority.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.11 Strategy Resources, 1.11.2 Enterprise Information Security Architectures

Question #2 of 150

Question ID: 1185769

What is the BEST way to verify that the method of obtaining an operational metric is accurate?

A) Repeat the measurement several times.

B) Ask a colleague if the results of the measurement are reasonable.

C) Compare the results with the results gained from an alternative method.

D) Verify that the metric complies with accepted standards.

Explanation

Comparing the results with the results gained from an alternative method is the best way to verify that the method of obtaining an operational method is accurate. If both means of measuring the operational metric yield comparable results, then there is a greater assurance of the accuracy of the metric.

Repeating the measurement several times is not the best way to verify its accuracy. Repeating the measurement several times would apply the same method of measurement to the same data set. If the results are the same, it cannot be concluded that the method is accurate, because it would be expected that doing the same thing to the same dataset should produce the same result. The only way this would help is if the results differ from each other. Then it can be concluded that the method is flawed.

Asking a colleague is not the best way to verify its accuracy because there exists no basis for comparison.

Compliance with accepted standards is not the best way to verify an operational metric's accuracy. Compliance with accepted standards is a management metric, not an operational one.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish, monitor and analyze program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.13 Security Program Metrics and Monitoring, 3.13.1 Metrics Development

Question #3 of 150

Question ID: 1135918

Which framework distinguishes between governance and management?

A) **COBIT 5**

B) SABSA

C) ISO/IEC 27001:2013

D) CMMI

Explanation

The Control Objectives for Information and Related Technologies (COBIT) 5 framework distinguishes between governance and management. According to principle 5 in this framework, governance should be distinguished from management. Governance ensures that objectives for stakeholders are evaluated. Management ensures that the directions set in the governance policies are achieved.

The Capability Maturity Model Integration (CMMI) does not formally distinguish between governance and management. It provides guidance for organizations to elevate performance by benchmarking capabilities and comparing their operations to good practices.

The Sherwood Applied Business Security Architecture (SABSA) does not formally distinguish between governance and management. It is an enterprise architecture framework that details the roles, entities, and relationships required to perform business processes.

ISO/IEC 27001:2013 does not formally distinguish between governance and management. It provides guidance on ensuring that the organization's information security system is properly built, maintained, and progressed.

Objective:
Information Security Governance

Sub-Objective:
Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.8 Information Security Strategy Objectives, 1.8.3 The Desired State

Question #4 of 150

Question ID: 1185754

Which of the following frameworks provide guidance for establishing a risk management program? (Choose all that apply.)

A) ISO/IEC 27005:2011

B) NIST SP 800-39

C) IEC 31010:2009

D) COBIT 5

E) NIST SP 800-53

F) ISO 31000:2009

Explanation

COBIT 5, ISO 3100:2009, IEC 010:2009, NIST 800-39, and ISO/IEC 27005:2011 are frameworks for establishing a risk management framework. They provide guidance for establishing a risk management program.

COBIT 5 is a framework for assessing risk. It is aligned with ISO/IEC 27005:2011, and includes risk identification, analysis, and evaluation.

ISO/IEC 31000:2009 provides principles and generic guidelines for risk management.

IEC 31010:2009 provides guidance for an integrated program for managing information security risk to organizational operations, assess, and individuals.

ISO/IEC 27005:2011 has guidelines for security risk management

NIST SP-800-53 provides guidance for implementing security controls that help with due diligence. It is not a framework for a risk management program.

Objective:
Information Risk Management

Sub-Objective:

Determine whether information security controls are appropriate and effectively manage risk to an acceptable level.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.6, Risk Assessment and Analysis Methodologies

, Chapter 2: Information Risk Management, 2.5 Implementing Risk Management, 2.5.2, Defining a Risk Management Framework

---

Question #5 of 150

Question ID: 1135954

Which of the following would be a valid method of assessing employee cybersecurity training and awareness?

A) Have participants of the training session fill out a self-evaluation form.

B) Track the number of incidents that occur after the training session.

C) Send official-looking emails to everyone in the company with spoofed links that will internally track whether people clicked them.

D) **Send out a quiz after the training session to test what participants learned.**

Explanation

Sending official looking emails to everyone in the company with spoofed links is a valid method of assessing employee cybersecurity training and awareness. Doing so will test how well the employees retained their training and are applying security awareness.

An assessment survey will not accurately assess employee cybersecurity training and awareness because listing recalled facts about security does not prove how employees will react when they encounter a real-life vulnerability. A self-evaluation form would not be valid for the same reason.

Tracking the number of incidents that occur after training will not accurately assess employee cybersecurity training and awareness, unless those incidents were specifically filtered to those that originated internally.

Objective:

Information Risk Management

Sub-Objective:

Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.2 Risk Management Strategy, 2.2.1 Risk Communication, Risk Awareness and Consulting

---

Question #6 of 150

Question ID: 1185741

A business case for improving the information security architecture was presented to management. The business case supported the installation of improved lighting, security cameras, and motion detectors. Senior management was not convinced of the need, saying it was too expensive. How might these concerns be addressed in a revised business case? (Choose three.)

A) **Include information about what other companies in the area are doing.**

B) Include data about the area’s crime rate.

C) Reduce the proposed number of lights to reduce power consumption expenses.

D) **Explain how an intrusion will trigger a call to law enforcement.**

E) **Develop a video about how these additions will enhance the organization’s security.**

F) Develop the presentation to include ROSI data.

Explanation

To provide a more convincing case to senior management, the business case could also include information about the crime rate in the area. To clarify to senior management how these enhancements will support business goals, it should include the return on security investment (ROSI) data. A video demonstration will help senior management to get a better picture of the benefits that the lights and cameras will provide.

The business case should not include information about what other companies in the area are doing. If the program cannot be shown to provide a benefit to the company, then it does not matter what other companies are doing.

The business case should not propose reducing the number of lights to save money. Doing so will defeat the purpose of improving the lighting.

The business case should not explain that an intrusion will trigger a call to law enforcement due to the possibility of false positives from inadvertent triggering of the motion detectors by animals, trees swaying in the wind, snow blowing past the cameras, and other non-emergency events.

Objective:
Information Security Governance

Sub-Objective:
Develop business cases to support investments in information security.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.4 Risk Management Roles and Responsibilities, 1.4.2 Obtaining Senior Management Commitment.

Question #7 of 150

Question ID: 1135906

During an investigation of a breach, you determined that a particular patch was not installed. Further investigation indicated that the server for which the patch was supposed to be applied was not included in any policy. Who or what is most responsible for this failure?

- **A)** Information security manager
- **B)** System owners
- **C)** Data custodian
- **D)** **Senior management**

Explanation

System owners are most responsible for this failure. System owners are responsible for ensuring that proper security controls are in place, and for ensuring the systems they oversee are included in any relevant policies.

Senior management does not ensure that all systems are included in relevant policies. Senior management is responsible for developing the business strategy and ensuring that security policies are integrated with the business strategy. The business strategy provides the guidance for all other programs, policies, and strategies. If senior management does not fully support the security policies and activities, they place organizational security at risk. But business strategies do not include individual systems.

The information security manager does not ensure that all systems are included in relevant policies. This manager is responsible for implementing the organization's security programs.

The data custodian does not ensure that all systems are included in relevant policies. The custodian is responsible for implementing controls for accessing resources on the network.

Objective:
Information Security Governance

Sub-Objective:
Establish and/or maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and/or ongoing management of the information security program.

References:

CISM Review Manual, 15th Edition, Chapter 1.4.1, Key Roles

Question #8 of 150

Question ID: 1135962

Under certain circumstances, small acceptable risks can simultaneously affect a large number of systems. What is the term for this kind of risk?

A) Residual risk

B) Information risk

C) **Aggregated risk**

D) Cascading risk

Explanation

Aggregated risk manifests when a threat simultaneously affects a number of small acceptable risks, causing a significant impact. It can also manifest when a large number of threats affect a number of minor vulnerabilities.

Residual risk is the risk remaining after mitigation and other treatment measures are applied to a risk.

Cascading risk occurs when one failure causes a series of failures. For example, if a risk applies to a database server, then that risk will also affect the applications that rely on that database server.

Information risk is the risk resulting from making information assets available for access either internally or publicly. Protecting the information is the purpose of a risk management program.

Objective:
Information Risk Management

Sub-Objective:
Ensure that risk assessments, vulnerability assessments, and threat analyses are conducted consistently, at appropriate times, and to identify and assess risk to the organization's information.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.7 Risk Assessment, 2.7.7 Aggregated Risk and Cascading Risk

---

Question #9 of 150

Question ID: 1136009

Which of the following statements is true about the design, implementation, and management of an information security program?

A) Because senior management has already supported information security governance, the information security program itself does not need the involvement of senior management.

B) The information security program must start with a risk assessment.

C) The information security program should only address risk.

D) **The information security program must execute a well-developed information security strategy.**

Explanation

The information security program must execute a well-developed information security strategy. The strategy must be closely aligned with and support organizational objectives.

The information security program must be designed with the cooperation and support of management. Ongoing support from senior management is the key to universal acceptance by the rest of the organization.

The information security program does not have to start with a risk assessment. It is not universally agreed that a risk assessment is the appropriate way to start.

The information security program does not only address risk. The program should also address the objectives for information security.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish and/or maintain the information security program in alignment with the information security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.1: Information Security Program Management Overview

---

Question #10 of 150

Question ID: 1138444

Which of the following is a qualitative metric?

- **A)** Perimeter breaches
- **B)** Open audit Items
- **C) CMMI levels at periodic intervals**
- **D)** Unremediated vulnerabilities

Explanation

Capability Maturity Model Integration (CMMI) levels at periodic intervals are considered a qualitative metric. CMMI has five levels of maturity from incomplete to optimizing processes.

Unremediated vulnerabilities, open audit items, and perimeter breaches are not correct. They are all quantitative measuring the number of vulnerabilities, open audit items and perimeter breaches. These are all quantitative metrics that could be used to determine key performance indicators (KPIs), but alone are not considered qualitative metrics. Qualitative metrics includes key goal indicators (KGIs), key risk indicators (KRIs), and Six Sigma quality indicators.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish, monitor and analyze program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.13.1 Metric Development

, Chapter 1: Information Security Governance, 1.8 Information Security Strategy Objectives, 1.8.3. The Desired State

Question #11 of 150

Question ID: 1135980

An organization suffers a breach where very sensitive data is obtained by a hacker. It was later determined that the breach was due to a vulnerability in a system that was not patched. Which phase of the SDLC failed to prevent the breach?

A) Configuration management
B) Initiation
C) **Operation/Maintenance**
D) Implementation

Explanation

This is a failure in the Operation/Maintenance phase. Patching and updating is part of system operations.

The phases of the SDLC are:

- Phase 1: The Initiation phase identifies the need for an IT system to addressed identified risks.
- Phase 2: The Development or Acquisition phase addresses the development of a system per identified risks.

- Phase 3: In the Implementation phase, the system features are configured, enabled, tested, and verified against the requirements for risk management.
- Phase 4: The Operation or Maintenance phase is where the system is performing its functions and undergoes periodic updates, per the configuration management policies for compliance with the requirements of risk management.
- Phase 5: The Disposal phase involves the secure disposition of information, hardware, and software assets.

Objective:
Information Risk Management

Sub-Objective:
Facilitate the integration of information risk management into business and IT processes to enable a consistent and comprehensive information risk management program across the organization.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.11 Risk Management Integration with Life Cycle Processes, 2.11.2 Life Cycle-Based Risk Management Principles and Practices

---

Question #12 of 150

Question ID: 1135995

Which statement is true regarding qualitative risk analysis?

A) It provides a cost-benefit analysis.

B) **It provides an AV estimate.**

C) It prioritizes risk.

D) It provides a measurement of the magnitude of the impact.

Explanation

Qualitative risk analysis prioritizes risk and identifies areas for improvement.

Qualitative analysis does not provide a cost benefit analysis, measurement of the impact's magnitude, or an estimate of the asset value (AV). Such measurements are quantitative.

The cost benefit analysis is performed by performing a Return on Security Investment (ROSI) that compares the cost of mitigation to the value of the asset. The metric for determining the magnitude of an impact is also a quantitative analysis, which is included in the Business Impact Analysis (BIA). The BIA prioritizes assets by their value to the organization.

Objective:
Information Risk Management

Sub-Objective:
Report noncompliance and other changes in information risk to facilitate the risk management decision-making process.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.7 Risk Assessment, 2.7.14 Analysis of Risk

---

Question #13 of 150

Question ID: 1135922

Of the following options, which is considered to be a policy statement?

A) Network administrators shall back up all systems nightly.

B) Control of resources must prevent unauthorized access.

C) All passwords shall be at least 15 random characters long.

D) Network backups should be started no later than 11:00 p.m.

Explanation

Control of resources must prevent unauthorized access is a policy statement. A policy is a high-level document that states management's intent, direction, and expectations.

None of the other options can be considered a policy statement.

Setting all passwords to 15 random characters is a standard, which defines a specific metric by which passwords should be measured.

Network admins backing up all systems nightly is a procedure that defines an action to be conducted.

Establishing that network backups shall be started no later than 11 PM is a guideline that clarifies the backup procedure.

Objective:
Information Security Governance

Sub-Objective:
Establish and maintain information security policies to guide the development of standards, procedures and guidelines in alignment with enterprise goals and objectives.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.11 Strategy Resources, 1.11.1 Policies and Standards

Question #14 of 150

Question ID: 1138429

In the accounting department of an organization, what security control could the accounts payable group use to prevent or reduce fraud?

A) **Separation of duties**
B) Least privilege
C) Data loss prevention system
D) Intrusion detection system

Explanation

Separation of duties is a security control that can be used to prevent or reduce fraud. Fraud can be prevented in the accounts payable group by having one person create the checks to be paid and another person sign them. Other controls that can help reduce fraud include mandatory vacations, job rotation, and two-man controls.

Least privilege would not specifically help the accounting group reduce fraud. All employees in every department should be subject to the principle of least privilege, whereby they are only granted the level of access that is required to do their job.

A data loss prevention (DLP) system would be applied to the entire network. A DLP system prevents data from being transmitted and has nothing to do with fraud prevention.

An intrusion detection system would be applied to the entire network or to individual systems. It would prevent outside attackers from attempting to infiltrate the accounts payable computers, but it would not prevent internal fraud.

Objective:

Information Security Program Development and Management

Sub-Objective:

Align the information security program with the operational objectives of other business functions (e.g., human resources [HR], accounting, procurement and IT) to ensure that the information security program adds value to and protects the business.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.2 Controls and Countermeasures, 3.12.2 Control Design Considerations

Question #15 of 150

Question ID: 1136081

Following a full interruption test, the actual recovery time exceeded the AIW. How should the organization respond?

A) Decrease the RTO.

B) Revise the IRP and redo the basic testing starting with a checklist review.

C) **Review the documentation, make corrections, and run the full-interruption test again.**

D) Increase the AIW.

Explanation

A full interruption test is very disruptive to the organization and represents the most risk. Therefore it should not be run frequently, and is generally recommended to run annually. After the results of the full interruption test are reviewed, the incident response plan (IRP) should be revised and the testing cycle should reset, starting with the checklist review.

The allowable interruption window (AIW) is a business decision and is the amount of time that normal operations must be restored before the existence of the organization is threatened. It cannot be changed to suit the recovery operations. It should only be changed through a formal change control process.

The full interruption test should not be run until the plan is reviewed and modified and all other tests are run successfully.

Decreasing the recovery time objective (RTO) is not logical because that choice would shorten the time objective for recovery. In this scenario, the allowable interruption window has been exceeded, which means the actual time for recovery is too long.

Objective:
Information Security Incident Management

Sub-Objective:
Test, review and revise (as applicable) the incident response plan periodically to ensure an effective response to information security incidents and to improve response capabilities.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.9: Developing an Incident Response Plan, 4.9.3 Business Impact Analysis

---

Question #16 of 150

Question ID: 1136079

Which of the following is the best KPI for determining the performance of the information security controls and policies?

A) The number of incidents resolved

B) The number of incidents resolved per year within 2 minutes of occurrence

C) The number of incidents reported

D) The number incidents resolved per year

Explanation

Key performance indicators (KPIs) are quantitative measures of activity. These measures are set up to assess how security systems are performing, such as the number of incidents resolved in a year within 2 minutes. This information allows response teams to determine how their information security controls are performing. The personnel must be trained to develop consistent and reliable tools for producing these measurements.

The number of incidents reported does not measure whether the controls have resolved those incidents over a certain time period. While this is a KPI, it does not help to determine performance. There is no way to determine if the number of reported incidents is increasing or decreasing, which can have a direct effect on how the response teams react.

The number of incidents resolved does not give information about the time period in which these resolved incidents were reported. It does not provide adequate information to response teams or measure the performance of the teams.

The number of incidents reported per year is a better measure than the number of incidents reported or resolved, but does not give sufficient information about how long the incidents took to resolve.

Objective:
Information Security Incident Management

Sub-Objective:
Organize, train and equip incident response teams to respond to information security incidents in an effective and timely manner.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.6 Incident Management Metrics and Indicators

Question #17 of 150

Question ID: 1138439

Which of the following activities would determine whether control objectives are being adequately supported or not?

A) Gap analysis
B) **Business impact analysis (BIA) development**
C) Risk assessment
D) Log analysis

Explanation

A gap analysis would determine whether control objectives are being adequately supported. A gap analysis of incident response investigates the differences between the current incident response capabilities and the desired incident response capability. This analysis identifies the processes that need to be improved and determines what resources are needed to achieve the desired capability.

All of the other options can be used as supplementary materials to the gap analysis.

A risk assessment values the assets, identifies the risk, and ranks the risks. It will document the current risks but will not determine whether control objectives are being adequately supported or not.

Log analysis can detect and determine the nature of attacks on the system. Log analysis does not determine whether control objectives are being adequately supported or not.

A business impact analysis (BIA) can be used in conjunction with the risk assessment to determine asset criticality, and can be used to identify which controls are needed based on identified risks.

Objective:
Information Security Program Development and Management

Sub-Objective:
Integrate information security requirements into organizational processes to maintain the organization's security strategy.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.7 Defining an Information Security Program Road Map, 3.7.3 Gap Analysis - Basis for an Action Plan

, Chapter 2: Information Risk Management, 2.5 Implementing Risk Management, 2.5.1 Risk Management Process

---

Question #18 of 150

Question ID: 1135997

Which of the following statements best describe the RPO? (Choose all that apply.)

A) **The minimal level of service that must be restored following a disaster**

B) The time frame in which operations must be restored before the organization's existence is threatened

C) The length of time an organization may operate in recovery mode

- **D)** The maximum amount of time allowed to recover resources
- **E)** **The acceptable amount of data that can be lost following a disaster**
- **F)** **The earliest point in time at which data will be recovered**

Explanation

The recovery point objective (RPO) is determined by how much data an organization can acceptably lose after a disaster. It is the earliest point in time at which data will be recovered.

The maximum amount of time allowed to recover resources is the recovery time objective (RTO).

The minimal level of service that must be restored following a disaster is the service delivery objective (SDO).

The length of time for an organization to operate in recovery mode is the maximum tolerable outage (MTO).

The amount of time that can be expended to restore operations before the organization's existence is threatened is the acceptable or allowable interruption window (AIW).

Objective:
Information Risk Management

Sub-Objective:
Ensure that information security risk is reported to senior management to support an understanding of potential impact on the organizational goals and objectives.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.9 Operational Risk Management, 2.9.3, Recovery Point Objectives

---

Question #19 of 150

Question ID: 1136030

Which of the following represents a security awareness tool?

- **A)** Quarterly security training classes
- **B)** Certifications
- **C)** **Posters**
- **D)** Security violation alarms

Explanation

Posters represent a security awareness tool. These serve as visual reminders of security policies.

Quarterly security training is not correct. These are educational tools, but they do not serve as day-to-day security awareness reminders.

Certifications are educational tools, but certifications are not required for everyone in the organization.

Security violation alarms follow the occurrence of a security issue. Awareness training seeks to be proactive to prevent security incidents.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish, communicate and maintain organizational information security standards, guidelines, procedures and other documentation to guide and enforce compliance with information security policies.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.10 Security Program Management and Administrative Activities, 3.10.2 Security Awareness Training and Education

---

Question #20 of 150

Question ID: 1135907

Which of the following is needed to begin developing an information security strategy?

A) **Well-defined objectives**
B) Knowledge of the security threats that exist
C) Applicable regulations
D) The cost of mitigation

Explanation

The initial requirements to develop a security strategy (or to achieve any objective) are well-defined objectives and an understanding of the current risk conditions. That is, before the information security strategy is developed, you must spend time studying where the organization is now and where the organization needs to go.

Knowledge of the existing threats forms a backdrop to developing the security strategy, but it is not part of the initial process.

The cost of mitigation is also not part of the initial development of the strategy. Without knowing the security objectives, there is no way of knowing what the cost will or might be or what mitigations will be needed.

Applicable regulations will be included in the strategy, but are not part of the initial considerations.

