Updated Feb 15, 2023 CISM Exam Dumps - PDF Questions and Testing Engine [Q180-Q202

Updated Feb 15, 2023 CISM Exam Dumps - PDF Questions and Testing Engine
New (2023) ISACA CISM Exam Dumps

NO.180 An internal audit has found that critical patches were not implemented within the timeline established by policy without a valid reason. Which of the following is the BEST course of action to address the audit findings?
* Evaluate patch management training.
* Monitor and notify IT staff of critical patches
* Perform regular audits on the implementation of critical patches.
* Assess the patch management process

NO.181 Which of the following situations must be corrected FIRST to ensure successful information security governance within an organization?
* The information security department has difficulty filling vacancies.
* The chief information officer (CIO) approves security policy changes.
* The information security oversight committee only meets quarterly.
* The data center manager has final signoff on all security projects.
Section: INFORMATION SECURITY GOVERNANCE

Explanation:

A steering committee should be in place to approve all security projects. The fact that the data center manager has final signoff for all security projects indicates that a steering committee is not being used and that information security is relegated to a subordinate place in the organization. This would indicate a failure of information security governance. It is not inappropriate for an oversight or steering committee to meet quarterly. Similarly, it may be desirable to have the chief information officer (CIO) approve the security policy due to the size of the organization and frequency of updates. Difficulty in filling vacancies is not uncommon due to the shortage of good, qualified information security professionals.

NO.182 An organization has acquired a company in a foreign country to gain an advantage in a new market Which of the following is the FIRST step the information security manager should take?

- Apply the existing information security program to the acquired company
- Evaluate the information security laws that apply to the acquired company
- Merge the two existing information security programs
- Determine which country&#8217;s information security regulations will be used

NO.183 After an information security business case has been approved by senior management, it should be:

- used to design functional requirements for the solution.
- used as the foundation for a risk assessment.
- referenced to build architectural blueprints for the solution.
- reviewed at key intervals to ensure intended outcomes.

Section: INFORMATION SECURITY PROGRAM MANAGEMENT

NO.184 Which of the following is the MOST likely to change an organization&#8217;s culture to one that is more security conscious?

- Adequate security policies and procedures
- Periodic compliance reviews
- Security steering committees
- Security awareness campaigns

Explanation/Reference:

Explanation:

Security awareness campaigns will be more effective at changing an organizational culture than the creation of steering committees and security policies and procedures. Compliance reviews are helpful; however, awareness by all staff is more effective because compliance reviews are focused on certain areas groups and do not necessarily educate.

NO.185 When designing an information security quarterly report to management, the MOST important element to be considered should be the:

- information security metrics.
- knowledge required to analyze each issue.
- linkage to business area objectives.
- baseline against which metrics are evaluated.

Explanation

The link to business objectives is the most important clement that would be considered by management.

Information security metrics should be put in the context of impact to management objectives. Although important, the security knowledge required would not be the first element to be considered. Baselining against the information security metrics will be considered later in the process.

NO.186 What is the MOST important item to be included in an information security policy?
* The definition of roles and responsibilities
* The scope of the security program
* The key objectives of the security program
* Reference to procedures and standards of the security program

Stating the objectives of the security program is the most important element to ensure alignment with business goals. The other choices are part of the security policy, but they are not as important.

NO.187 The systems administrator did not immediately notify the security officer about a malicious attack. An information security manager could