Objective:
Information Security Governance

Sub-Objective:
Establish and/or maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and/or ongoing management of the information security program.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.7 Information Security Strategy Overview

Question #21 of 150

Question ID: 1135943

The CEO of a company has not received any reports regarding exploits, attacks, or threats. She therefore assumes that the company has not been attacked, and is considering reducing support for the information security program. How best can this situation be remedied?

A) Senior management must be given training to understand the need for information security.

B) Senior management must be presented with reports of the number of threats averted.

C) Senior management must be given regular updates regarding the state of the information security program and its continuing benefits.

D) Senior management must be presented with the key goal indicators.

Explanation

The information security manager must produce regular updates for senior management regarding the state of the information security program and its continuing benefits. Senior management must be kept up to date on how the security program is working and how it supports the business goals. Without that information, it might be assumed that the expenditure is not needed because there are apparently no successful attacks.

Senior management should not be given training to understand the need for information security. Presumably, since the program is already implemented and operational, senior management was already supporting the program and already received training.

Presenting senior management with the number of threats averted would not be the best remedy. A better indicator would be graphs showing how the number of averted threats has changed over time compared to the number of threats over time, especially in relationship to the appropriate key goal indicators.

Presenting senior management with the key goal indicators (KGIs) would not be the best remedy. Just giving the goals does not reflect whether the goals are being met. Additionally, senior management probably would have been aware of these goals already

Objective:
Information Security Governance

Sub-Objective:
Establish, monitor, evaluate and report key information security metrics to provide management with accurate and meaningful information regarding the effectiveness of the information security strategy.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.4 Risk Management Roles and Responsibilities, 1.4.2 Information Security Roles and Responsibilities

, Chapter 1: Information Security Governance, 1.13 Action Plan to Implement Strategy, 1.13.5 Action Plan Metrics

---

Question #22 of 150

Question ID: 1135971

Which concept describes determining the disparity between existing controls in a system and the control objectives?

A) Performing a cost-benefit analysis

B) **Performing a gap analysis**

C) Determining the risk management context

D) Completing the BIA

Explanation

Performing a gap analysis determines any disparity (gap) between existing controls and the control objectives. Control objectives can change as threats, exposures, and business objectives change.

Given a certain level of risk and impact, the cost benefit analysis will determine level of controls needed to achieve acceptable risk. However, a cost-benefit analysis does not compare existing controls to control objectives.

Determining the risk management context defines the processes to be assessed, the scope of risk management activities, the roles and responsibilities of those participating risk management, and organizational culture. It is used to establish control objectives, but does not review existing controls.

Completing a business impact analysis (BIA) is obtains a list of all assets and resources on the system and the impact to the organization if those assets and resources are lost. It is used to establish control objectives, but does not review existing controls.

Objective:
Information Risk Management

Sub-Objective:
Determine whether information security controls are appropriate and effectively manage risk to an acceptable level.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.5 Implementing Risk Management, 2.5.6 Gap Analysis

Question #23 of 150

Question ID: 1136058

A company has implemented multiple systems. They want a solution that can classify and respond to incidents in one or more of the implementations by combining input from multiple systems. The solution must automate the processing of the information. What kind of incident management system would be most appropriate?

- **A) SIEM**
- **B)** NIDS
- **C)** Syslog
- **D)** HIDS

Explanation

A Security Information and Event Manager (SIEM) combines the output of multiple logs across multiple systems and correlates that data into meaningful incident information. It can prioritize incidents and generate alarms if the incident severity is higher than a preset level. It tracks the history, the source or sources of the potential attack, and the targets of that potential attack.

A host-based intrusion detection system (HIDS) monitors traffic into and out of an individual host according to preset rules. This data can be collected by an SIEM, but a HIDS only monitors one host, not multiple implementations.

A network-based IDS (NIDS) monitors into and out of an individual network, similar to the HIDS. The data it accrues can be collected by an SIEM. This only monitors traffic on the network and may not provide a complete picture of an incident. An SIEM would centralize all the content from multiple sources, including the NIDS.

Syslog is a server to which network logs can be sent. The syslog format is not generally intended for human readability and makes automated analysis of the log data challenging.

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate classification and categorization of and response to incidents.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.2 Incident Response Procedures, 4.2.5 Incident Management Systems

Question #24 of 150

Question ID: 1136073

A security analyst notices some suspicious activity on the network but does not think it is serious enough to escalate. He decides to contain it. Several hours later, he observes that the activity is increasing and that containment requires additional personnel. The person he is supposed to contact to escalate this incident is tied up with another issue, and will require several hours to respond. In the meantime, the situation is severely affecting business operations. How should this situation have been avoided?

- **A) The escalation process should have included alternate contacts.**
- **B)** Additional mitigation measures should have been installed.
- **C)** The analyst should have called someone other than the designated person for incident escalation.
- **D)** The escalation process should have included a required response time.

Explanation

The incident response plan should have included a directory of contacts. It should describe the procedures to be followed during an incident and indicate when it should be escalated. Each contact person listed should have an equally capable alternate to contact.

The analyst should have called someone else only after the primary contact was found to be unavailable and AFTER consulting with the incident response plan to determine the secondary contact.

The incident response plan should include a time limit for each action, but the time limit is not the issue here. The unavailability of the primary contact means that a secondary contact should have been provided by the incident response plan.

Additional mitigation measures do not fix all incidents. The amount of mitigation required depends on a number of factors, and the goal is reduce the risk to acceptable levels. Incidents will still occur, and some cannot be predicted, such as zero-day attacks. The last line of defense is proper execution of a well-prepared incident response plan.

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain incident notification and escalation processes to ensure that the appropriate stakeholders are involved in incident response management.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.9 Developing an Incident Response Plan, 4.9.4 Escalation Process for Effective Incident Management

Question #25 of 150

Question ID: 1135959

Before risk can be prioritized, what must be done?

A) Mitigation controls must be put in place.

B) A BIA must be performed.

C) Roles and responsibilities must be determined.

D) The cost of mitigation must be determined.

Explanation

Before risk can be prioritized, a business impact analysis (BIA) should be performed. The BIA produces an inventory of all assets and determines the impacts of the loss of those assets. The outcome of this process allows the risks to be prioritized for the organization. Without understanding asset criticality and loss impact, it is not possible to prioritize risks.

You would not implement mitigation controls before prioritizing risks. Implementing controls comes later and depends on the outcome of the BIA, threat analysis and likelihood of an exploit, as well as the value of the assets being considered weighed against cost of the mitigation.

You would not determine roles and responsibilities before prioritizing risks. Determining responsibilities and personnel depends on what controls, if any, will be put in place.

You cannot determine the cost of mitigation before prioritizing risks because the value of the assets and the risk to those assets must be determined first.

Objective:
Information Risk Management

Sub-Objective:
Ensure that risk assessments, vulnerability assessments, and threat analyses are conducted consistently, at appropriate times, and to identify and assess risk to the organization's information.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.8, Information Asset Classification, 2.8.2 Impact Assessment and Analysis

Question #26 of 150

Question ID: 1185745

The value of an asset in a company is subject to market forces, which sometimes undergo large changes in a short time. What would be the most cost effective way of protecting the asset?

- **A)** The company's expenditure for security should be based on the average of the fluctuations of the asset's value.
- **B)** The company's expenditure for security should be calculated for the asset value's low point.
- **C)** The company's expenditure for security should be calculated for the asset value's high point.
- **D)** **The expenditure for securing the asset should be adjusted to provide maximum Return on Security Investment (ROSI) according the changing value of the asset.**

Explanation

Expenditures for security of assets whose value undergoes rapid or extreme fluctuation should be based on the average of the fluctuations of the asset's value. The cost of asset mitigation should be optimized. Further, it is impractical to change the mitigation of the asset every time the value of the asset changes. When the value falls, reducing the amount of controls can also reduce the controls for other assets. When the value rises, purchasing and adding new controls can take time, during which the value can fall causing the expenditure to be unnecessary.

ROSI is in part based on the asset value and policy and business goals. ROSI must determine which value to use, and adjusting the controls to rapidly changing asset values is not practical.

Expenditures based on the asset’s high or low values is not optimal because the company will either overspend or underspend when the asset rises or falls in value.

Objective:

Information Security Governance

Sub-Objective:
Identify internal and external influences to the organization to ensure that these factors are continually addressed by the information security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.12 Strategy Constraints, 1.12.6 Costs

---

Question #27 of 150

Question ID: 1185763

Which of the following protects the organization after an internal breach of proprietary data?

A) Performance review

B) Log review

C) Visible enforcement of the security rules

D) Nondisclosure agreement

Explanation

A nondisclosure agreement (NDA) protects the organization after an internal breach of proprietary data. All employees should sign an NDA to protect the organization. The NDA serves as a reminder to the employee from day one. Thus, if the employee causes a breach, the organization has legal remedies to help to offset the damage caused by the breach. The NDA serves as administrative preventive control.

Log review can reveal the breach, but it is not a preventive control. It is a detective control.

Performance reviews will not protect the organization from an internal breach of proprietary data. The review examines the employee’s performance. Performance reviews are administrative controls. They can be considered deterrent controls because they can be used to reinforce good behavior and deter bad behavior.

Visible enforcement of the security rules serve as a deterrent, but will not stop a determined attacker.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish, promote and maintain a program for information security awareness and training to foster an

effective security culture.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.10 Security Program Management and Administrative Activities, 3.10.2 Security Awareness Training and Education

Question #28 of 150

Question ID: 1138434

What level of metrics will enable you to determine whether the information security program is achieving its defined objectives and outcomes?

A) **Strategic**

B) Systemic

C) Operational

D) Management

Explanation

Strategic metrics will determine whether the security program is achieving the defined objectives and outcomes. Strategic metrics are designed to determine if the security program is on track.

Management metrics are used to manage the level of policy and standards compliance, incidents, response effectiveness, and resource utilization.

These metrics are used common technical and procedural metrics used to measure open vulnerabilities and other technical operations.

Systemic is not an official category of metrics.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish, communicate and maintain organizational information security standards, guidelines, procedures and other documentation to guide and enforce compliance with information security policies.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.13 Security Program Metrics and Monitoring, 3.13.1 Metrics Development

Question #29 of 150

Question ID: 1135982

What follows the risk identification step in the IT risk management life cycle?

A) Risk Response and Mitigation

B) Initiation

C) **Risk Assessment**

D) Risk Control Monitoring and Reporting

Explanation

The four stages of the IT risk management life cycle are IT risk Identification, IT risk assessment, risk response and mitigation, and risk and control monitoring and reporting. As a life cycle, this process is continuous. Once monitoring and reporting is completed, the lifecycle returns to the identification step.

Initiation is not one of the steps in the IT risk management life cycle.

Objective:
Information Risk Management

Sub-Objective:
Facilitate the integration of information risk management into business and IT processes to enable a consistent and comprehensive information risk management program across the organization.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.11 Risk Management Integration with Life Cycle Processes, Figure 2.26: The IT Risk Management Life Cycle

Question #30 of 150

Question ID: 1185747

Which of the following is required to establish a process to protect an organization's assets? (Choose all that apply.)

- **A) Perform a risk analysis.**
- **B)** Analyze event logs.
- **C) Perform a BIA.**
- **D) Refer to TOGAF for guidance.**
- **E) Estimate ROSI.**
- **F) Establish security governance.**

Explanation

To establish a process to protect an organization’s assets, it is necessary to perform a business impact analysis (BIA) to inventory all assets to determine the impact of a risk of the organization's resources. This prioritizes the assets according to the sensitivity of each, which is used to establish as system of classification and asset ownership. Return on Security Investment (ROSI) is an estimate of how much will be saved by the investment in mitigation methods. ROSI is necessary for establishing the process of protection of the organization's assets. Risk analysis estimates the likelihood of a loss. This is important to estimate risk, which is the likelihood of a threat actor exploiting a vulnerability to cause damage to the organization's information resource and systems.

Establishing security governance is not correct. Risk management must be addressed without consideration of how far along the organization has developed its governance.

The Open Group Architecture Framework (TOGAF) is not required to establish a process to protect an organization's assets. TOGAF is framework to describe the elements in an enterprise's architecture and how they must relate to each other.

Analysis of event logs is not correct. It is a detective measure that investigates events and incidents that have already occurred. It is a retrospective measure.

Objective:
Information Risk Management

Sub-Objective:
Establish and/or maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.1 Risk Management Overview, 2.1.1: The Importance of Risk Management

HYPERLINK "https://www.amazon.com/CISM-Review-Manual-15th-Isaca/dp/1604205083/ref=as_sl_pc_qf_sp_asin_til?tag=transcender02-20&linkCode=w00&linkId=0a13ea046dadf2cc511dd1e82cb7d97a&creativeASIN=1604205083" CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.7 Risk Assessment, 2.7.10: Threats

---

Question #31 of 150

Question ID: 1185760

Which role is responsible for developing the security monitoring process and metrics to determine the effectiveness of the information security processes in protecting an organization’s information assets?

A) **Information security manager**

B) System administrator

C) Individual business owners

D) Chief information officer (CIO)

Explanation

The information security manager is responsible for developing the security monitoring process and metrics to determine the effectiveness of information security processes for protecting the organization’s information assets.

The accountable person is the individual who is ultimately answerable for the activity or decision. The responsible person is the individual who actually completes the task.

The CIO is responsible for IT planning, budgeting, and performance.

The individual business owners are responsible for assigning the proper security controls.

The system administrator implements the security controls.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish and maintain information security processes and resources to execute the information security

program in alignment with the organization's business goals.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.11 Security Program Services and Operational Activities, 3.11.1 Information Security Liaison Responsibilities

, Chapter 1: Information Security Governance, 1.4 Risk Management Roles and Responsibilities, 1.4.1 Key Roles

, Chapter 3: Information Security Program Development and Management, 3.11 Security Program Services and Operational Activities, 3.11.5 Management of Security Technology

Question #32 of 150

Question ID: 1136033

All employees of an organization should undergo training in the following areas, EXCEPT:

A) Contingency plans

B) Incident response

C) Log reviews

D) Social engineering

Explanation

All employees of an organization should undergo training in all the areas listed EXCEPT log reviews. Logs should be securely protected and accessed only by suitable analysts who will have specific training on keeping logs secure and analyzing events in logs.

Incident response, contingency plans, and social engineering are all areas in which all employees should undergo training. This ensures that they know what to do if there is a breach, and provides training for avoiding social engineering scams.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish, promote and maintain a program for information security awareness and training to foster an

effective security culture.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.10 Security Program Management and Administrative Activities, 3.10.2 Security Awareness Training and Education

Question #33 of 150

Question ID: 1138427

Which of the following frameworks can be used to help develop information security objectives?

A) Zachman

B) ISO/IEC 15288:2015

C) NIST SP 800-53

D) **ISO/IEC 27001:2013**

Explanation

The ISO/IEC 27001:2013 framework provides high-level requirements for information security programs.

The ISO/IEC 15288:2015 framework addresses life-cycle processes but without addressing security.

The NIST SP 800-53 framework provides security controls for risk management.

The Zachman framework is an enterprise architectural framework that allows you to classify various aspects of an organization by functional areas.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish and/or maintain the information security program in alignment with the information security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.5 The Information Security Management Framework, 3.5.2 ISO/IEC 27001:2013

Question #34 of 150

Question ID: 1136018

A service level agreement (SLA) with an outsourced vendor will include wording about all of the following activities, EXCEPT:

- **A)** Undo downtime
- **B)** **Authorized access guidelines**
- **C)** A security breach of the vendor's systems
- **D)** Standard operating procedures by the vendor

Explanation

A service level agreement (SLA) with an outsourced vendor will NOT include verbiage covering a security breach of the vendor's system. The SLA generally includes items like compliance with industry and regulatory requirements, performance requirements, and access limitations. Even if a vendor or any organization is in compliance with regulatory requirements, it does not guarantee that the vendor or organization is secure. Because breaches can happen anywhere, an SLA does not usually include wording about a security breach of the vendor's system.

All of the other options will be included in the SLA.

Downtime requirements and penalties should be covered in the SLA. Standard operating procedures are described in the SLA. Authorized access guidelines are described in the SLA.

Objective:
Information Security Program Development and Management

Sub-Objective:
Identify, acquire and manage requirements for internal and external resources to execute the information security program.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.11 Security Program Services and Operational Activities, 3.11.9 Outsourcing and Service Providers

Question #35 of 150

Question ID: 1185773

A company has incurred a breach where personally identifiable information (PII) was released. This PII is regulated by HIPAA and the organization is potentially at risk for a legal violation. The organization needs to prove that it met the regulatory requirements for protection of that data. Which of the following should the organization do?

A) Shut down the affected systems to protect them from further attack.

B) Move the affected systems to a secure location.

C) **Document the organizational policies and procedures regarding data and evidence protection.**

D) Make copies of the drives that were compromised.

Explanation

Documenting the organizational procedures and policies regarding data and evidence protection would be the most important means for proving regulatory compliance. Adhering to the regulations does not, however, guarantee the absence of risk. Following regulations and documenting the procedures followed should remove the organization's liability if a breach occurs.

Shutting down systems is not always the best strategy and is not universally accepted as a response to a breach. Shutting down the system may result in losing volatile data that could be important for the investigation. Rather, the breached system should be isolated from the rest of the organization’s networks.

Making copies of disk drives is not an acceptable response with respect to the chain of evidence and forensic investigations. If copies need to be made, only bit copies of the hard drive should made. In addition, a hash value should be documented for any bit copies that are made.

Rather than moving the affected system, it should be isolated and contained. It should be protected from access by any individuals except for authorized investigators.

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain processes to investigate and document information security incidents in order to determine the appropriate response and cause while adhering to legal, regulatory and organizational requirements.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.13 Postincident Activities and Investigation,

---

Question #36 of 150

Question ID: 1136040

An organization discovers that in case of a disruption, they are unable to meet the RPO requirement. It is important that the defined RPO be met. What should be done to change this?

A) Increase the RPO.

B) Employ RAID for the backup systems.

C) Deploy faster servers for the backup systems.

D) **Run more frequent backups.**

Explanation

The company should run more frequent backups. This shortens the time between backups so that the recovery point objective (RPO) can be achieved.

Increasing the RPO is not correct. This is a business decision that should be carried out only after careful review by management. Increasing the RPO means that a larger amount of data will be lost.

Deploying faster servers will not affect the RPO. If the backups are spaced too far apart, then a faster server will not fulfill the requirements.

Employing RAID backups will not affect the RPO. RAID simply provides redundancy in the case of the loss of a hard drive, and while it can improved performance, achieving the RPO depends on the frequency of backups.

Objective:
Information Security Program Development and Management

Sub-Objective:
Integrate information security requirements into organizational processes to maintain the organization's security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 4 Information Security Incident Management, 4.10 Business Continuity and Disaster Recovery Procedures, 4.10.6 Basis for Recovery Site Selections

---

Question #37 of 150

Question ID: 1136020

When reviewing the information security program, the information security manager determines that some areas are not being covered adequately due to personnel shortages. Filling these gaps is an urgent issue. How should the manager handle this situation in the most cost-effective manner?

A) Assign more tasks to existing personnel.

B) Hire additional personnel.

C) **Outsource the areas that lack coverage to vendors.**

D) Reduce the scope of the program to match the available personnel resources.

Explanation

The manager should outsource the areas that lack coverage to other vendors. Using reliable vendors with excellent security records will probably be the most cost effective method. For one thing, outsourcing can unload some of the responsibilities of the manager and not incur long-term costs, such as employee benefits.

Reducing the scope of the security program would introduce vulnerabilities into the system.

Assigning more tasks to existing personnel will take attention away from the tasks that people are already doing and overload them, leading to errors and shortcuts.

Hiring and training new people takes time. Because the need for coverage is urgent, this is not a viable option in the short term.

Objective:
Information Security Program Development and Management

Sub-Objective:
Identify, acquire and manage requirements for internal and external resources to execute the information security program.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.10 Security Program Management and Administrative Activities, 3.10.11 Vendor Management

Question #38 of 150

Question ID: 1135977

In which phase of the SDLC should risk first be addressed?

A) Operation or maintenance

B) Development or Acquisition

C) Initiation

D) Implementation

Explanation

Risk should first be addressed at the beginning or Initiation phase of the system development life cycle (SDLC). This includes consideration of risk that the new system or software may present as well including secure development processes. Failing to consider risk until later in the process can add to product development or deployment delays, which can increase the cost.

While risk should be considered throughout the SDLC, it should be first considered at the start. None of the other options is the first phase of the SDLC.

Consideration of risk should be included in all phases of the SDLC. In the implementation phase, the product development should be done against the products requirements risk. If risk is not considered at this stage, it may require reworking the software later to comply with risk requirements, a process that can be difficult and inject new vulnerabilities.

Consideration of risk should not be an add-on to the system or software, and therefore consideration of risk during development/acquisition phase is important here. If risk is not considered when a product is being acquired, vulnerabilities that show up later on can adversely affect the business.

Continued consideration of risk during the operation phase is important to determine if the product is continuing to perform according to the requirements. This should not be the first time that risk is considered in the product since it is already deployed.

The phases of the SDLC are as follows:

1. Initiation

2. Development or Acquisition
3. Implementation
4. Operation or Maintenance
5. Disposal

Objective:
Information Risk Management

Sub-Objective:
Facilitate the integration of information risk management into business and IT processes to enable a consistent and comprehensive information risk management program across the organization.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.11 Risk Management Integration with Life Cycle Processes, 2.11.1 Risk Management for IT System Development Life Cycle

---

Question #39 of 150

Question ID: 1135979

What is the correct order of activities for risk assessment in COBIT 5?

A) **None of the above**

B) Risk evaluation, Risk Identification, Context establishment, Risk evaluation, Risk Treatment

C) Context establishment, Risk identification, Risk analysis, Risk evaluation, Risk treatment

D) Risk Identification, Context Establishment, Risk evaluation, Risk Analysis, Risk Treatment

Explanation

The order of activities for establishing an information security risk management process according to COBIT 5 is:

1. Context Establishment
2. Risk Identification
3. Risk Analysis

4. Risk Evaluation
5. Risk Treatment

COBIT 5 is a framework for assessing risk. It is aligned with ISO/IEC 27005:2011, and includes risk identification, analysis, and evaluation.

Objective:
Information Risk Management

Sub-Objective:
Facilitate the integration of information risk management into business and IT processes to enable a consistent and comprehensive information risk management program across the organization.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.6 Risk Assessment and Analysis Methodologies, Figure 2.4 Information Security Risk Management Process

---

Question #40 of 150

Question ID: 1185756

Which of the following statements is most important for the security program?

A) A gap analysis of the current risk and the acceptable level of risk must guide the security program.

B) **The security program is the execution of a well-developed security strategy.**

C) The security program must be designed such that risk is eliminated.

D) Management must have a choice of controls.

Explanation

The security program must be the execution of a well-developed security strategy. The information security strategy defines the direction and goals for the information security program.

A gap analysis is a comparison between the current state of the program and the desired state. This analysis is not possible until the security strategy defines the desired state. The gap analysis does not guide the security program; rather, the security strategy does.

Management does not require a choice of controls in the security program. The security strategy must define the organization's security goals and document which assets must be protected. The security strategy then defines the security controls. In some cases, it is not possible to provide a choice of controls because only a single control will provide the protection needed.

It is not feasible to eliminate risk, only to determine an acceptable level of risk

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish and/or maintain the information security program in alignment with the information security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.0 Introduction

---

Question #41 of 150

Question ID: 1135986

Which factors need to be considered when assessing risk? (Choose all that apply.)

A) Frequency of occurrence

B) Type of threat

C) Threat actor

D) Vulnerabilities

E) **Impact of exploit**

F) **Value of asset**

Explanation

All of the selections need to be considered when assessing risk. Risk is generally defined at the probability that a threat actor can exploit a vulnerability in a system, thereby causing harm. Quantification of harm requires that you value both the assets and the impact of an exploit.

The type of threat is determined by the type of threat actor and whether or not the actor represents a low level threat, such as from a script kiddie, or from an organized criminal who means to steal personally identifiable information or financial assets from the organization.

The frequency of occurrence of an event will in part determine the resources needed to protect the assets and the cost of the losses that might occur.

Objective:
Information Risk Management

Sub-Objective:
Monitor for internal and external factors that may require reassessment of risk to ensure that changes to existing, or new, risk scenarios are identified and managed appropriately.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.9 Determining the Current State of Security, 1.9.1 Current Risk

, Chapter 2: Information Risk Management, 2.7 Risk Assessment

---

Question #42 of 150

Question ID: 1136053

The information security manager has determined that the number of network packets processed by an IDS node has decreased over the last few weeks. The manager is attempting to determine the cause. Which type of metric is being used by the manager?

A) Security cost effectiveness

B) Regulatory compliance

C) Genuine

D) **Operational productivity**

Explanation

The type of metric being used by the manager is operational productivity. This metric is a measure of how well the technical resources are performing.

Regulatory compliance is not being used. The number of network packets is not a regulatory issue. Regulatory compliance metrics would measure compliance with procedural or process standards.

Security cost effectiveness is not being used. An example of this type of metric is the cost of the network packets being processed.

Genuine is not a metric. This is an attribute applicable to all metrics in that metrics should not be subject to manipulation. But itself, this is not a measurable metric.

Objective:

Information Security Program Development and Management

Sub-Objective:

Compile and present reports to key stakeholders on the activities, trends and overall effectiveness of the IS program and the underlying business processes in order to communicate security performance.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.13 Security Program Metrics and Monitoring

---

Question #43 of 150

Question ID: 1135935

The CEO of an organization is struggling to balance the costs of development of a potentially lucrative new product against the costs incurred by the information security program. What information could the CISO use to continue funding the information security program?

A) Lists of new exploits that might represent a serious threat to the organization

B) **Estimates of the costs savings from the exploits that were prevented**

C) Data regarding the number of exploits that have been prevented

D) Lists of all the resources that are being protected

Explanation

Estimates of cost savings from the exploits that were prevented is the best approach to convincing the CEO of maintaining or even increasing his support of the security program. The CEO is primarily interesting in the business operations, and this kind of information is important for determining the organization's budget.

Data regarding the number of exploits does not present business data to the CEO. The number of exploits does not provide any real insight into savings for the company.

Listing new exploits would not be of interest to the CEO unless he understood how they could impact business.

Listing the protected resources would not be convincing without information regarding cost savings.

Objective:

Information Security Governance

Sub-Objective:

Gain ongoing commitment from senior leadership and other stakeholders to support the successful implementation of the information security strategy.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.4 Risk Management Roles and Responsibilities, 1.4.2 Information Security Roles and Responsibilities

, Chapter 1: Information Security Governance, 1,4 Risk Management Roles and Responsibilities, 1.4.1 Key Roles

---

Question #44 of 150

Question ID: 1135930

Company XYZ's regulations state that it must retain records for a minimum of two years. Company XYZ's internal business policies require it to retain records for three years. Company ABC's regulations state that it must retain records for a minimum of five years. Company ABC's internal business policies require it to retain records for seven years. After the companies are integrated into one organization, they will still be governed by the regulations that affected both separate companies. What should the record retention period be for the new company?

A) **The retention period should be 7 years.**
B) The retention period should be 3 years.
C) The retention period should be 2 years.
D) The retention period should be 5 years.

Explanation

The retention period should be seven years. The retention policies should meet both the regulations and the business requirements of the newly merged organization. The regulations set a baseline for retention policies, and the policies of the organization can exceed that baseline. The combined company is a new company in the sense that it may be governed by different regulations and laws than previously applied to the two parent companies. You should always adopt the longest retention period if the retention periods dictated by the regulations and internal business policies are different.

The retention periods of two, three, or five years are not correct. The retention period is determined by the company's policies in excess of what is required by regulations, which in this case would be the requirements of the internal policies set by Company ABC.

Objective:
Information Security Governance

Sub-Objective:
Identify internal and external influences to the organization to ensure that these factors are continually addressed by the information security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.12 Strategy Constraints, 1.12.1 Legal and Regulatory Requirements

---

Question #45 of 150

Question ID: 1135944

A CISO for a very large corporation wants to do a security assessment to determine the state of the security program in the company. What would be the biggest challenge facing the CISO?

A) Getting senior management support
B) Gaining support from the employees
C) Performing vulnerability analyses
D) **Identifying assets**

Explanation

Identifying assets is part of a business impact analysis (BIA), which is part of a current-state evaluation. The obstacles for this identification are the number of resources that have to be identified. Some tools exist to determine some of the software running on the different devices as well as enumerate those devices. However, these tools do not list other assets, such as information that is critical for business operations.

Obtaining this information would most likely have to be done manually with the aid of the various business owners. Impacts cannot be prioritized if assets are not identified.

Getting senior management support would not be the best remedy. Because the organization has a CISO and a security program, senior management most likely already supports the security program.

Performing vulnerability analyses would not be the best remedy. There are numerous tools that automate this process, such as NESSUS, nmap, and openVAS.

Getting support from employees would not be the best remedy. Because senior management is supporting the security program and there are probably consequences in place for non-compliance with the organization's security policies, most employees should already be on board.

Objective:
Information Security Governance

Sub-Objective:
Establish, monitor, evaluate and report key information security metrics to provide management with accurate and meaningful information regarding the effectiveness of the information security strategy.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.3 Effective Information Risk Management, 2.3,1, Developing a Risk Management Program

, Chapter 1: Information Security Governance, 1.9 Determining the Current State of Security, 1.9.1 Current Risk

, Chapter 1: Information Security Governance, 1.11 Strategy Resources, 1.11.16. Business Impact Analysis

---

Question #46 of 150

Question ID: 1136091

The incident response plan includes several phases. Which of the following is involved in the containment phase?

A) Obtaining the most recent backups

B) Verifying if an incident has occurred

C) Performing a vulnerability analysis

D) Activating the incident management team

Explanation

The containment phase includes activating the incident management team who has the responsibility of containing the incident. This phase also includes notification of the stakeholders, and obtaining and preserving evidence.

The verification phase includes developing procedures for handling incidents and developing a communication plan.

The eradication phase includes running vulnerability analyses and locating the most recent backups.

The phases of the incident response plan are as follows:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Lessons learned

Objective:
Information Security Incident Management

Sub-Objective:
Conduct postincident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.9 Developing an Incident Response Plan, 4.9.1 Elements of an Incident Response Plan

Question #47 of 150

Question ID: 1136088

What process should be undertaken if it is determined that the time to communicate an incident and the response time for acting on the incident is too long?

A) **Gap analysis**

B) Business continuity planning

C) Disaster recovery planning

D) Business impact analysis

Explanation

A gap analysis investigates the differences between the current incident response capabilities and the desired incident response capability. This analysis identifies the processes that need to be improved and determines what resources are needed to achieve the desired capability.

The business impact analysis (BIA) identifies possible events and considers the impacts of those events on the resources of the organization.

The business continuity plan (BCP) addresses various aspects of incidents and the processes for restoring operations.

The disaster recovery plan (DRP) defines the processes to recover business activities following an incident or disaster.

Objective:
Information Security Incident Management

Sub-Objective:
Conduct postincident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.9 Developing an Incident Response Plan, Gap Analysis - Basis for an Incident Response Plan

, Chapter 4: Information Security Incident Management, 4.9 Developing an Incident Response Plan, 4.9.3 Business Impact Analysis

---

Question #48 of 150

Question ID: 1138430

Many, if not most, breaches occur due to insider threats or inadvertent actions on the part of an employee. How should the security manager deal with these threats?

A) Install host intrusion detection systems.

B) **Build a security-aware culture.**

C) Implement a data loss prevention system.

D) Impose stricter technological controls.

Explanation

The manager should deal with this threat by building a security aware culture. This includes developing relationships with people in other departments, implementing training sessions and quizzes, and impressing the importance of the roles within the organization and that each person takes ownership for their part in the security of the organization.

The manager should not impose stricter technological controls. While these will reduce the likelihood of breaches, it will not necessarily protect against all breaches that originate inside the company.

The manager should not implement a data loss prevention (DLP) system. This will also reduce some kinds of breaches, but data can be hidden outside the scope of the DLP.

The manager should not install a host intrusion detection system (HIDS). These generally detect incoming traffic on a single host and are not used to control traffic within a network.

Objective:
Information Security Program Development and Management

Sub-Objective:
Identify, acquire and manage requirements for internal and external resources to execute the information security program.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.10 Security Program Management and Administrative Activities, 3.10.2 Security Awareness Training and Education

---

Question #49 of 150

Question ID: 1135919

The board of directors is developing a policy that will require the IT department to maximize network performance. It will also require the information security program to maximize security. How should senior management respond to the board of directors' proposed policy?

A) The CISO should ask for the directive to specify an adequate level of performance for IT and an acceptable level of risk for information security.

B) **The CISO should ensure that the security program links the policy to the business objectives.**

C) Senior management should decrease the network performance policy requirements before implementing it.

D) Senior management should create a security policy that also maximizes network performance.

Explanation

The CISO should change the goals to specify an adequate level of performance for IT and an acceptable level of risk for information security. Since the policy from the BOD is under development, the board members should be informed that these are conflicting goals and can expose the organization to an unacceptable level of risk. It is not possible to maximize network performance while simultaneously maximizing security.

Linking the policy to business objectives is not correct. In this case two objectives regarding IT and security are mutually exclusive. If network performance is maximized, it often means that the security program suffers. If the security program is maximized, it often means that network performance suffers.

Creating a security program that also maximizes network performance is not correct. Given conflicting directives, a security program that maximizes network performance is likely to provide inadequate security, which does not comply with regulations or the level of acceptable risk.

It is not up to senior management to modify the policy from the board of directors before implementing it. The policy from the board of directors is still under development and not final. The network performance policy should only be lowered after a risk assessment is done and the security issues for the policy have been identified.

Objective:
Information Security Governance

Sub-Objective:
Integrate information security governance into corporate governance to ensure that organizational goals and

objectives are supported by the information security program.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.2.1 Effective Information Security Governance, 1.2.1 Business Goals and Objectives

, Chapter 1: Information Security Governance, 1.3 Roles and Responsibilities, 1.3.1 Board of Directors

, Chapter 1: Information Security Governance, 1.3 Roles and Responsibilities, 1.3.2 Senior Management

Question #50 of 150

Question ID: 1135963

What of the following steps must be included in developing a risk management program to ensure that risk and vulnerability assessments and threat analyses are conducted in a consistent and timely manner to identify the organization's risks? (Choose all that apply.)

A) Determine the scope and charter of the program.

B) Document the objectives of the program.

C) Define the reason for the program and its context.

D) Perform an inventory of assets, including identification, classification, and ownership.

Explanation

All of the listed options are steps in the risk management program.

According to ISACA, the steps in the risk management program are as follows:

- Define the reason for the program and its context.
- Determine the scope and charter of the program.
- Define the authority, structure, and reporting relationships for the program.
- Identify and classify assets, and determine asset owners.
- Document the objective of the program.
- Determine the methodologies to be used.
- Designate the team responsible for implementing the program.

Objective:

Information Risk Management

Sub-Objective:

Ensure that risk assessments, vulnerability assessments, and threat analyses are conducted consistently, at appropriate times, and to identify and assess risk to the organization's information.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.3, Effective Information Risk Management, 2.3.1 Development a Risk Management Program

---

Question #51 of 150

Question ID: 1136054

A set of metrics yields information regarding compliance, emerging risk, resource utilization, and alignment with business goals. To which group or role would these metrics be targeting?

A) **Senior management**

B) System administrators

C) IT security manager

D) Information security manager

Explanation

These metrics would be targeted to the information security manager. These metrics are classified as management or tactical metrics for management of the security program, which includes compliance with policy and standards and resource utilization.

The metrics are not targeted to senior management. Both senior management and the information security manager need strategic metrics to determine whether the security program is headed in the right direction. Senior management is not likely to be interested in emerging risk or resource utilization.

The metrics are not targeted to the IT security manager and the system administrator. These roles need more technical metrics, such as open vulnerabilities, patch manager status, firewall configuration data, and log reviews.

Objective:

Information Security Program Development and Management

Sub-Objective:

Compile and present reports to key stakeholders on the activities, trends and overall effectiveness of the IS program and the underlying business processes in order to communicate security performance.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.13 Security Program Metrics and Monitoring, 3.13.1 Metrics Development

Question #52 of 150

Question ID: 1185762

To determine what vulnerabilities exist in a network, a penetration tester is hired. What would be the best method for the pen tester to use to determine whether employee education trained employees to avoid social engineering attacks?

A) Surveying each employee about social engineering attacks

B) Sending a report to all employees about the statistics regarding phishing attacks.

C) Sending out quizzes to determine the level of awareness of social engineering attacks.

D) **Sending out a fake specially constructed phishing email that looks like an official company communication, with links directing the employee to a specially designed web site that informs the employee about what they did.**

Explanation

Sending a fake but official looking email will determine the effectiveness of employee training on social engineering. This type of testing will demonstrate to the company how effectively the information security training program performs, as well as providing direct and immediate feedback to the employee. It is designed to see how aware employees are when they are busy with their normally assigned tasks.

Surveys and quizzes are not correct. People will generally know the right answers, but these instruments do not test employees’ actual security performance during their everyday job activities.

Sending out reports about the phishing statistics would be part of an education and training program, but it would not test the employees’ retained knowledge from the training programs.

Objective:

Information Security Program Development and Management

Sub-Objective:

Establish, promote and maintain a program for information security awareness and training to foster an effective security culture.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.10 Security Program Management and Administrative Activities, 3.10.2 Security Awareness Training and Education

ISSA International Series: Trials & Tribulations of Social Engineering, https://www.brighttalk.com/webcast/16125/329181?utm_campaign=add-to-calendar&utm_medium=calendar&utm_source=brighttalk-transact

---

Question #53 of 150

Question ID: 1135933

You are developing a business case to gain support from senior management for enhancements to the security program that will cost a relatively large sum of money. You have included a current analysis of the system to show what areas need improvement. You have addressed requirements for the enhancements and the needs of the stakeholders. The report includes the approach, the resources required to implement and maintain the enhancements, and a review of the planned upgrades. Senior management rejects this proposal. Which of the following would be the best reason for the rejection?

A) **The key goal indicators are missing from the report.**

B) The technical details of the upgrades were not specified.

C) The report does not state what other companies are doing to protect against the emerging threats.

D) The project scope was not defined.

Explanation

The components of any business to be presented to senior management should generally include the project scope, current analysis, requirements, and the approach. In this case, the project scope was not defined. The project scope should define the business problem and any opportunities that may exist. Senior management is primarily concerned with the business goals of the organization and the strategies that support it. If the proposed enhancements are not shown to support the business goals, then most likely senior management will not be in favor of the proposal.

What other companies are doing, technical details, and key goal indicators are not generally included in the business case.

Objective:
Information Security Governance

Sub-Objective:
Gain ongoing commitment from senior leadership and other stakeholders to support the successful implementation of the information security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.4 Risk Management Roles and Responsibilities, 1.4.2 Information Security Roles and Responsibilities

---

Question #54 of 150

Question ID: 1185771

Which of the following is an example of a centralized incident management system?

A) Firewall

B) NIDS

C) **SIEM**

D) HIDS

Explanation

A security incident and event management (SIEM) system is an example of a centralized incident management system. This system identifies, monitors, records, and analyzes security events or incidents within a real-time IT environment. All the logs for the different security devices, such as routers, firewalls, HIDS, and NIDS, could send their data to a centralized SIEM system for analysis.

A host-based intrusion detection system (HIDS) will collect data regarding intrusions for a single host. It is not centralized because the data is collected for a single host, and because the data for each host is usually stored on each separate host.

A network-based intrusion detection system (NIDS) will collect data regarding intrusions for an entire network. It is not centralized because its log will only contain data on intrusions and not for any other type of event.

A firewall will manage the flow of network traffic between networks and will allow or deny traffic based on the rules that have been configured. It is not a centralized solution because the firewall logs will only contain data on traffic through that single firewall.

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate classification and categorization of and response to incidents.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.2 Incident Response Procedures, 4.2.5 Incident Management Systems

Question #55 of 150

Question ID: 1136093

What determines the basis and priority for the incident or disaster response plans?

A) RTO
B) **BIA**
C) SDO
D) AIW

Explanation

The basis and priorities for the incident and disaster response plans are determined by the impacts of those incidents and disasters, as determined by the business impact analysis (BIA). The BIA identifies and prioritizes all assets and resources for the organization, thereby determining which services are most important to protect and restore.

The recovery time objective (RTO) is a target for restoration of services. The order of restoration is determined by the BIA.

The acceptable interruption window (AIW) is the maximum amount of time that services can be restored before the company experiences severe problems. The recovery priorities are set by the BIA. Recovery operations should be less than the RTO, and definitely less than the AIW.

The service delivery objective (SDO) is the acceptable level of service that must be attained within the time period specified by the RTO. It does not specify the priorities of recovery.

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain integration among the incident response plan, business continuity plan and disaster recovery plan.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.10 Business Continuity and Disaster Recovery Procedures, 4.10.9 Integrating Incident Response with Business Continuity

Question #56 of 150

Question ID: 1135992

As part of his job duties, a government employee was tasked with classifying data as per the mandatory access control policy. The employee was suspected of misclassifying the data containing information about weapons systems. How should this data be classified?

A) Sensitive
B) Top Secret
C) Secret
D) Confidential

Explanation

Data with information about weapons systems should be classified as Top Secret.

The levels of data classification used by the government are, from highest to lowest:

- Top Secret - includes information that could gravely damage national security if disclosed, such as weapons blueprints or spy satellite information.

- Secret - includes information that could seriously damage national security if disclosed, such as deployment plans.
- Confidential - includes data that could seriously affect government operations, such as patents and trade secrets.
- Sensitive but not classified - includes data that might not cause serious damage to national security if revealed, but contains personal data.
- Unclassified - includes all other data and is publicly accessible.

Objective:

Information Risk Management

Sub-Objective:

Report noncompliance and other changes in information risk to facilitate the risk management decision-making process.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.8 Information Asset Classification

---

Question #57 of 150

Question ID: 1136023

Which of the following is the FIRST step in the process of developing an information security program?

A) Perform a gap analysis

B) Determine the current state

C) Define the security objectives

D) Determine the desired outcomes for security

Explanation

Determining the desired outcomes for security is the first step.

The next step is to define the security objectives. A parallel step is to determine the current state.

With information from these two steps, you can perform a gap analysis between the current state and the desired state.

Objective:

Information Security Program Development and Management

Sub-Objective:

Establish and maintain information security processes and resources to execute the information security program in alignment with the organization's business goals.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.4 Scope and Charter of an Information Security Program, Figure 3.1 - Steps in Information Security Program Development

Question #58 of 150

Question ID: 1185758

As part of the organization’s information security program, management wants to protect sensitive information from being revealed via social media. Which part of the information security policy would address this issue?

A) A packet-inspection firewall

B) An intrusion detection system

C) **Education**

D) Log analysis

Explanation

Education would address the social media issue. Employees must be trained to recognize the security vulnerabilities inherent in posting to social media. For one thing, attackers may be lurking on the social media site, waiting for some juicy piece of sensitive information. Education is used to ensure that all users understand security issues they will face. Social media usage and policies should always be addressed during this training. Education is considered an administrative, deterrent control.

A packet inspection firewall, log analysis, and an intrusion detection system would not prevent sensitive information from being revealed by social media. The use of personal devices can bypass these controls. These are not part of the information security policy. Rather they are implemented to support the policy.

Log analysis allows administrators to determine the actions taken by users, depending on how the audit policies are configured. An intrusion detection system (IDS) is used to detect attempts by attackers to gain access to internal resources. A packet-inspection firewall is used to prevent certain traffic from entering or exiting a network based on configured rules.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish and/or maintain the information security program in alignment with the information security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.11 Security Program Services and Operational Activities, 3.11.1, Information Security Liaison Responsibilities

---

Question #59 of 150

Question ID: 1138446

Which of the following performance indicators would be of the most interest to upper management?

A) The kinds of preventative controls that are in place
B) The number of incidents
C) The number of attacks that have been blocked
D) The avoided cost or savings by controls that mitigate attacks

Explanation

The avoided cost or savings by control that mitigate attack would be the performance indicator that upper management would have the most interest. Upper management is primarily interested in how the business is performing. Cost-saving measures would be of great interest to the executives because it shows that the investment in cyber security is working and supporting the business goals.

The number of incidents, the kinds of preventative controls, and the number of attacks that have been blocked are important metrics, but by themselves they are not useful. Without looking at these metrics over time, they represent just a snapshot of the aspects of the system. They can serve to distract and alarm upper management because they are not put into context. Just giving the number of incidents or the number of attacks that have been blocked may look either good or bad, but without looking at these metrics over time and comparing to the key goal indicators, they do not convey information about the performance of the security program.

Objective:
Information Security Program Development and Management

Sub-Objective:
Compile and present reports to key stakeholders on the activities, trends and overall effectiveness of the IS program and the underlying business processes in order to communicate security performance.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.13 Security Program Metrics and Monitoring

---

Question #60 of 150

Question ID: 1136071

How should an organization ensure that legal, regulatory, and organizational requirements are followed during or after a security incident?

A) Preserving all evidence

B) Immediately contact the legal department

C) Immediately contact law enforcement

D) **Incorporate the legal framework into the IRP**

Explanation

The incident response plan (IRP) should include the legal framework for investigating a security incident by considering the laws and regulations in effect when the plan is created. These laws define sensitive data and reporting requirements. Chain of evidence must also be followed.

An organization should consider contacting law enforcement when developing the IRP. Specific incidents that will require law enforcement should be defined. However, not all security incidents will require law enforcement intervention.

While legal counsel should be consulted during the development of an IRP, the legal department should not be contacted for all incidents. Doing so is unnecessary and will introduce additional delays that can interfere with the incident response. If the legal framework is incorporated into the plan, personnel will know what to do at the time of the incident and whether to contact law enforcement or legal counsel.

Preserving evidence is important, but guidelines established in the IRP should enumerate the evidence collection and preservation requirements, such as chain of evidence.

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain processes to investigate and document information security incidents in order to determine the appropriate response and cause while adhering to legal, regulatory and organizational requirements.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.13 Postincident Activities and Investigation, 4.13.3 Establishing Procedures

, Chapter 4: Information Security Incident Management, 4.13 Postincident Activities and Investigation, 4.13.5 Legal Aspects of Forensic Evidence

---

Question #61 of 150

Question ID: 1135991

Which statement is true about a BIA that that reports only worst-case outcomes to management?

A) A BIA that reports only worst-case outcomes is cost effective.

B) The BIA should be concerned with low impact assets that have a high probability of risk

C) Reporting only worst-case outcomes will ensure that all risks are covered.

D) **Reporting only worst-case scenarios results in management discounting these reports.**

Explanation

When a BIA reports only worst-case outcomes, management will dismiss it as unrealistic because of impact inflation. This can have a negative effect on future reports to management.

Worse case outcomes do not include all risks, only those that can cause the greatest damage. If an asset has high value that can cause great damage to the organization if exploited, but a very low risk probability, it does not fairly represent the risks to and impacts of other assets.

Assets with low impact value are of little concern regardless of the risk level.

Reporting worst-case outcomes may result in unnecessary and costly mitigation measures.

Objective:
Information Risk Management

Sub-Objective:
Report noncompliance and other changes in information risk to facilitate the risk management decision-making process.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.8 Information Asset Classification, 2.8.2 Impact Assessment and Analysis

---

Question #62 of 150

Question ID: 1136067

What is the most important factor for ensuring that the incident response plan will handle security incidents successfully and effectively?

A) Obtain senior management approval of the plan
B) Perform an annual review of the plan
C) Test all aspects of the plan
D) Conduct personnel training

Explanation

Testing all aspects of the incident recovery plan is the most important factor in achieving success in an emergency situation. It will ensure that the plans will be correctly executed during an emergency, and it enables the collaboration and coordination between teams.

Annual review of the plan will ensure that the plan is up to date, but like any plan, it must be tested in a relatively realistic scenario. For example, after military teams develop an attack plan, the plan must be tested in various scenarios that they might encounter to verify that the plan is good and to identify gaps.

Training of personnel is just one step toward achieving the goal of assuring that incidents will be handled successfully. The knowledge gained from training must be able to be put into action. Knowledge and execution are separate but related entities.

Senior management approval of the plan does not guarantee that the plan can be carried out successfully. It does guarantee that the plan will be accepted by the organization.

Objective:
Information Security Incident Management

Sub-Objective:
Develop and implement processes to ensure the timely identification of information security incidents that could impact the business.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.11 Testing Incident Response and Business Continuity/Disaster Recovery Plans

---

Question #63 of 150

Question ID: 1185764

How can an organization ensure that all employees support and buy in to the security policies and procedures?

A) Employ technical controls to remind people of their responsibilities.

B) Test all employees on their knowledge of the security program components.

C) Implement periodic reminders of the importance of security practices.

D) **Provide employee training that explains how employees' activities can help to protect the organization's assets.**

Explanation

To ensure that all employees support the security policies and procedures, the organization should train employees regarding their roles in protecting the assets. This requires personalized training and good interpersonal relationships between the information security manager and the other employees. Employee training provides a sense of ownership and inclusion.

Employing technical controls will not ensure that all employees support the security policies and procedures. While technical controls are necessary, they do educate employees about the importance of their individual roles in information security. Furthermore, controls can be bypassed if someone unknowingly clicks a link in an email that turned out to be a phishing attack.

Testing employees will not ensure that all employees support the security policies and procedures. People may know the right answers on paper, but not be able to act on them in a consistent manner in real-world scenarios.

Periodic reminders will not ensure that all employees support the security policies and procedures. While such reminders can help initially, after a while people will ignore them as part of the background noise.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish, promote and maintain a program for information security awareness and training to foster an effective security culture.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.10 Security Program Management and Administrative Activities, 3.10.1 Personnel, Roles, Skills and Culture

Question #64 of 150

Question ID: 1135937

Which role must fully support the risk management effort in order for it to succeed?

A) Chief Information Security Officer (CISO)

B) **Senior management**

C) Chief Information Officer (CIO)

D) Information security manager

Explanation

Senior management's support of the security strategy is essential for the program to succeed.

The role of the CIO is responsible for planning, budgeting and performance consistent with the policies.

The CISO, while a member of the senior management staff, must also gain the support of the rest of senior management, including the Chief Executive Officer (CEO), for the program to succeed.

The information security manager is responsible for implementing the security program.

Objective:
Information Security Governance

Sub-Objective:
Gain ongoing commitment from senior leadership and other stakeholders to support the successful implementation of the information security strategy.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, 1.4.1, Key Roles

, 1.4.2, Information security roles and responsibilities, Obtaining Senior Management Commitment.

Question #65 of 150

Question ID: 1138442

Which of the following can be used to assess the state of risk management for an organization?

A) **KPI**

B) The average amount of time required to resolve an incident

C) The number of events that were preventable

D) The number of issues that were eliminated versus those that were not eliminated

Explanation

The state of risk management for an organization can be assessed by comparing the number of issues that were eliminated versus those that were not. This would provide a measureable metric that demonstrates an improvement (or lack thereof) in risk management over time.

The average amount of time required to resolve an incident does not assess the state of risk management. This measurement is used to evaluate the state of the incident response.

The number of events that were preventable does not assess the state of risk management. This metric is used to evaluate loss prevention.

KPI does not assess the state of risk management. It is an acronym for Key Performance Indicator, and it is classifier for performance metrics.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish, monitor and analyze program management and operational metrics to evaluate the effectiveness and efficiency of the information security program.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.13 Security Program Metrics and Monitoring, 3.13.4 Measuring Information Security Risk and Loss

---

Question #66 of 150

Question ID: 1138432

A startup organization has hired an information security manager, but has not adopted an information security strategy or formal charter. What could the information security manager use to guide decision making?

A) his or her best judgement

B) appropriate regulations

C) consult with senior management

D) **industry standards**

Explanation

The information security manager could use industry standards. Following the standards, coupled with COBIT 5 or the ISO/IEC documentation, can help with the development of the scope and charter of the information security program and thus with decision-making.

The information security manager should NOT use his/her best judgement. Decisions should still be made in conjunction with the business goals of the organization so that they are guided decisions, not ad hoc ones.

Compliance with appropriate regulations is not correct does not guarantee that the organization is secure. It is easiest to use industry standards than appropriate regulations to guide the decision making. Often regulations are harder to understand than standards, and standards are usually designed to address regulations.

The information security manager should not consult with senior management. Individual decisions may involve highly technical considerations that senior management may not be able to evaluate especially since their focus is on the business side of things.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish and maintain information security processes and resources to execute the information security program in alignment with the organization's business goals.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.4 Scope and Charter of an Information Security Program

---

Question #67 of 150

Question ID: 1136061

For an appropriate response to a data breach to be implemented, what is required in addition the six-phase model for developing an incident response plan?

A) Defining an RTO
B) Having trained personnel
C) Testing the plan
D) Establishing a communication plan

Explanation

In addition to the incident response plan, having trained personnel who are familiar with the plan and have the skills to deal with any incidents is required for an appropriate response to a data breach to be implemented.

Establishing a communication plan and testing the plan are included in the six-phase incident response plan model.

The recovery time objective (RTO) is established when the business continuity plan is developed, and is included in the six-phase model.

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.9 Developing an Incident Response Plan, 4.9.1 Elements of an Incident Response Plan

---

Question #68 of 150

Question ID: 1135972

The information security manager has determined that the level of security employed by the organization meets both industry standards and regulatory requirements. What else, if anything, must the information security manager do?

A) The information security manager should increase the baseline security measures to provide an extra layer of protection.

B) **The information security manager must determine if the level of security is sufficient for all the different assets belonging to the organization.**

C) The information security manager should develop organizational standards to set the higher boundaries of protection for each security domain.

D) The information security manager does not have to do anything further since the standards and regulatory requirements are met.

Explanation

The information security manager must assess the level of security required by the organization against the levels set by the standards and regulations. Some assets in the organization may be more sensitive and require additional controls over and above those specified by the standards and regulations.

Developing organizational standards should be set to the lower, not higher, boundaries of protection for each security domain.

Increasing the baseline security measures to provide an extra layer of protection can increase costs without concurrent benefit. Adequate metrics should be used to determine if the baseline security level is sufficient.

Doing nothing is not correct. Compliance with standards and regulations does not mean that the systems are secure.

Objective:
Information Risk Management

Sub-Objective:
Determine whether information security controls are appropriate and effectively manage risk to an acceptable level.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.12 Security Control Baselines

---

Question #69 of 150

Question ID: 1135960

Which of the following components is most important for achieving a successful risk management program?

A) A bottom-up approach

B) Implementation of the proper controls

C) Support by senior management

D) Support by business owners

Explanation

Support by senior management is one of the most important components of a security program. This is a top-down approach and aligns the security program with business goals. A security policy defines the broad security objectives of an organization. It establishes each individual's authority and responsibility. It also establishes procedures to enforce the security policy. An organization's senior management has the primary responsibility for the organization's security. Therefore, they must determine the level of protection needed and endorse the security policy. Without senior management's support for a security program, the program will not be taken seriously by the rest of the organization.

Business owner support is not as important as the support by senior management. It will then be up to the various business owners to comply with the risk management program. A business owner is only responsible for a single business unit in the organization and cannot affect personnel outside the business that they own.

A bottom-up approach is not the most efficient means of implementing a risk management program since it will not be a unified program. Senior management has the business goals in mind when supporting the program, which is not necessarily be the case in a bottom-up approach. In a bottom-up approach, the risks management program is initiated by the general personnel, who have no real power to enforce any policies that they deem important.

Implementing the proper controls is not the most important factor. The controls will be implemented later in the program after the goals and priorities are determined. Aligning security goals with the business goals articulated by senior management is the most important factor.

Objective:
Information Risk Management

Sub-Objective:
Ensure that risk assessments, vulnerability assessments, and threat analyses are conducted consistently, at appropriate times, and to identify and assess risk to the organization's information.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.3 Effective Information Risk Management

---

Question #70 of 150

Question ID: 1136078

Which incident management or recovery team is responsible for determining which assets are restorable?

A) Emergency action team

B) Emergency management team

C) Security team

D) **Damage assessment team**

Explanation

The damage assessment team is comprised of individuals qualified to assess the extent of the damage and make an initial determination of which assets are salvageable.

The emergency action team is the first responders to deal with emergency response scenarios.

The emergency management team coordinates the activities of the other teams.

The security team, also referred to as the computer security incident response team (CSIRT), has responsibilities that include monitoring the security of the systems, identifying security threats, and assuring proper installation of the security packages.

Objective:
Information Security Incident Management

Sub-Objective:
Organize, train and equip incident response teams to respond to information security incidents in an effective and timely manner.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.9 Developing an Incident Response Plan, 4.9.6 Incident Management and Response Teams

Question #71 of 150

Question ID: 1135961

Which of the following is the initial step in the development of a risk management program?

A) Determine the methodologies for assessing, analyzing and mitigating risk

B) Develop the authority, structure and reporting relationships.

C) **Establish the context and purpose of the risk management program.**

D) Determine the scope and charter

E) Determine the classification, identity, and ownership of assets

F) Determine the objectives of the program

Explanation

You should first establish the context and purpose of the risk management program.

The steps in the risk management program are as follows:

1. Define the reason for the program and its context.
2. Determine the scope and charter of the program.
3. Define the authority, structure, and reporting relationships for the program.
4. Identify and classify assets, and determine asset owners.
5. Document the objective of the program.
6. Determine the methodologies to be used.
7. Designate the team responsible for implementing the program.

Objective:
Information Risk Management

Sub-Objective:
Ensure that risk assessments, vulnerability assessments, and threat analyses are conducted consistently, at appropriate times, and to identify and assess risk to the organization's information.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.3 Effective Information Risk Management, 2.3.1 Developing a Risks Management Program

Question #72 of 150

Question ID: 1135952

Risk appetite is generally based on which of the following factors?

A) the regulatory requirements for the organization

B) the governance and control objectives for the industry

C) the costs to eliminate risks

D) **the acceptable level of risk determined by management**

Explanation

Risk appetite is generally based on the acceptable level of risk, as determined by management. Management must assess all factors that affect risk and document the acceptable level of risk.

Risk appetite is not based on governance and control objectives. Governance and control objectives are outcomes of what is considered to be acceptable risk. Governance and control objectives affect the controls that an organization implements, but do not serve as a basis for risk appetite.

Risk appetite is not based on the costs to eliminate risk. Risk can never effectively be eliminated; it can only be reduced to acceptable levels. Risk appetite should not be driven by costs. It should be driven by the acceptable level of risk determined by management. The value of assets is often more than just the cost of the asset.

Risk appetite is not based on regulatory requirements. Regulatory requirements must be considered with regard to risk and impact. Management may also decide that the organization needs greater controls than specified by the regulations.

Objective:
Information Risk Management

Sub-Objective:
Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.3 Effective Information Risk Management, 2.3.1 Developing a Risk Management Program

Question #73 of 150

Question ID: 1136060

Which organizational role takes responsibility for managing an incident?

A) Business managers

B) Security steering group

C) Information security manager

D) Incident response manager

Explanation

The information security manager takes responsibility for managing incidents. This role is also responsible for managing risks, developing and maintaining the incident management and response capability, and performing proactive and reactive measures to control the information risk level. Most other security roles report to the information security manager.

The security steering group has the responsibility for the overall incident management and response concept. This group also approves the incident management team charter, approves exceptions and deviations, and makes final decisions on incidents.

The incident response manager supervises the incident response tasks. This individual also coordinates resources for incident response, takes responsibility for execution of the incident response plan, and presents incident response reports and lessons learned.

The business manager or managers make decisions related to the information assets and systems when an incident happens. They also provide a clear understanding of business impact in the business impact assessment (BIA) or in the incident response plan (IRP).

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, Figure 4.2

Question #74 of 150

Question ID: 1185753

To establish a risk management process, both the internal and external environments must be considered. Which of the following is considered part of the external environment with regards to risk management?

A) The cloud

B) The legal and regulatory environment

C) Key business drivers

D) Lighting around the property

Explanation

The external environment refers to the environment in which the organization operates. It includes the local market, the legal and regulatory environment, social and cultural conditions, and other external conditions, such as the political climate.

Perimeter lighting is a physical preventive control. It does not define the environment in which the organization operates.

Key business drivers are part of the definition of the internal environment of the organization, not the external environment. The internal environment also includes the organization's strength and weaknesses, organizational structure, resource assets, and goals and objectives.

The cloud is a means by which information is stored and access to that information is managed.

To design an effective risk management program, the organization must understand the internal factors that directly affect the assets to be protected, and understand external factors that indirectly affect or influence the assets to be protected.

Objective:
Information Risk Management

Sub-Objective:
Determine whether information security controls are appropriate and effectively manage risk to an acceptable level.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.5 Implementing Risk Management, 2.5.3 Defining the external environment

, Chapter 2: Information Risk Management, 2.5 Implementing Risk Management, 2.5.4, Defining the internal environment

Question #75 of 150

Question ID: 1135921

For which of the following activities are the information security manager and the business process owner jointly responsible?

A) Define target IT capabilities.

B) Conduct a gap analysis.

C) Communicate the IT strategy and direction.

D) Define the strategic plan and road map.

Explanation

The information security manager and the business process owner are both responsible for conducting a gap analysis. The chief information officer is accountable for the gap analysis.

The information security manager and the business process owner are not both responsible for defining target IT capabilities. The chief information officer is responsible for defining target IT capabilities. The information security manager is consulted, while the chief executive officer is accountable. The business process owner is informed of the target IT capabilities.

The information security manager and the business process owner are not both responsible for defining the strategic plan and road map. The information security officer and chief executive officer are consulted about the strategic plan and road map. The chief information officer is accountable for the strategic plan and road map.

The information security manager and the business process owner are not both responsible for communicating IT strategy and direction. The information security manager, board of directors, and business process owner are informed of the IT strategy and direction. The chief information officer and chief executive officer are responsible for the IT strategy and direction.

Objective:
Information Security Governance

Sub-Objective:
Establish and maintain information security policies to guide the development of standards, procedures and guidelines in alignment with enterprise goals and objectives.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.3 Roles and Responsibilities

, Chapter 1: Information Security Governance, 1.4 Key Roles

Question #76 of 150

Question ID: 1136066

Which organizational role is responsible for defining security-related incidents?

A) System owner

B) Data owner

C) **Senior management**

D) Information security manager

Explanation

The information security manager is responsible for defining which incidents are security related. These include malicious code attacks, unauthorized access, and so on. The information security manager must also determine if what appeared to be a malicious attack turns out to be internal human errors.

The data owner determines the level of classification for the information for which he or she is responsible.

Senior management oversees the organization's security, as well as business operations.

System owners ensure that the proper controls are in place.

Objective:
Information Security Incident Management

Sub-Objective:
Develop and implement processes to ensure the timely identification of information security incidents that could impact the business.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.3 Incident Management Organization, 4.3.1 Responsibilities

Question #77 of 150

Question ID: 1135970

Which risk assessment model organizes risk into a binary tree?

A) FAIR

B) COBIT 5

C) ISO/IEC 27005

D) **PRA**

Explanation

The Factor Analysis of Information Risk (FAIR) uses a binary tree as a logical framework for evaluating risk. Each risk is evaluated in two areas: loss event frequency and probable loss magnitude. FAIR is not meant to replace other risk assessment models, but is instead meant to complement them.

None of the other options organizes risk into a binary tree.

ISO/IEC 27005 and COBIT 5 are interrelated. The COBIT 5 framework consists of five principles for governance and management: Meeting Stakeholder Needs, Covering the Enterprise End to End, Applying a Single Integrated Framework, Enabling a Holistic Approach, and Separating Governance from Management. ISO/IEC 27005 is a framework for assessing risk. It uses elements from COBIT 5 for evaluation of risk: Control, Value, and Threat condition imposing a notable level of risk.

The Probabilistic Risk Assessment model (PRA) is a systematic methodology that analyzes risk according to three basic questions: What can go wrong?, How likely is it?, and What are the consequences? PRA models tend to look more like a decision tree than a binary tree.

Objective:
Information Risk Management

Sub-Objective:
Identify, recommend or implement appropriate risk treatment/response options to manage risk to acceptable levels based on organizational risk appetite.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.7 Risk Assessment, 2.7.8Other Risk Assessment Approaches

, Chapter 1: Information Security Governance, 1.8 Information Security Strategy Objectives, 1.8.3: The Desired State

Question #78 of 150

Question ID: 1136095

An organization is evaluating changes in its security requirements in conjunction with threat analyses uncovering new threats. Which of the following need to be coordinated with regard to incident response? (Choose all that apply.)

A) **RTO**

B) **RPO**

C) **MTBF**

D) **AIW**

E) **MTTR**

F) CIA

Explanation

In order to effectively integrate the incident response plan with business continuity and the disaster recovery plan, the organization should consider the recovery time objective (RTO), recovery point objective (RPO), and the acceptable interruption window (AIW), as well as other metrics.

New threats require an evaluation and possible update to mitigation mechanisms, hardware and software, which would require a determination of how these new additions affect the ways in which the team can respond and how it affects the various recover objectives. The new features must comply with business objectives with regard to recovery time and loss of business operations.

The mean time between failures (MTBF) and the mean time to repair (MTTR) are reliability estimates produced by the manufacturer of the hardware, which determines which equipment to purchase derived from the recovery objectives.

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain integration among the incident response plan, business continuity plan and disaster

recovery plan.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.10 Business Continuity and Disaster Recovery Procedures, 4.10.9 Integrating Incident Response with Business Continuity

---

Question #79 of 150

Question ID: 1136090

Several months after a serious incident was handled very quickly and successfully, the same kind of incident occurred and was not handled as well. The incident report for the first incident was never properly created, although the root cause was identified. During this time, the incident response team experienced high turnover. A review of the second incident indicated the source of the problem. What is the most likely the problem encountered here by this organization?

A) The loss of critical personnel

B) Equipment failure

C) **The failure to properly log and evaluate the root cause of the first event**

D) Inadequate incident response planning

Explanation

The most likely cause of the second incident is inadequate incident response planning. The incident response plan should include the lessons learned as a final step. Lessons learned reviews the incident report, including root cause analysis. This forms the basis for improving the incident response and the security of the system. Because it was not done following the first incident, based on the fact that an incident report was not created, there was a failure of the response plan.

Logging and evaluation of root cause of an incident should be part of the incident response plan, which was not followed. The scenario indicates that the root cause of the first incident was identified.

Loss of critical personnel is not the cause of the recurrence of the incident. If the incident response plan had been followed and a proper review of the first incident had occurred, then the second incident would probably not have happened.

Equipment failure was not a cause of either incident. If the equipment had failed the first time, it would have been replaced and the likelihood of a recurrence due to the same piece of equipment would be very low.

Objective:

Information Security Incident Management

Sub-Objective:

Conduct postincident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.9 Developing an Incident Response Plan, 4.9.1 Elements of an Incident Response Plan

Question #80 of 150

Question ID: 1136057

When does an event that is reported by an IDS become a security incident?

A) When any event occurs

B) When a single negative event occurs

C) **When a series of events causes an interruption in service**

D) When a single failed login attempt occurs

Explanation

An event that is reported in an IDS becomes a security incident when series of events causes an interruption in service.

A single event, such as when a single failed login attempt occurs, is not considered to be an incident unless it results in service issues. If a service issue occurs, then the event or events are elevated to incident status.

A single negative event should not trigger an incident and require the incident response team. There are generally numerous events that are logged. If each one required a response, it would consume the resources of the incident response team, and then real incidents will not be responded to in an appropriate manner.

A single failed login attempt should be logged but not responded to. Depending on the configuration of the controls, a single failed login attempt may not even generate an event.

If the logging and reporting system indicates that every event is an incident, then the threshold for reporting is too low, and the results will tie up the incident response team.

Objective:

Information Security Incident Management

Sub-Objective:

Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents to allow accurate classification and categorization of and response to incidents.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program and Development, 3.13 Security Program Metrics and Monitoring, 3.13.13 Monitoring and Communication

Question #81 of 150

Question ID: 1185744

Company ABC has outsourced management of the air conditioning for the server rooms, which will be done remotely through the ABC's network. What is the most important security concern for ABC regarding the outsourced company's access?

- **A)** Network outages
- **B)** **Unauthorized access into the organization's production systems by the service company**
- **C)** Security of the service company's network
- **D)** Response time

Explanation

The security of the service company's network is the most important security concern. An attacker could gain access to the environmental controls in the server room if the outside company's network is breached. If those controls are tampered with, the servers can overheat and be damaged, seriously affecting the organization's ability to operate.

Unauthorized access to the organization's production system from the service company's system is not the most important security concern. The service company’s network should be isolated from the organization's production network. The service company should only have access to the environmental systems, not to production systems. The service level agreement (SLA) should contain conditions for the service company granting appropriate access. For this reason, this is not the most important security concern.

Management needs to ensure that the response time for an HVAC outage is appropriate for the needs of the organization. Because response time is stipulated in the SLA, this should not be as high a security concern as the service company’s network security.

Network outage is not the most important security concern. Network outages should always be a consideration and can be managed by implementing redundant access to the internet and the internal network. Network outage is usually addressed in the SLA and for this reason, is not as high of a concern.

Objective:
Information Security Governance

Sub-Objective:
Identify internal and external influences to the organization to ensure that these factors are continually addressed by the information security strategy.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.5 Governance of Third-Party Relationships

, Chapter 1: Information Security Governance, 1.6, Information Security Governance Metrics

---

Question #82 of 150

Question ID: 1136085

When an incident is escalated, which of the following activities must be accomplished within the time established by the RTO? (Choose all that apply.)

- **A) Containing the threat**
- B) Activating backup facilities
- **C) Notifying personnel**
- D) Retrieving and unloading data
- E) Executing transportation arrangements

Explanation

In order to meet the recovery time objective (RTO), all of the following activities must be competed: notifying personnel, activating backup facilities, containing the threat, arranging for transportation and ensuring that those arrangements are carried out, retrieving and unloading data, and testing.

Objective:

Information Security Incident Management

Sub-Objective:

Establish and maintain communication plans and processes to manage communication with internal and external entities.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.9 Developing an Incident Response Plan, 4.9.4 Escalation Process for Effective Incident Management

Question #83 of 150

Question ID: 1185743

What strategy should be employed to protect the organization from threats by impersonation due to the use of mobile devices inside and outside of the organization?

A) Limit mobile devices to accessing the public servers only

B) Ban all mobile devices from accessing the organization's servers

C) Require multifactor authentication that can include the location of the devices

D) Require all mobile device be installed with the company's proprietary security controls

Explanation

The best strategy would be to require multifactor authentication including the device location. Multifactor authentication would include the use of a factor from each category: something you are, something you have, somewhere you are, and something you know. Including location as an authentication mechanism provides additional assurance that the device is accessing the network from known or authorized locations, such as when an employee is traveling on business with the device.

The best strategy is not to ban all mobile devices from accessing the servers. Mobile devices include laptops and tables as well as phones. Often an employee is issued a laptop for business-related activities, and banning it from the servers would prevent the employee from doing his or her work.

The best strategy is not to limit all mobile devices to the public servers. This would also inhibit employees from performing their job functions.

The best strategy is not to install proprietary controls on all personal mobile devices that can be used for work-related activities. Some devices, such as tablets or phones, would require rooting or jailbreaking to install the controls. This is generally frowned upon because it can expose additional vulnerabilities in the device. However, proprietary control software can be installed on laptops computers.

Objective:
Information Security Governance

Sub-Objective:
Identify internal and external influences to the organization to ensure that these factors are continually addressed by the information security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.9 Architecture Implementation

---

Question #84 of 150

Question ID: 1185752

An organization is in the early stages of its existence. Because of limited funding and limited internal resources, the organization decides to outsource all of its IT functions to a third party to mitigate the risk of the IT operations. Which risk treatment option or response is being used?

A) Accept the risk.

B) Avoid the risk.

C) Implement appropriate control measures.

D) Transfer the risk.

Explanation

The organization has chosen the risk transference option. They considered the costs of mitigation relative to the value of the assets compared with the costs of third party management, and determined that the outsourcing option was best cost-saving measure.

The organization did not avoid the risk. Risk avoidance is an option for managing risk by either terminating the risky activity or choosing an approach that is less risky. This decision is made by comparing the costs for the different methods of managing risk, such as transferring the risk to a third party or implementing mitigation measures.

The organization did not implement appropriate control measures. Implementing control measures includes incorporating technological controls, such as firewalls, Intrusion Detection or Prevention Systems (IDS/IPS), and two-factor authentication. This approach is chosen after considering the costs of implementing these measures by performing a Return on Security Investment (ROSI) to determine if the measures will be cost effective

The organization did not accept the risk. Risk acceptance means that the organization has determined that the asset is of low value to the organization. Because of this, it would not be cost effective to add additional security controls over and above what might be already in place or to choose a different risk management option.

Objective:
Information Risk Management

Sub-Objective:
Identify, recommend or implement appropriate risk treatment/response options to manage risk to acceptable levels based on organizational risk appetite.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.7 Risk Assessment, 2.7.18 Risk Treatment (Response) Options

---

Question #85 of 150

Question ID: 1138445

A company has been running periodic social engineering challenges. Along with these challenges, there are regular information security awareness training sessions. The challenges consist of sending out fake phishing emails to all employees, designed to get the recipients to click the link in the email. If an employee clicks the link, they are notified that they clicked a link that could have compromised their computer and possibly the entire network. The results are tallied and reviewed monthly to determine the success of the program. What kind of a metric does this challenge represent?

A) Key operational indicator

B) Key goal indicator

C) **Key risk indicator**

D) Key performance indicator

Explanation

This challenge represents a key risk indicator (KRI). A KRI enables an organization to identify the likelihood of the occurrence of a risk. It is well known that while people are the greatest asset for a company, they can also pose its greatest risk. Social engineering and phishing attacks represent one of the most prevalent risks to an organization. Measuring the reduction of the number of clicks on the fake phishing emails is one measure of risk for an organization.

A key performance indicator (KPI) is a metric used to determine the levels of performance relative to established norms.

A key goal indicator (KGI) shows progress toward a predefined goal. It would be used in conjunction with other indicators.

The term key operational indicator (KOI) is another name for KPI.

Objective:
Information Security Program Development and Management

Sub-Objective:
Compile and present reports to key stakeholders on the activities, trends and overall effectiveness of the IS program and the underlying business processes in order to communicate security performance.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.13 Risk Monitoring and Communication, 2.13.2 Key Risk Indicators

---

Question #86 of 150

Question ID: 1185738

Which of the key principles in COBIT 5 states that enterprises exist to create value by balancing the realization of benefits against optimizing risk and resource utilization?

A) Applying a single integrated framework

B) Covering the enterprise end to end

C) **Meeting Stakeholder needs**

D) Separating governance from management

Explanation

Meeting stakeholder needs is correct.

COBIT 5 has five principles:

- Principle 1: Meeting stakeholder needs. The enterprise exists to create value for its stakeholders by maintaining a balance between the realization of benefits and the optimization of risk and resource utilization.
- Principle 2: Covering the enterprise end-to-end. COBIT 5 integrates IT governance into enterprise governance. It covers all the functions and processes in the enterprise.
- Principle 3: Applying a single integrated framework. COBIT 5 aligns with other relevant standards and frameworks.
- Principle 4: Enabling a holistic approach. COBIT 5 takes into account all interacting components and defines a set of enablers that includes: principles, policies, and frameworks; processes; organizational structures; culture, ethics, and behavior; information; services, infrastructure, and applications; and people, skills, and competencies.
- Principle 5: Separating governance from management. The framework makes a clear distinction between governance and management.

Objective:
Information Security Governance

Sub-Objective:
Establish and/or maintain an information security governance framework to guide activities that support the information security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.8 Information Security Strategy Objectives, 1.8.3 The Desired State

Question #87 of 150

Question ID: 1185737

You must assess the state of the security program for the purposes of deciding if the controls are sufficient. What is the best means for making this determination?

A) Reviewing benchmarks

B) Reviewing the KPIs

C) Performing full audits

D) Consulting with experts

Explanation

Reviewing the key performance indicators (KPIs) will help you decide whether the controls are sufficient. Good metrics provide the information needed to make decisions about the effectiveness of the security program. To manage an activity, you must be able to accurately measure its performance relative to the company's goals.

Once the appropriate metrics are obtained, then expert opinion can be more useful.

Performing full audits provides a snapshot, and while important, day to day information provided by KPIs is needed to manage the security program.

Reviewing benchmarks provides comparisons to standards. While they are useful, benchmarks do not provide information about the day to day activity relative to the company's goals.

Objective:
Information Security Governance

Sub-Objective:
Establish and/or maintain an information security governance framework to guide activities that support the information security strategy.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.6 Incident Management Metrics and Indicators

, Chapter 1: Information Security Governance, 1.2 Effective Information Security Governance, 1.2.1 Business Goals and Objectives

Question #88 of 150

Question ID: 1136070

Which of the following policies, standards, and procedures are important for the incident response plan? (Choose all that apply.)

A) Identify and set requirements for alternate personnel.

B) Provide guidance for operational needs.

C) Establish proper expectations.

D) Align incident management activities with incident management team goals.

E) Establish clearly defined roles and responsibilities.

F) Maintain consistent and reliable services.

Explanation

To establish and maintain processes, the incident response plan should include all of the following policies, standards, and procedures:

- Align incident management activities with Incident management team goals.
- Establish proper expectations.
- Provide guidance for operational needs.
- Maintain consistent and reliable services.
- Establish clearly defined roles and responsibilities.
- Identify and set requirements for alternate personnel.

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain processes to investigate and document information security incidents in order to determine the appropriate response and cause while adhering to legal, regulatory and organizational requirements.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.4 Incident Management Resources, 4.4.1 Policies and Standards

Question #89 of 150

Question ID: 1185748

What is the first step to determine information asset importance?

A) Determine the number of times the asset is attacked

B) **List the critical function layers.**

C) List the assets.

D) List the business units or departments.

Explanation

The steps to determine information asset importance shown in the organizational structure tree:

1. From the top level of the organizational structure, list the business units or departments.
2. Prioritize the importance of each business unit.
3. Identify critical organizational functions.
4. Assign assets to each function.
5. Determine asset vulnerabilities.

The number of times an asset is attacked is not relevant to its importance. While an asset may be known to attackers and attacked frequently, this does not correlate to the asset's importance. It may be that the asset is poorly protected and easily attacked. It could also be that the organization has determined that the asset is of low value and thus does not represent a high degree of risk to the organization.

Objective:
Information Risk Management

Sub-Objective:
Establish and/or maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.8 Information Asset Classification

Question #90 of 150

Question ID: 1136094

Which of the following statements is TRUE of the incident response plan, business continuity plan, and disaster recovery plan?

A) Only the incident response plan and the disaster recovery plan should be combined into a single plan.

B) **The RTO for the incident recovery plan and the disaster recovery plan should assume a worst-case scenario.**

C) All three plans should consider the RTO, RPO, SDO, and MTO.

D) All three plans should be combined into a single plan.

Explanation

All three plans should consider the recovery time objective (RTO), recovery point objective (RPO), service delivery objective (SDO), and maximum tolerable outage (MTO). To effectively integrate the three plans, the relationships between the RTO, RPO, SDO, and MTO should be considered. Depending on the extent of the incident of disaster, it may be necessary to transfer operations to an alternative site, which can affect the RTO and acceptable interruption window (AIW).

The three plans do not necessarily have to be combined, but they must be consistent with each other for effective transition following a disaster.

The incident response plan and disaster recovery plan do not have to be combined for the same reason.

The RTO must be considered in relationship to the nature of the incident or disaster. A very serious disaster that disrupts all business operations has to be restored more quickly than the loss of a server that does not have highly critical data.

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain integration among the incident response plan, business continuity plan and disaster recovery plan.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.10 Business Continuity and Disaster Recovery Procedures, 4.10.9 Integrating Incident Response with Business Continuity

Question #91 of 150

Question ID: 1135913

A security problem was detected in an organization's computer network. When tested individually, all systems and processes work as intended. However, when several of the systems and processes are running, a problem occurs with the network. What approach to manage this network would be most appropriate?

- **A)** Improve compliance with federal regulations
- **B)** Modify defenses to protect against exploits of the vulnerability
- **C)** **Perform vulnerability testing**
- **D)** Use the Business Model for Information Security

Explanation

The Business Model for Information Security (BMIS) would be most appropriate for managing the network. This model follows system theory, in which the parts of the system are not necessarily looked at individually but as a complete functioning unit. It examines the interactions between the components. The components of the network that interact with each other are people, technology, processes, and organizational design and strategy.

Vulnerability testing would not be most appropriate. It shows vulnerabilities that exist, but would not necessarily show how the interactions of the various components of the system can create vulnerabilities.

Improving compliance with federal regulations would not detect the network issues. The regulations can define certain policies to which the organization must adhere. The overall design and operation of the network must support these policies. The regulations cannot pinpoint, however, where the problem in the network resides.

Modifying defenses to protect against exploits of the vulnerability does not fix the vulnerability. It may work in the short term, but the risk is still present.

Objective:
Information Security Governance

Sub-Objective:
Establish and/or maintain an information security governance framework to guide activities that support the information security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.2 Effective Information Security Governance, 1.2.5 Business Model for Information Security

Question #92 of 150

Question ID: 1135987

A business operation is located in an area that can suffer earthquakes. It is estimated that in the event of an earthquake, 25% of the assets could be lost. The likelihood of such an event is once every 5 years. The cost of the assets is one million dollars. What is the expected annualized loss?

A) $200,000

B) $250,000

C) $1,000,000

D) **$50,000**

Explanation

The formula to calculate the expected annualized loss expectancy is the annualized rate of occurrence times the single loss expectancy. The calculations in this scenario are as follows:

- The asset value (AV) is $1 million dollars ($1,000,000).
- The exposure factor (EF) is 0.25.
- The single loss expectancy is SLE = EF x AV = 0.25 x $1,000,000 = $250,000.
- The annualized rate of occurrence is ARO = 1/5 = 0.2.
- The annual loss expectancy is ALE = ARO x SLE = 0.2 x $250,000 = $50,000.

Objective:

Information Risk Management

Sub-Objective:

Monitor for internal and external factors that may require reassessment of risk to ensure that changes to existing, or new, risk scenarios are identified and managed appropriately.

References:

CISM Review Manual, 15th Edition, Chapter 2L Information Risk Management, 2.7 Risk Assessment

Question #93 of 150

Question ID: 1136012

What is the best strategy for aligning the information security program with the operational objectives of the various departments within an organization?

A) **The information security program should have different elements that apply to different departments.**

B) The same technologies should be applied uniformly to only those departments that handle non-private data.

C) The information security program should be developed solely with the overall business goals in mind.

D) The information security program should be applied in the same way to all departments.

Explanation

The information security program should have different elements that apply to the different departments. Each department has different requirements for its business goals, infrastructure, topologies, risk levels, and technologies. In essence, one size does not fit all.

The program should NOT be applied in the same way to all departments. The information security program often results in different elements being customized to departmental needs.

The same technologies should not be applied uniformly to only those departments that handle non-private data. Each department has different requirements.

The program should not be applied solely with the overall business goals in mind. While the organization has a set of business goals, each department applies those goals in different ways while being in alignment with the overall goals. The information security program should support those departmental goals so that the departments can support the overall business goals of the organization.

Objective:
Information Security Program Development and Management

Sub-Objective:
Align the information security program with the operational objectives of other business functions (e.g., human resources [HR], accounting, procurement and IT) to ensure that the information security program adds value to and protects the business.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.2 Information Security Program Objectives

Question #94 of 150

Question ID: 1138431

Which person or group is responsible for helping to achieve consensus on priorities and trade-offs with regards to security considerations?

A) Senior management

B) Chief Information Security Officer (CISO)

C) Business process owners

D) **Steering committee**

Explanation

The steering committee, which is composed of representatives of the different groups in the organization, can help to achieve consensus on the various security issues that the organization faces.

Business process owners do not achieve consensus on security priorities and trade-offs. Individually the business process owner aligns the security activities of his or her department with the business objectives.

The CISO does not achieve consensus on security priorities and trade-offs. The CISO is primarily focused on the regulatory role and execution of the security program.

Senior management does not achieve consensus on security priorities and trade-offs. Senior management is responsible for supporting the security program and ensuring that the needed functions, resources, and support structures are available.

Objective:
Information Security Program Development and Management

Sub-Objective:
Identify, acquire and manage requirements for internal and external resources to execute the information security program.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.3 Roles and Responsibilities, 1.3.4 Steering Committee

Question #95 of 150

Question ID: 1135996

Which of the following best describes which activities are affected by the RTO?

A) AIW

B) SDO

C) RPO

D) **BIA**

Explanation

The business impact analysis (BIA) determines the consequences of losing a resource to an organization. The recovery time objective (RTO) is the amount of time allowed to recover operations to an acceptable level. The RTO is both affected by and affects the BIA. The BIA determines the RTO, but if the RTO is different than that stated it the BIA, it may be necessary to edit the BIA to a more reasonable RTO. The acceptable RTO level is defined by the service delivery objectives (SDO). If recovery operations exceed the RTO, the RTO is not met.

The acceptable interruption window (AIW) is the amount of time that normal business operations can be down before the company faces major financial problems. It is determined by business considerations and not the nature of the interruption. The AIW limits how long recovery operations can take.

The recovery point objective (RPO) is the minimal level of service that must be restored following a disaster. This level of service is defined by the SDO.

Objective:
Information Risk Management

Sub-Objective:
Ensure that information security risk is reported to senior management to support an understanding of potential impact on the organizational goals and objectives.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.9 Operational Risk Management, 2.9.1 Recovery Time Objectives

Question #96 of 150

Question ID: 1136077

The incident response team has determined that for the incident response plan to be successful, the KGI must be greater than 75% when 600 incidents are reported. The goal is to have those 600 incidents resolved within 5 minutes. At the point in time when the system logged 600 incidents, it was found that 400 incidents were resolved in the allotted 5 minutes. What is the KGI at this point in time?

- **A)** 75%
- **B)** 33%
- **C)** **67%**
- **D)** 80%

Explanation

The KGI at the point of measurement is the number of incidents resolved divided by the target number of incidents resolved times 100%, or (400/600) = .66666 or 67%.A key goal index (KGI) is a measurement that tells management, after the fact, whether an IT process has achieved its business requirements.

Objective:
Information Security Incident Management

Sub-Objective:
Organize, train and equip incident response teams to respond to information security incidents in an effective and timely manner.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.6 Incident Management Metrics and Indicators

Question #97 of 150

Question ID: 1136083

What is the first activity for determining the adequacy of the incident response plan?

A) Structured walk-through

B) Checklist review

C) Simulation test

D) Parallel test

Explanation

The checklist review is the first step in reviewing the adequacy of the incident response plan. It is reviewed by the incidence response team members to ensure that the checklist for the items in the plan are up-to-date.

The structured walk-through is an activity where the incident response team reviews and edits the incident response plan to identify weaknesses and strengths. It would be done after the checklist review.

During the simulation test, the incident response team responds to a disaster scenario in a simulated environment. It depends on having the updated incident response plan.

The parallel test is one in which the recovery site is active in parallel with the primary site so that a disaster scenario can be enacted without interruption of the business operations. The activity would follow the simulation test as the next step to determine the preparedness of the incident recovery team.

A full interruption test is one in which operations at the primary site are completely shut down and operations at the backup site are restored as stated in the recovery plan.

Objective:
Information Security Incident Management

Sub-Objective:
Test, review and revise (as applicable) the incident response plan periodically to ensure an effective response to information security incidents and to improve response capabilities.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.11 Testing Incident Response and Business Continuity/Disaster Recovery Plans, 4.11.3 Types of Tests

Question #98 of 150

Question ID: 1136003

An organization finds that the time to recover data given the RPO is greater than the RTO. What is the result of this determination?

- **A) The time between backups should be reduced.**
- **B)** The RTO can be ignored.
- **C)** The between backups should be increased.
- **D)** The RPO should be changed.

Explanation

If the volume of data to be restored from backups is so great that it takes longer to restore the data than required by the recovery time objective (RTO), the time between backups should be reduced. This will reduce the volume of data to be restored, and therefore the time to restore that data.

Increasing the time between backups increases the volume of data to be restored after a disaster and therefore increases the time to restore that data.

The RTO is the amount of time to recover operations to an acceptable level. The recovery point objective (RPO) indicates the most recent point in time to which it is acceptable to recover data. RPO determines the amount of data loss that could occur. This is a business decision and is determined by the service delivery objective (SDO), which is the minimal level of service to be restored to meet business requirements.

Objective:
Information Risk Management

Sub-Objective:
Ensure that information security risk is reported to senior management to support an understanding of potential impact on the organizational goals and objectives.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.9 Operational Risk Management, 2.9.3 Recovery Point Objectives

Question #99 of 150

Question ID: 1136064

An incident is discovered that at first appears minor, but quickly escalates into a very serious threat. Who should be contacted to escalate the response?

- **A) Whoever is listed in the incident response plan**
- **B)** Senior management and business owners
- **C)** Business owners and response teams
- **D)** Security steering group and customers

Explanation

The incident response plan should map out a responsible person and alternate for each type of event.

Senior management and others (security steering group, business owners, HR, response teams, insurance, and customers) should all be notified but they are not necessarily the go-to person or persons when an incident is being escalated.

The business owners and the security steering group may be listed in the incident response plan, but are not necessarily the people who should escalate the response to the incident.

Objective:
Information Security Incident Management

Sub-Objective:
Develop and implement processes to ensure the timely identification of information security incidents that could impact the business.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.9 Developing an Incident Response Plan, 4.9.4 Escalation Process for Effective Incident Management

---

Question #100 of 150

Question ID: 1135994

An analysis of the security logs revealed that a breach had occurred affecting an asset that was previously protected. What is the appropriate response to this event? (Choose all that apply.)

- **A) Reassess the risk and applicable controls.**
- **B)** Take the affected systems offline.
- **C) Report the breach to senior management.**

D) **Initiate a change management process.**

E) **Immediately implement new security controls.**

Explanation

Security policies should state that in the event of a breach of protected resources, a report to senior management should be generated. In addition, the risk and applicable controls should be reassessed.

Immediate implementation of new controls is not correct. New controls should only be implemented once the analysis is completed and only if the analysis determines that a new control is needed.

Taking the affected systems offline may not be appropriate depending on the extent of the breach, such as if an asset was corrupted. Taking affected systems offline can have detrimental effects. A thorough analysis of the breach should be completed to determine the next steps to be taken.

Initiating change management is not correct. Until an analysis of the breach is completed, there is no way to determine which change may need to occur.

Objective:
Information Risk Management

Sub-Objective:
Report noncompliance and other changes in information risk to facilitate the risk management decision-making process.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.13 Risk Monitoring and Communication, 2.13.3 Reporting Significant Changes in Risk

---

Question #101 of 150

Question ID: 1138437

When the information security manager discusses information security with the human resources (HR) manager, what should be the main topic of discussion?

A) Security of HR resources

B) The department's information security budget

C) **Information security training for employees**

D) Hiring new employees

Explanation

The HR department must be convinced of the need for cybersecurity training of the employees by the information security manager. Legal responsibilities require this cooperation.

The information security manager would not discuss hiring new employees. New employees may not have the necessary information security training and must be able to comply with the company's information security policies, through adequate training programs.

The information security manager would not discuss budget considerations. Besides being an accounting function, HR must develop the budget based on the cybersecurity programs that HR has agreed to enact in the discussions with the information security manager.

The information security manager would not discuss the security of HR resources. Analysis of the security posture would occur outside the purview of the HR department.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish, promote and maintain a program for information security awareness and training to foster an effective security culture.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.11 Security Program Services and Operational Activities, 3.11.1 Information Security Liaison Responsibilities

---

Question #102 of 150

Question ID: 1135990

Which of the following should be considered when classifying assets? (Choose all that apply.)

A) **Asset labels**

B) **Retention policies**

C) **Classification levels**

D) Asset purpose

E) Asset ownership

F) Asset rights

Explanation

When classifying assets, the following should be considered:

- Classification levels
- Asset labels
- Asset rights
- Asset ownership
- Retention policies

The classification levels determine the security levels, as well as the level and types of controls needed to protect the asset. Labeling an asset sets the parameters for access. Ownership of the asset determines who has control of that asset. Retention policies are not only required for security policies; they are also required by many regulations.

The purpose of the asset is not correct. It does not matter if the asset is a server or a router. The important thing is its relative importance.

Objective:
Information Risk Management

Sub-Objective:
Report noncompliance and other changes in information risk to facilitate the risk management decision-making process.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.8 Information Asset Classification

---

Question #103 of 150

Question ID: 1138447

Which of the following represents meta-metrics that can be used to rank individual metrics by their usefulness? (Choose all that apply.)

A) Key performance indicators

B) Metric quantifiability

C) Metric accuracy

D) Metric reliability

E) Key risk indicators

F) Key goal indicators

Explanation

Meta-metrics provide information about the metric itself and not what the metric measures. For a metric to be useful, it must be accurate and reliable. The degree to which the metric conforms with these attributes can be used to rank the metric.

Key goal indicators, key risk indicators, and key performance indicators are categories or types of metrics, not meta-metrics

Metric quantifiability is not a type of meta-metric. Some metrics are not quantitative. Additionally, this term is too vague.

Objective:
Information Security Program Development and Management

Sub-Objective:
Compile and present reports to key stakeholders on the activities, trends and overall effectiveness of the IS program and the underlying business processes in order to communicate security performance.

References:

CISM Review Manual, 15th Edition, Chapter 13: Information Security Program Development and Management, 3.13 Security Program Metrics and Monitoring, 3.13.1,Metric Development

---

Question #104 of 150

Question ID: 1135968

A very sensitive asset for an organization is stored in a system that has no known vulnerabilities with adequate defensive measures in place. However, it would be very lucrative if an attacker gained access to this asset. How should the organization best treat this risk?

- **A) The organization should consider purchasing insurance.**
- **B)** The organization should duplicate the same level of risk treatment given to similar assets.
- **C)** The organization should accept the risk.
- **D)** The organization should not do anything because the risk is zero.

Explanation

The organization should accept the risk. Although there are no known vulnerabilities, risks still exist. They just have not been identified yet. Nothing is without risk. Risk is defined as the probability of a threat actor exploiting a vulnerability to cause harm to the organization.

Although it is determined that there are no known vulnerabilities, the risk is NOT zero. It just means that there is no risk yet identified. Vulnerabilities will be discovered and exploited at some point. The asset should still be periodically reviewed for vulnerabilities.

Purchasing insurance is not correct because the organization has not documented any risks that could not be covered by the organization itself.

Increasing the level of protection is not correct because no known vulnerabilities have been identified and the asset appears to be adequately protected.

Objective:
Information Risk Management

Sub-Objective:
Identify, recommend or implement appropriate risk treatment/response options to manage risk to acceptable levels based on organizational risk appetite.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.7 Risk Assessment, 2.7.18, Risk Treatment (Response) Options

Question #105 of 150

Question ID: 1135927

What question should be answered in a business case to support the development of an information security program?

A) What are the threats to the organization?

B) Why should this project be undertaken?

C) What if there are no exploits after implementing the program?

D) Who should be in charge of the security program?

Explanation

The question to be answered in a business case to support the development of an information security program is why the project should be undertaken. The material in the business case should answer this question.

The business case should not ask about the threats to the organization. The assumption is that threats exist, and what is important is to establish a program to protect against and reduce the number and types of exploits.

The business case should not ask who should be in charge. After the program is accepted, details such as roles and responsibilities will be determined.

The business case should not ask whether there are no exploits after implementing the program. Finding no exploits would only be a temporary condition that an organization might achieve after implementing an information security program. But it would not be permanent.

Objective:
Information Security Governance

Sub-Objective:
Develop business cases to support investments in information security.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.4 Risk Management Roles and Responsibilities, 1.4.2 Information Security Roles and Responsibilities

Question #106 of 150

Question ID: 1185739

Which entity is responsible for overseeing all security projects to ensure that they align with the information security strategy?

A) board of directors

B) senior management

C) CISO

D) **steering committee**

Explanation

A steering committee should oversee all security projects to ensure that they align with the information security strategy. The steering committee also ensures alignment of the security program with business objectives. The steering committee helps to achieve consensus on priorities and tradeoffs.

The CEO and CISO, along with the rest of senior management, are responsible for providing leadership regarding the implementation of the security program. In doing so, they must follow the directives of the board of directors. However, these entities are not responsible for ensuring that all security projects align with the information security strategy.

Objective:
Information Security Governance

Sub-Objective:
Establish and maintain information security policies to guide the development of standards, procedures and guidelines in alignment with enterprise goals and objectives.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.3 Roles and Responsibilities, 1.3.4 Steering Committee

---

Question #107 of 150

Question ID: 1135988

While completing the threat modeling for an organization, the CISO determines that the threat to a particular set of assets has been greatly overestimated. What would be the best course of action?

A) Reduce the level of security controls to baseline.

B) Remove the controls protecting those assets.

C) Start a change management process.

D) Communicate this finding to senior management.

Explanation

After determining that the threat level has changed, the CISO should start the change management process. This would include documenting all details about the threat and changes needed, approving the changes, implementing the changes, and testing the changes to ensure that they fulfill their original intent.

Communicating this finding to senior management, while important, would be part of the change management process. However, this step is usually only completed after the change has been analyzed and documented.

The controls should not be removed until the CISO has gone through the change management process first. Controls should never be removed until a thorough analysis of the change is completed.

Reducing the existing controls may be appropriate, but is not a course of action that should be authorized until the change management process is complete. Even so, it would only be undertaken if the change management process indicates that the existing controls should be changed.

Objective:
Information Risk Management

Sub-Objective:
Monitor for internal and external factors that may require reassessment of risk to ensure that changes to existing, or new, risk scenarios are identified and managed appropriately.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.11 Risk Management Integration with Life Cycle Processes

---

Question #108 of 150

Question ID: 1185775

How often should the incident response plan be tested, reviewed, and revised? (Choose all that apply.)

A) As needed

B) The frequency is determined by the plan’s effects on business processes

C) **Yearly**

D) Semi-annually

E) When the CEO requests it

F) When personnel have time from their normal duties

Explanation

The incident response plan should be tested, reviewed, and revised yearly, semi-annually, and at the frequency determined by the plan’s effects on business processes. Depending on the type of testing being performed, from a structured walkthrough to full interruption test, business processes can be affected, and risk to the organization can increase. A testing schedule should be established that is dependent on both the risk and the projected impact of the disruption, which should be minimized. Additionally, if changes to the plan are needed, they should be tested when each revision occurs and then retested either yearly or semi-annually. The exact frequency would depend on a number of factors, such as how mature the plan is, the changing nature of security threats, and changes in software and hardware assets.

While review and revision of the plan can be done on an "as needed" basis, testing should be performed according to a schedule to minimize disruption to the organization and to ensure the plan stays updated.

While the CEO, senior management, and the board of trustees have legal responsibilities for the security of the organization, the frequency with which the plan should be tested should be determined the information security officer.

The plan should not be tested when personnel have time. If an organization relies on personnel availability, personnel will rarely have time to test, review, or revise the plan. Other duties or tasks will always take precedence.

Objective:
Information Security Incident Management

Sub-Objective:
Test, review and revise (as applicable) the incident response plan periodically to ensure an effective response to information security incidents and to improve response capabilities.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.11 Testing Incident Response and Business Continuity/Disaster Recovery Plans

, Chapter 1: Information Security Governance, 1.3 Roles and Responsibilities, 1.3.5 Chief Information Security Officer

, Chapter 1: Information Security Governance, 1.4 Risk Management Roles and Responsibilities, 1.4.1, Key Roles

Question #109 of 150

Question ID: 1185755

What is the formula to calculate the objective for MTD?

A) MTD > WRT+RTO

B) MTD < RTO

C) MTD < WRT + RTO

D) **WRT > RTO**

Explanation

Since the maximum tolerable downtime (MTD) is the maximum time an organization can suffer a loss of availability before a loss becomes unacceptable, it must be greater than the sum of the work recovery time (WRT) and the recovery time objective (RTO).

The WRT is the difference between the RTO and MTD, which is the time remaining that left after the RTO.

None of the other options provides the correct formula for determining MTD.

Objective:
Information Risk Management

Sub-Objective:
Ensure that information security risk is reported to senior management to support an understanding of potential impact on the organizational goals and objectives.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.9 Developing an Incident Response Plan, 4.9.3, Business Impact Analysis, pg. 232

Question #110 of 150

Question ID: 1136013

What kind of a control compares the existing system activity, such as adding a patch, against the approved functionality?

- **A) Preventative**
- **B)** Compensating
- **C)** Detective
- **D)** Administrative

Explanation

A detective control would involve comparing an activity, such as configuration changes, against approved functionality. Reviewing these logs is important to assure that system activities stay aligned with policies.

Compensating is not correct. This type of control reduces the impact of a deficiency. For example, if you discovered that an attack was coming from a certain MAC address, you could deploy a rule on the firewall that prevented all traffic from that MAC address.

Administrative is not correct. Administrative controls include standards and other directives.

Preventative is not correct. A preventative control is proactive, such as the use of an Intrusion Prevention System.

Objective:
Information Security Program Development and Management

Sub-Objective:
Align the information security program with the operational objectives of other business functions (e.g., human resources [HR], accounting, procurement and IT) to ensure that the information security program adds value to and protects the business.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.15 Case Study.

Question #111 of 150

Question ID: 1135965

When is it appropriate for an organization to ignore a risk? (Choose all that apply.)

A) None of these options are correct

B) When the cost is higher than the value of the asset

C) When the cost to mitigate the risk is too great

D) When the organization does not have sufficient resources to deal with the risk

E) When the impact is sufficiently small

F) When the likelihood is very rare

Explanation

An organization should consider it advisable to ignore a risk when the likelihood, exposure, or impact is small enough that it is not of concern to the organization, or when the cost of the risk impact is higher than the value of the asset. Organizations can never fully mitigate all risks.

A risk should not be ignored if the cost of mitigation is too great. Under this circumstance, it is more appropriate to transfer the risk, such as purchasing insurance to cover the loss, or avoiding the risk by using a different activity. If a particular access method, for example, is too risky and expensive to mitigate, then a different access method could be selected.

Similarly, when an organization simply does not have the resources to deal with incidents that relate to the risk, then the risk should be transferred to another party, such as by purchasing insurance.

Objective:
Information Risk Management

Sub-Objective:
Identify, recommend or implement appropriate risk treatment/response options to manage risk to acceptable levels based on organizational risk appetite.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.7 Risk Assessment, 2.7.18 Risk Treatment (Response) Options

Question #112 of 150

Question ID: 1135942

Which of the following is a SMART metric?

A) The metric is repeatable.

B) The metric is actionable

C) The metric is attainable.

D) The metric is predictable.

Explanation

Security metrics are SMART if they are:

- Specific - based on a clear goals
- Measurable - quantifiable, not subjective
- Attainable - realistic and based on important goals
- Relevant - measures of a specific goal or activity
- Timely - based on a specific time frame

Metrics that are actionable and repeatable are not included in the SMART designation, but are additional aspects to consider.

Measurements should be predictive, but not predictable.

Objective:
Information Security Governance

Sub-Objective:
Establish, monitor, evaluate and report key information security metrics to provide management with accurate and meaningful information regarding the effectiveness of the information security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.6 Information Security Governance Metrics, 1.6.1 Effective Security Metrics

Question #113 of 150

Question ID: 1185765

When an organization employs third-party service providers, what is the most important factor to ensure vendor compliance with the organization's security policies?

- **A)** Monitoring the SLA performance
- **B)** Penetration testing of the vendor's network
- **C)** Security awareness training
- **D)** **Regular audits**

Explanation

Regular audits are the most important factor to ensure compliance with the security policies of the organization. Periodic reviews by an auditor will identify risks that the third-party vendor may present to the organization.

Security awareness training will not ensure vendor compliance. Security awareness training will address operational issues within the organization, not within the organization of the third party.

Monitoring performance per the service level agreement (SLA) will not ensure vendor compliance. SLA performance does not necessarily address security policy compliance. It only ensures that the third party is providing service levels within the parameters of the SLA.

Penetration testing will not ensure vendor compliance. Penetration testing will address possible vulnerabilities, but not detect whether the vendor is compliant with the security policies of the organization.

Objective:
Information Security Program Development and Management

Sub-Objective:
Integrate information security requirements into organizational processes to maintain the organization's security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.11 Security Program Services and Operational Activities, 3.11.4 Security Reviews and Audits

---

Question #114 of 150

Question ID: 1135926

A company has been in business for a long time and has not suffered any security breaches. The company is compliant with the regulations and laws that apply to the company's business. Senior management thinks that being in compliance with the regulations means that the company is secure. What would convince senior management of the need to do more than just complying with regulations?

A) Present scenarios of potential attacks

B) Present statistics of breaches and losses of similar companies

C) Present estimates of losses in the event of a breach

D) Set up an exploit by a certified penetration tester

Explanation

Setting up an exploit by a certified penetration tester is the best option to convince senior management of the need to do more than just comply with regulations. Using a pen tester (preferably in-house) to demonstrate the exploitability of the organization's assets would be a convincing way of demonstrating to senior management that the assets are not secure and that the company has been lucky so far. This can be done using a development system running the same software as production with different data to isolate the test from the production environment. The test does not have to be extensive, just enough to show the exploitability of the systems. This can be done under the guise of routine security testing or even for educational and training purposes. The results of the penetration testing would provide valuable metrics for senior management. Only by providing a true scenario that is actually tested would you be likely to convince senior management of the risks.

Senior management appears to be under the impression that the company has not been hacked and will not be in the future. For this reason, scenarios of potential attacks and estimates of potential losses would likely be dismissed. Reports of breaches and losses of similar companies may also be dismissed by senior management.

Objective:
Information Security Governance

Sub-Objective:
Develop business cases to support investments in information security.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.4 Risk Management Roles and Responsibilities, 1.4.2 Information Security Roles and

Responsibilities

, Chapter 1: Information Security Governance, 1.6 Information Security Governance Metrics, 1.6.1 Effective Security Metrics

Question #115 of 150

Question ID: 1136089

Once an incident has been dealt with, what is potentially the most valuable part of the incident response effort?

- **A)** Threat elimination determination
- **B)** Resource restoration
- **C)** **The follow-up process**
- **D)** Senior management reports

Explanation

After the incident has been handled and determined to be over, the follow-up process can be the most valuable activity. This includes review of the documentation of the incident and lessons learned. The overall cost of the incident can be determined. This provides a metric justifying the existence of the incident response team, as well as providing legal evidence if needed in court.

Resource restoration is part of the incident response itself, which has already been completed in this scenario.

Senior management reports would be part of the follow-up report from the information security manager. Senior management reports are not as important as the follow-up process because the reports only contain information that is relevant to senior management.

Threat elimination determination is part of the incident response itself, not the follow-up.

Objective:
Information Security Incident Management

Sub-Objective:
Conduct postincident reviews to determine the root cause of information security incidents, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.13 Postincident Activities and Investigation

---

Question #116 of 150

Question ID: 1135975

Which of the following approaches is the best way to determine whether information security controls are effective?

- **A) Compare the observed incidence of alerts to the baseline level of alerts.**
- **B)** Determine the number of alerts.
- **C)** Track the number of alerts over time.
- **D)** Increase the baseline if the number of alerts consistently exceeds the baseline.

Explanation

Comparing the number of alerts to the baseline gives an indication of whether or not the chosen controls are effective, since the baseline is established as the minimum acceptable security level.

Tracking the number of alerts of time does not give any indications of how the controls are performing relative to the minimum acceptable security level. Tracking the number of alerts over time may help to establish the baseline. However, new alert numbers must be compared to the baseline to determine if the controls are effective.

Determining the number of alerts is not the best approach. Without a metric to compare it to, raw data such as the number of alerts provides no meaning.

Increasing the baseline is not the best approach. Changing the baseline is appropriate if control configuration has changed, if the number of users or devices increases, or if the protection level is changed. Organizations should determine the parameters that would define the need to capture a new baseline and document these parameters.

Objective:
Information Risk Management

Sub-Objective:
Determine whether information security controls are appropriate and effectively manage risk to an acceptable level.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.7 Risk Assessment, 2.7.24 Events Affecting Security Baselines

---

Question #117 of 150

Question ID: 1185757

What is the primary purpose of an information security program?

- **A)** To define the information security strategy
- **B)** To develop security metrics
- **C)** To develop asset classification
- **D) To execute the information security strategy**

Explanation

The primary purpose of an information security program is to execute the information security strategy. Another purpose is to achieve the objectives for acceptable risk levels and business disruption.

The primary purpose of an information security program is not to define the information security strategy. While the information security strategy is defined as part of the information security program, that is not the information security program's primary purpose.

The primary purpose of an information security program is not to develop security metrics. Developing metrics is important, but it is a secondary purpose.

The primary purpose of an information security program is not to develop asset classification. This is also an important goal, but it is secondary to executing the information security strategy.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish and/or maintain the information security program in alignment with the information security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, Introduction

Question #118 of 150

Question ID: 1135947

While developing a risk management program, an organization determines that the cost of providing additional mitigation of threats to a particular set of assets is greater than the value of the assets themselves. The assets under consideration are important, but not critical to the organization's business continuity. The risk was estimated to be about 50% of the asset's value. What should the risk response be for this situation?

- **A) The risk should be accepted.**
- **B)** The risk should be avoided.
- **C)** The risk should be transferred.
- **D)** The risk should be mitigated anyway.

Explanation

The response should be to accept the risk because the asset is not critical to the company's operation and the value of the asset is lower than the cost of mitigation.

The risk should be not be transferred. Enabling a third party, such as an insurance company, to assume the risk at a lower cost than implementing additional mitigation procedures is often a viable solution for higher-level risks or risks to assets that have high value.

Implementing additional mitigation does not make economic sense. The cost of additional mitigation measures would increase the cost of protecting the asset beyond what it is worth.

The risk should not be avoided because the asset is important and needs to be accessible. Avoiding a risk usually means avoiding the situation or condition that would lead to the risk, such as decommissioning the asset to avoid the risk. However, decommissioning the asset would impede business operations.

Objective:
Information Risk Management

Sub-Objective:
Establish and/or maintain a process for information asset classification to ensure that measures taken to

protect assets are proportional to their business value.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.12 Strategy Constraints, 1.12.11, Risk Acceptance and Tolerance

, Chapter 2: Information Security Risk Management, 2.7 Risk Assessment, 2.7.18, Risk Treatment (Response) Options

Question #119 of 150

Question ID: 1135936

To obtain the support for senior leadership for a security program, a request was made to develop an enterprise-wide security architecture that focuses on risk. Which architecture framework would be appropriate?

A) ITIL

B) CMMI

C) Zachman

D) **SABSA**

Explanation

The Sherwood Applied Business Security Architecture (SABSA) is an enterprise security architecture framework that is risk driven. It consists of six communication questions (What, Where, When, Why, Who, and How) against six organizational layers (operational, component, physical, logical, conceptual and contextual). The six questions and layers form a 2-D matrix. The resulting object in each cell of the 2-D matrix is one aspect of security. SABSA is similar in structure to and derived from the Zachman framework.

The Zachman framework is an enterprise architectural framework that allows you to classify various aspects of an organization by functional areas. However, the Zachman framework does not focus on risk. It is a two dimensional framework that enables the analysis of the organization to be communicated in ways that are appropriate for each group.

The IT Infrastructure Library (ITIL) is an IT best practices framework.

The Capability Maturity Model Integration (CMMI) is a process improvement model.

Objective:

Information Security Governance

Sub-Objective:

Gain ongoing commitment from senior leadership and other stakeholders to support the successful implementation of the information security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.11 Strategy Resources, 1.11.2 Enterprise Information Security Architecture(s)

Question #120 of 150

Question ID: 1136065

Which phase of the six-phase incident response model must be followed to determine whether a security incident has occurred?

A) **Identification**

B) Recovery

C) Preparation

D) Business impact analysis

Explanation

The identification phase of the model includes verifying that events qualify as an incident, assigning ownership of the event that may be an incident to an incident handler, determining the severity of the incident, and establishing custody regarding evidence handling.

The recovery phase is about restoring systems and services to the requirements established by the service delivery objectives or the business continuity plan.

The preparation phase develops the incident response plan.

The business impact analysis is not part of the six-phase model. It is a separate activity included in the development of the business continuity plan.

The six phases of the incident response plan model are as follows:

- Preparation
- Identification

- Containment
- Eradication
- Recovery
- Lessons learned

Objective:
Information Security Incident Management

Sub-Objective:
Develop and implement processes to ensure the timely identification of information security incidents that could impact the business.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.9 Developing an Incident Response Plan, 4.9.1 Elements of an Incident Response Plan

---

Question #121 of 150

Question ID: 1136043

Which statement is true about outsourcing services to third-party vendors?

A) **The total cost of the service will generally be less than insourcing if used for the length of the contract.**

B) If the requirements of the organization change, it is easy to adjust the contract to coordinate the level of service with the changing requirements.

C) Prior to implementing an SLA, the third-party security policies and track record must be evaluated

D) If the vendor is highly recommended by the industry, a third-party evaluation is not required.

Explanation

Prior to implementing an SLA, the third-party security policies and track records must be evaluated. Like any other security activity in an organization, contracting with an outside vendor should be treated like change or configuration management, in which a thorough review is mandated.

The total cost of the service will not generally be less than insourcing if used for the length of the contract. A long-term contract has very little economic benefit. Service levels are fixed by contract, but circumstances can result in the vendor demanding higher fees if additional services are needed. Additionally, if the requirements for the service are reduced, then the organization is buying unneeded services.

You should never bypass the evaluation of a highly recommended vendor. Acquiring the services of a third-party vendor should always be fully researched, even if highly recommended.

If the requirements of the organization change, it is not easy to adjust the contract. Unless there are clauses in the contract to adjust the level of service to changing requirements, then it will be very difficult to change and may result in the company overpaying for services or paying higher costs for additional unexpected requirements.

Objective:
Information Security Program Development and Management

Sub-Objective:
Integrate information security requirements into contracts and activities of third parties and monitor adherence to established requirements in order to maintain the organization's security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.11 Security Program Services and Operational Activities, 3.11.9 Outsourcing and Service Providers

---

Question #122 of 150

Question ID: 1135915

In order to establish an information security strategy, what should be the first consideration?

A) Business impact analysis

B) Business strategy

C) Conformance with regulations

D) Risk assessment

Explanation

The first consideration of an information security strategy is the business strategy. The information security strategy must support the business strategy. The business strategy defines the objectives of the organization.

A risk assessment requires knowing in part what needs to be protected in the organization. Additionally, risk assessments are performed by personnel which has not been defined yet.

A business impact analysis will be part of the evaluation of the current state of the organization, but until the business strategy is consulted, the impact of a loss cannot be known.

The regulations for which the organization must comply cannot be determined without the business strategy. Additionally, conformance with regulations does not ensure that the organization has sufficient security.

Objective:
Information Security Governance

Sub-Objective:
Integrate information security governance into corporate governance to ensure that organizational goals and objectives are supported by the information security program.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.7 Information Security Strategy Overview

---

Question #123 of 150

Question ID: 1185761

What is the most important technology to deploy when implementing a BYOD policy?

A) Firewall
B) **IPS**
C) DLP
D) MDM

Explanation

The most important technology to deploy when implementing a bring your own device (BYOD) policy is mobile device management (MDM). A BYOD policy allows people to use their personal devices in the business environment. The MDM configures these devices to comply with the organization's security policies.

An intrusion prevention system (IPS) is not part of a BYOD policy. Mobile devices can bypass the organization's network controls. An IPS examines incoming traffic only which is important to protect the organization's resources.

Data loss prevention (DLP) is not correct. DLP ensures that data is protected from being transmitted outside the organization based on policies. While is DLP could enhance a BYOD policy, it's primary usage is to protect data, not control BYOD usage.

A firewall is not correct. A firewall protects networks from certain types of traffic based on the configured access control lists (ACLs). ACLs can be based on a variety of factors, including application type, port number, and MAC address. A firewall would control traffic that could be sent to the mobile device through the firewall.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish and maintain information security processes and resources to execute the information security program in alignment with the organization's business goals.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.7 Risk Assessment, 2.7.10 Threats

---

Question #124 of 150

Question ID: 1136086

A login failure is logged by the organization's SIEM. How should this be handled?

A) The event is probably a one-off event due to an employee's typographical error and should be ignored.

B) The event should be elevated to the information security manager.

C) **The event should be logged.**

D) The event should be elevated to an incident.

Explanation

A single negative event, such as a single login failure, should simply be logged for reference. This is not a security concern. However, if the SIEM reports a number of failed login attempts, it could be the result of an attack, which should be escalated to an incident and the incident response team contacted. This kind of event should be part of the incident response policies.

An event is a change of state of the system and includes negative and positive events. An incident is a series of events that can negatively affect the organization's operations and security.

The single failed login attempt is an event and should not be elevated. The SIEM may be reporting other, more serious incidents that should not be overlooked because of single event.

All events should be logged for future reference.

Because the single failed login attempt does not negatively affect the organization, the event does not need to be elevated to a higher tier of support.

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain communication plans and processes to manage communication with internal and external entities.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.8 Current State of Incident Response Capability

, Chapter 4: Information Security Incident Management, 4.9 Developing an Incident Response Plan, 4.9.1 Elements of an Incident Response Plan

---

Question #125 of 150

Question ID: 1135948

What is the third step in the NIST SP 800-30 risk assessment methodology?

A) System characterization

B) Control analysis

C) Vulnerability identification

D) Threat identification

Explanation

The steps for the NIST SP 800-30 risk assessment methodology are:

- System characterization
- Threat identification
- Vulnerability identification
- Control analysis
- Likelihood determination
- Impact analysis
- Risk determination
- Control recommendations
- Results documentation

Objective:
Information Risk Management

Sub-Objective:
Establish and/or maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.7 Risk Assessment, 2.7.5 NIST Risk Assessment Methodology

Question #126 of 150

Question ID: 1138435

What is the ultimate purpose of the various metrics in the information security program?

A) **Performance indicators**

B) Measuring compliance with standards and regulations

C) Goal indicators

D) Decision-making support

Explanation

Metrics are used to support decision-making. The ultimate purpose of collecting metrics is to manage and provide information to make informed decisions.

Performance indicators, goal indicators, and compliance measurement are not correct. These are all types of metrics that are used for making decisions, but are not the ultimate purpose of the program.

Objective:
Information Security Program Development and Management

Sub-Objective:
Establish, communicate and maintain organizational information security standards, guidelines, procedures and other documentation to guide and enforce compliance with information security policies.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.13 Security Program Metrics and Monitoring, 3.13.1 Metrics Development

---

Question #127 of 150

Question ID: 1135993

An organization has suffered a breach of their database due to improper configuration management of their systems. The breach resulted in the capture of millions of encrypted and hashed records containing personally identifiable information. Which of the following would occur as a result of this breach? (Choose all that apply.)

A) Loss of credibility

B) Loss of public confidence

C) Regulatory actions

D) Loss of availability

E) Loss of confidentiality

F) Loss of integrity

Explanation

The exposure of personally identifiable information would result in the loss of credibility and public confidence for the simple reason that it was exposed. Also, because personally identifiable information is protected by regulations and laws, some form of regulatory action would be involved, such as an investigation and possible sanctions.

Because the data is encrypted, it is protected and unreadable by the attacker. Therefore, there is no loss of confidentiality.

Hashing the data does not guarantee that the data will not be modified. Hashing anonymizes the data, and hashes can be used to verify if the data was modified. Within the given scenario, loss of integrity cannot be verified without comparing the hashing values of the data.

Unless the data was modified, removed from the servers, or subject to a DoS or DDoS attack, availability of the data is not affected. In this case, the data in question was exposed and not lost.

Objective:
Information Risk Management

Sub-Objective:
Report noncompliance and other changes in information risk to facilitate the risk management decision-making process.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.7 Risk Assessment, 2.7.1 Information Asset Identification and Valuation.

Question #128 of 150

Question ID: 1135946

Which of the following is the BEST description of security controls?

A) Security controls include specific mitigation measures.

B) **Security controls include processes that counter specific threats.**

C) Security controls include configuring a firewall to block a specific IP address.

D) Security controls include any means of managing risk.

Explanation

Security controls include any means of managing risk, including those that are administrative, technical, management, or legal in nature. They are part of the risk management framework, which includes policies, standards, procedures, practices, and organizational structures. The framework guides all subsequent information security activities.

Security controls do not include processes to counter specific threats. They counter specific risks, not threats. Countermeasures are used to counter specific threats.

Configuring a firewall to block a specific IP address is a countermeasure. Implementing a firewall is a technical security control, but blocking a specific IP address on the firewall is a measure taken against a specific threat, not general risk prevention. The firewall is a security control, while the IP address blocking rule is a countermeasure.

Mitigation measures are countermeasures to block specific attacks.

Objective:
Information Risk Management

Sub-Objective:
Establish and/or maintain a process for information asset classification to ensure that measures taken to protect assets are proportional to their business value.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.1 Risk Management Overview

Question #129 of 150

Question ID: 1135981

Which of the following is included in the risk management life cycle?

A) Evaluation of the types of attacks that are getting through the controls

B) **Change management integration with risk identification, analysis, evaluation, and mitigation activities.**

C) Performing a business impact analysis (BIA)

D) Strict adherence to COBIT 5

Explanation

The risk management life cycle includes assessment, treatment, and monitoring phases. These phases provide integration of change management processes during the entire cycle to improve control over the organizations information resources.

The four stages of the IT risk management life cycle are IT risk Identification, IT risk assessment, risk response and mitigation, and risk and control monitoring and reporting.

The business impact analysis (BIA) is not included in the risk management life cycle. It precedes the life cycle. Prior to identification of risks and the other phases of the life cycle, the BIA will prioritize how compromises will impact the organization. Once these impacts are identified, then the risk to the assets included in the BIA can be identified. As assets change, the BIA should be repeated.

Strict adherence to COBIT 5 is not included in the risk management life cycle. The methods outlined within COBIT and other frameworks can be used when performing the BIA. However, adherence to COBIT 5 is not required as part of the risk management life cycle.

Evaluation of the types of attacks that are getting through the controls is not included in the risk management life cycle. Examining the types of attacks is a part of normal monitoring and reporting operations. The results of this analysis could trigger the risk management life cycle.

Objective:
Information Risk Management

Sub-Objective:
Facilitate the integration of information risk management into business and IT processes to enable a consistent and comprehensive information risk management program across the organization.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.11 Risk Management Integration with Life Cycle Processes, 2.11.2 Life Cycle-Based Risk Management Principles and Practices

---

Question #130 of 150

Question ID: 1185767

You are working with a vendor to develop an SLA. The vendor will maintain certain devices on an organization’s network. Which of the following should be included as part of the SLA?

A) MTD

B) MTBF

C) RTO

D) MTTR

Explanation

The mean time to repair (MTTR) should be included as part of the SLA. This would state the requirements for the vendor to repair or replace a device and restore it to service within a certain time frame.

The mean time between failures (MTBF) is an estimate by an equipment vendor of the life span of the device. It would not be included in the SLA.

Recovery time objective (RTO) and maximum tolerable downtime (MTD) are part of the organization's security program and determined by business needs. They would determine the MTTR to be included in the SLA. The RTO and MTD would not be determined by the vendor providing the SLA.

Objective:
Information Security Program Development and Management

Sub-Objective:
Integrate information security requirements into contracts and activities of third parties and monitor adherence to established requirements in order to maintain the organization's security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.11 Security Program Services and Operational Activities, 3.11.9 Outsourcing and Service Providers

Question #131 of 150

Question ID: 1136039

What would be the most likely outcome if restrictive procedures were applied uniformly across all departments in the organization?

A) Some departments might have excessive restrictions.

B) **Security procedures are likely to be circumvented.**

C) Some departments might have insufficient controls.

D) Centralized administrative control of all security procedures and processes would occur.

Explanation

Security procedures are likely to be circumvented if restrictive procedures were applied uniformly across all departments in the organization. A blanket policy applied across the entire organization is likely to have procedures that are too restrictive for some departments, increasing the likelihood of those procedures being circumvented.

Centralized administrative control is already part of a uniform approach. This is simply a restatement of the question, in that a blanket security policy is likely to be centrally administered.

Departments having excessive or insufficient controls is not the most likely outcome.

Objective:
Information Security Program Development and Management

Sub-Objective:
Integrate information security requirements into organizational processes to maintain the organization's security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.12 Controls and Countermeasures

---

Question #132 of 150

Question ID: 1185759

Which of the following basic tenets of security raises potential conflicts between the security program and the information technology (IT) department?

A) Availability

B) Authentication

C) Confidentiality

D) **Integrity**

Explanation

The availability tenet raises potential conflicts between the security program and the information technology (IT) department. One important function of the IT department is to make resources on the network available to users. However, doing so can sacrifice security. Security policies have to apply the access policies, which can include multifactor logins that can limit availability.

Confidentiality refers to applying cryptographic methods, such as PKI certificates, to communications. Confidentiality should not limit availability once the proper software is implemented.

Integrity refers to ensuring that data is not modified as it traverses communication paths. Integrity is guaranteed with certificates and hashes, and does not limit an employee's access to resources.

Authentication is not one of the three basic tenets of security.

Objective:
Information Security Program Development and Management

Sub-Objective:
Align the information security program with the operational objectives of other business functions (e.g., human resources [HR], accounting, procurement and IT) to ensure that the information security program adds value to and protects the business.

References:

CISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.11 Security Program Services and Operational Activities, 3.11.1 Information Security Liaison Responsibilities

---

Question #133 of 150

Question ID: 1136063

How often should an incident response plan be reviewed to ensure that an organization is fulfilling the incident response goals?

A) On an ad hoc basis

B) Semi-annually

C) Before an incident occurs

D) **At least annually**

Explanation

After the incident response plan has been developed, management has approved it, and the plan is implemented, it should be reviewed at least annually. This ensures that the road map established by the plan is being followed.

Semi-annual review is not necessary given the requirement of annual or more frequent reviews. The frequency would depend on the threat environment and other factors, but a working goal is that it be reviewed at least annually so as not to overload personnel who have other tasks.

Reviewing the plan before an incident occurs is not feasible because incident occurrence cannot be predicted.

Ad hoc review is hit or miss. The criteria for actually doing the review are not established. This kind of strategy can often be superseded by other seemingly more important or urgent activities.

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.10 Business Continuity and Disaster Recovery Procedures, 4.10.8 Response and Recovery Plan

---

Question #134 of 150

Question ID: 1135999

The information security manager has been informed by a vendor that the servers the organization is using will no longer be manufactured. When researching replacement servers, the manager finds that many of the initial estimates regarding repair and/or replacement have changed, which could adversely affect the organization's business operations. The information security manager must decide whether to replace the current servers with the new servers or to purchase additional backup servers identical to the ones currently in operation. Which of the following tools should he used to help in this determination?

A) **BIA**

B) BCP

C) RPO

D) RTO

Explanation

The recovery time objective (RTO) must be considered when purchasing new equipment. Repair or replacement time may be adversely affected with new equipment such that the repair time may exceed the RTO, while this should be a known quantity with regards to the current equipment.

The business impact analysis (BIA) is an analysis of the sensitivity of the assets to loss and the associated cost. A BIA should have already been completed to obtain the costs associated with service interruptions for business systems or processes.

The business continuity plan (BCP) is a plan used to an organization to respond to disruption of critical business processes.

The recovery point objective (RPO) refers to a point in time to recover data from an interruption in service. It delineates the most recent point in time to which it is acceptable to recover the data, which is usually the latest backup. Depending on the asset criticality to the organization, the RPO may be higher or lower than other assets.

Objective:
Information Risk Management

Sub-Objective:
Ensure that information security risk is reported to senior management to support an understanding of potential impact on the organizational goals and objectives.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.9 Operational Risk Management, 2.9.1 Recovery Time Objectives

---

Question #135 of 150

Question ID: 1135985

In most cases, which is the best method for determining resource valuation?

A) By determining whether the asset is tangible or intangible

B) By considering the cost of developing the asset

C) By considering loss scenarios

D) By looking at the value of similar assets from other companies

Explanation

In most cases, effective resource valuation is best based on loss scenarios. This can be done by developing a matrix with each loss scenario. This procedure enables the company to prioritize the resources, if it is done in a consistent manner.

The value of assets used by other companies is not correct. Each company has different requirements for valuing resources. What is very important for one company may be of lesser importance to another, and therefore they will prioritize the resources differently.

The cost of developing the asset is incorrect because this method does not take into account the amount by which the company profits from that asset.

Intangible assets include intellectual property such as trade secrets, patents, brand reputation, etc. Tangible assets include the physical facilities, hardware, software, and information. All assets should be valued to determine the degree of protection that is needed for the asset, and not whether the asset is tangible or intangible.

Objective:
Information Risk Management

Sub-Objective:
Monitor for internal and external factors that may require reassessment of risk to ensure that changes to existing, or new, risk scenarios are identified and managed appropriately.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.7 Information Asset Identification and Valuation

---

Question #136 of 150

Question ID: 1135912

When developing the information security governance, which of the following frameworks or standards provides a model for continuous improvement?

A) CMMI

B) **Balanced Scorecard**

C) COBIT 5

D) EISA

Explanation

The Capability Maturity Model Integration (CMMI®) is a framework for continual improvement of the process of developing information security governance. It consists of five maturity levels that start at level 0, where the process is incomplete, and move up from the initial stage to managed, defined, qualitatively managed, and optimized. The framework can achieve better quality of development of information security governance.

COBIT 5 is a governance and management of enterprise IT framework. It is based on five principles for governance and management, which are:

- Meeting stakeholder needs
- Covering the enterprise end to end
- Applying a single integrated framework
- Enabling a holistic approach
- Separating governance from management

The balanced scorecard is a management system that helps measure, clarify, and realize the organization's vision and strategy.

The Enterprise Information Security Architecture (EISA) is a subset of the entire organization's architecture with a foundational structure or set of structures.

Objective:
Information Security Governance

Sub-Objective:
Establish and/or maintain an information security governance framework to guide activities that support the information security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.8 Information Security Strategy Objectives, 1.8.3 The Desired State.

Question #137 of 150

Question ID: 1136062

What is the most common impediment to developing an incident management plan?

- **A) Lack of communication processes**
- **B)** Failure to obtain management buy-in and consensus among the business units
- **C)** Turnover of incident management team members
- **D)** Mismatch with organizational goals

Explanation

Most challenges to developing an incident management plan result from a lack of management buy-in and organizational consensus. This can be the result when senior management and other stakeholders are not involved in the planning process. Ownership of the plan is important for its support.

A mismatch with organizational goals can be a challenge to developing an incident management plan, but it is not as likely to occur as lack of management buy-in. When a business is operating at a rapid rate with many changes occurring over a short time, incident management may not be able to keep up.

Incident management planning takes time and people involved may leave unexpectedly. While turnover rate can affect the development of an incident management plan, it is not as likely as lack of management buy-in.

Failure to communicate or ineffective communication results in stakeholders not receiving the appropriate information. While this is an issue, it is not as likely to be the problem as lack of management buy-in.

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.9 Developing an Incident Response Plan, 4.9.9 Challenges in Developing an Incident Management Plan

Question #138 of 150

Question ID: 1135905

Which role or group is responsible if an organization fails to adequately implement an information security program?

- **A)** Chief Information Security Officer
- **B) Board of directors**
- **C)** Chief Executive Officer
- **D)** Information security manager

Explanation

The board of directors is responsible if an organization fails to adequately implement an information security program. The need for development and implementation of an adequate information security program must be raised at the BOD level.

The CEO and CISO, along with the rest of senior management, are responsible for providing leadership regarding the implementation of the security program. In doing so, they must follow the directives of the board of directors.

The information security manager is responsible for the overseeing the security programs in the organization, along with the CISO.

Objective:
Information Security Governance

Sub-Objective:
Establish and/or maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and/or ongoing management of the information security program.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.3 Roles and Responsibilities, 1.3.5 Chief Information Security Officer

, Chapter 1: Information Security Governance, 1.3 Roles and Responsibilities, 1.3.1, Board of Directors

, Chapter 1: Information Security Governance, 1.4 Risk Management Roles and Responsibilities, 1.4.1 Key Roles

Question #139 of 150

Question ID: 1135908

What is the preferred way of implementing the information security program?

- **A)** Bottom-up implementation
- **B)** By presenting it to senior management
- **C)** By modeling the program after companies in the same industry
- **D)** **Top-down implementation**

Explanation

The top-down approach is the preferred way of implementing the security program. It has been shown that the support of senior management is essential for an effective information security program. Senior management has the clearest grasp of the business goals of the organization, which drive the development of the information security program. Because these policies come from the top of the organization, employees are far more likely to comply.

Bottom-up is not the preferred way to implement the security program. The information security program must be driven by business goals, which the employees on the lower levels of the organization chart do not have.

A security program is not implemented after being developed for senior management. That program is not developed by senior management and may not have their full support nor cover all the goals of the organization.

A security program is not implemented by being modeled after other organizations' programs. No two organizations have the same security requirements, even if they are in the same industry. The structure and business goals of another organization will be different from yours.

Objective:
Information Security Governance

Sub-Objective:
Establish and/or maintain an information security strategy in alignment with organizational goals and objectives to guide the establishment and/or ongoing management of the information security program.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.1 Effective Information Risk Management, 2.3.1 Developing a Risk Management Program

Question #140 of 150

Question ID: 1136082

Which of the following is a part of protect phase of the incident response plan process flow?

A) Establish incident-handling criteria

B) Provide input to the detect phase

C) **Remediation efforts**

D) Log analysis

Explanation

Providing input to the detect phase is part of the protect phase of the incident response plan process flow. The goals of the protect process are to protect and secure assets during an incident response.

Incident-handing criteria are established in the prepare phase, in which planning and design functions are performed and coordination policies are created.

Remediation is included in the triage process, which includes prioritization of actions to ensure maximum effectiveness of the limited resources available after an incident.

Log analysis is included in the respond process, which attempts to resolve or mitigate the incident.

The phases of the incident response planning process flow are:

- Prepare
- Protect
- Detect
- Triage
- Respond

Objective:
Information Security Incident Management

Sub-Objective:
Test, review and revise (as applicable) the incident response plan periodically to ensure an effective response

to information security incidents and to improve response capabilities.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.7 Defining Incident Management Procedures

Question #141 of 150

Question ID: 1135958

Which level of an organization should be aware of regulatory issues?

A) Regular staff

B) Senior management

C) **Middle management**

D) Technical staff

Explanation

Senior management must be aware of applicable regulations regarding their industry.

Technical staff, regular staff, and middle management do not need awareness training regarding regulatory issues. Upper management requires training in both regulatory and legal issues. Middle management's training should include policies, standards, and baselines. Technical staff should be trained in policies, standards, the configuration of security controls, and attack recognition. Regular staff should be trained in programs to guide their day-to-day activities in a secure manner.

Objective:
Information Risk Management

Sub-Objective:
Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.7 Risk Assessment, 2.7.22 Legal and Regulatory Requirements

Question #142 of 150

Question ID: 1135925

You need to develop a feasibility study, which will be used to document the business case. Which of the following should be included for developing a feasibility study to senior management for implementing a new security control? (Choose all that apply.)

A) **Business impacts**

B) Project scope

C) **The estimated return on security investment**

D) **What systems can be affected**

E) Technical details about a newly discovered threat

F) Total estimated cost of mitigation

Explanation

The business case should include:

1. Project scope
2. Current analysis to explain why the current system is not adequate and what systems can be affected
3. Requirements, including regulatory processes, and end-user needs
4. Recommended mitigation strategies and alternatives
5. Evaluation of work already completed, estimated number of employees and time, total estimated costs, and return on security investment
6. Formal review by stakeholders

Technical details about a threat would not be needed by senior management. Their interest lies in terms of business impacts.

Objective:
Information Security Governance

Sub-Objective:
Develop business cases to support investments in information security.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.4 Risk Management Roles and Responsibilities, 1.4.2 Information Security Roles and Responsibilities

Question #143 of 150

Question ID: 1185751

Which of the following items refers to the level of deviation from the acceptable risk level?

- **A)** Risk appetite
- **B)** Risk evaluation
- **C)** Risk assessment
- **D)** **Risk tolerance**

Explanation

Risk tolerance is the acceptable level of deviation from the acceptable level risk.

Risk appetite refers to what management considers to be an acceptable level of risk.

Risk assessment includes activities that are undertaken to measure risk, including auditing all of the organization’s assets to determine their sensitivity or value to the organization. Their value includes the cost to the organization if any or all of the assets were unavailable, stolen, or copied. Risk assessments include analyses of threats, vulnerabilities, and impacts for each asset. The analyses are used to estimate acceptable risk and develop policies.

Risk evaluation involves analyzing the identified risks and developing the Business Impact Analysis (BIA) to determine whether the risk is acceptable or must be mitigated.

Objective:
Information Risk Management

Sub-Objective:
Ensure that risk assessments, vulnerability assessments, and threat analyses are conducted consistently, at appropriate times, and to identify and assess risk to the organization's information.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.1 Risk Management Overview, 2.3 Effective Information Risk Management, 2.3.1 Developing a Risk Management Program

Question #144 of 150

Question ID: 1136014

All business units, including accounting and human resources, must be included in the information security program. What must the security manager do to align the information security program with those units?

- **A)** Members of the different business units should be involved with security and awareness training.
- **B)** The business manager should set up strict access controls for all members of the different business units.
- **C)** Members of the different business units should be informed of the policies that will be put in place.
- **D)** **For uniformity, all units should have the same security policy implementation details.**

Explanation

Member of the different business units should be involved with security and awareness training. In general, members of the business units are not necessarily security aware and may not have technical skills. The security manager must engage these groups for an appropriate level of training and make them aware of the risks inherent in careless computer activity.

Because the different business units do not all have the same security requirements, each unit should be have difference implementations of the security policies. Human resources, for example, must have personnel data kept private from the rest of the company.

Informing the members of the different business units about what policies will be put in place with not align them with the information security program. As a group, they will not necessarily subscribe to those policies unless they have had some input and training. Even with good policies that the members can agree upon, implementing the policies will not protect the business unit from human error or misuse without awareness training. In addition, engaging the members as the policies are designed will help to ensure user buy-in and will result in a more successful program.

The business manager should not set up the access controls for each business unit. Access controls are up to the data owners and data custodians. For example, the head of the business unit should have access to all data for that unit, with varying degrees of access for the other members of the unit. Only the head of the business unit understands what those roles are and what privileges should be granted.

Objective:

Information Security Program Development and Management

Sub-Objective:

Align the information security program with the operational objectives of other business functions (e.g., human resources [HR], accounting, procurement and IT) to ensure that the information security program adds value to and protects the business.

References:

CISM Review Manual, 15th EditionCISM Review Manual, 15th EditionCISM Review Manual, 15th Edition, Chapter 3: Information Security Program Development and Management, 3.10 Security Program Management and Administrative Activities

, Chapter 3: Information Security Program Development and Management, 3.10 Security Program Management and Administrative Activities, 3.10.2 Security Awareness Training and Education

, Chapter 3: Information Security Program Development and Management, 3.10 Security Program Management and Administrative Activities, 3.10.1 Personnel, Roles, Skills and Culture,

---

Question #145 of 150

Question ID: 1136084

Where should the staff directory and incident response plans be stored so that they are quickly accessible in case of fire and not susceptible to interruptions in network availability?

A) **Off site storage**

B) Hard copies in desk drawer

C) Notebook computer

D) Central server

Explanation

In the case of a fire, grabbing papers from a drawer would be the quickest way to get the incident response plan and respond to the emergency, because a fire threatens human safety and response time can be a critical factor.

Accessing the directory and response plan from web servers, from individual computers, or from off-site storage may not work because of potential interruptions to power and connectivity. These solutions will not provide the portability and ease of a hard copy.

Objective:

Information Security Incident Management

Sub-Objective:

Establish and maintain communication plans and processes to manage communication with internal and external entities.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.2 Incident Response Procedures

---

Question #146 of 150

Question ID: 1185749

An audit determines that an organization specifies greater security requirements than the applicable regulations. The organization is in compliance with the regulatory requirements, but not with its organizational security policies. What should the organization do?

A) The organization does not need to do anything further because systems are secure.

B) **The organization should increase its security posture to the levels required by its policies.**

C) The organization should substitute a different regulation that specifies a greater degree of security that matches the organization's policies.

D) The organization should request an improvement in the security requirements described by the regulations.

Explanation

When an organization's security requirements exceed those required by regulations, the organization should increase their security controls to the levels required by its policies. The requirements in a regulation describe the baseline security levels.

Meeting regulatory requirements does not mean that the organization is secure. Meeting the regulatory requirements is not a reason to do nothing to improve the organization’s security posture. When the audit discovered that the security posture does not comply with the organization's security policies, then the security posture needs to be increased.

Requesting that the regulations should improve their security requirements is not correct. Those requirements are established to provide a baseline level of security and offer the minimal acceptable level of security across the specific industries that the regulations represent.

The choice of which regulations to follow is determined by the nature of the organizations business. For example, if an organization finds that the PCI-DSS regulation does not meet its security requirements it would be inappropriate to substitute the HIPAA regulations if it is found that the requirements in HIPAA offer greater security. However, that does not mean that the organization does not need to meet the requirements of the regulations required by the particular industry. The organization can also implement security requirements from other regulations as appropriate. It is always best for the security posture to exceed the recommended baseline.

Objective:
Information Risk Management

Sub-Objective:
Identify legal, regulatory, organizational and other applicable requirements to manage the risk of noncompliance to acceptable levels.

References:

CISM Review Manual, 15th Edition, Chapter 2: Information Risk Management, 2.7 Risk Assessment, 2.7.22 Legal and Regulatory Requirements

Question #147 of 150

Question ID: 1136044

Which document is essential for guaranteeing performance requirements for a vendor?

A) Non-compete agreement

B) SLA

C) **Contract**

D) NDA

Explanation

A service level agreement (SLA) is essential for guaranteeing performance requirements for a vendor. The SLA is a contract between the organization and the vendor. It includes details regarding response times to issues, service uptimes, and penalties for non-compliance.

A nondisclosure agreement (NDA) is not correct. While this document must be signed by the vendor if they have access to the organization's data, it does not provide guarantees regarding performance requirements.

A non-compete agreement is a document that prevents the signer from providing services that compete with the organization.

While the NDA and SLA are contracts, simply calling a document a contract does not make it essential for guaranteeing vendor performance.

Objective:
Information Security Program Development and Management

Sub-Objective:
Integrate information security requirements into contracts and activities of third parties and monitor adherence to established requirements in order to maintain the organization's security strategy.

References:

CISM Review Manual, 15th Edition, Glossary, Service Level Agreement

---

Question #148 of 150

Question ID: 1136087

An organization has experienced a severe breach that is determined to be a criminal act. Who is responsible for contacting law enforcement?

A) Public relations representative

B) Information security manager

C) Senior management

D) Legal department

Explanation

The responsibility for contacting law enforcement lies with senior management. Involving law enforcement prematurely can interrupt the activities of the incident response team because of the restrictions imposed by law enforcement. Properly trained members of the team, who are the most familiar with the systems involved, can perform forensic examinations that adhere to chain of evidence. Including law enforcement may impose different personnel and requirements.

The information security manager is generally not involved with contacting external organizations. Such contact has to be carefully organized to minimize the damage to the company's reputation.

Public relations will generally be involved with contacting media regarding incidents that affect the company's operations. This is done with the goal of not just informing the public but also for minimizing damage to the organization's reputation.

The legal team would be involved with assisting developing the legal actions against the individuals involved with causing the breach. The legal team is also involved in consultations with other teams including the development communication plans, liability protections, legal compliance with regulatory requirements, etc.

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain communication plans and processes to manage communication with internal and external entities.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.10 Business Continuity and Disaster Recovery Procedures, 4.10.10 Notification Requirements

---

Question #149 of 150

Question ID: 1136075

How should escalation of an event be handled?

A) The event should be escalated to the next available person.

B) The incident response actions should be paused if the responsible person is not available.

C) The event should be escalated to the responsible person, even if minor.

D) **Escalation should be done based on the IRP and the sequence of actions described in it.**

Explanation

Escalation of an event should be done when it is evident that it is an incident that has generated an alarm. It should be done on the basis of the list of actions to be taken in the sequence that has been defined.

Events do not need to be escalated until it is clear that they represent an actual threat, such as repeated attempted failed logins. A single failed login is an event, but does not constitute a threat or generate an alarm. Therefore, involving someone who may be available in a minor event will just lead to confusion and take people away from their other tasks.

In the case where a responsible person is not available, the response actions should not be paused. Rather, the plan should identify alternates who would be contacted for each action.

Events do not need to be escalated unless they turn into incidents and generate an alarm.

Objective:
Information Security Incident Management

Sub-Objective:
Establish and maintain incident notification and escalation processes to ensure that the appropriate stakeholders are involved in incident response management.

References:

CISM Review Manual, 15th Edition, Chapter 4: Information Security Incident Management, 4.9 Developing an Incident Response Plan, 4.9.4 Escalation Process for Effective Incident Management

---

Question #150 of 150

Question ID: 1185742

What is the most important reason for establishing and maintaining information security policies?

- **A)** To avoid legal and regulatory non-compliance issues
- **B) To support the business goals of the organization**
- **C)** To obtain metrics about the performance of the security program
- **D)** To educate all users about their responsibility to keep assets secure

Explanation

The most important reason for establishing and maintain information security policies is to support the organization’s business goals. The information security policies must be designed to support the overall information security strategy, which in turn must support the business goals. Senior management will not support a program that does not support the business goals.

Obtaining metrics is one way to ensure or verify that the security policies support business goals, but it is not its most important purpose.

User education is important, but is also just one aspect to supporting business goals.

Avoiding legal and regulatory non-compliance is not the most important reason for establishing and maintaining information security policies. Rather, complying with laws and regulations is one of the ways that the security policies support the business goals.

Objective:
Information Security Governance

Sub-Objective:
Identify internal and external influences to the organization to ensure that these factors are continually addressed by the information security strategy.

References:

CISM Review Manual, 15th Edition, Chapter 1: Information Security Governance, 1.2 Effective Information Security Governance, 1.2.1 Business Goals and Objectives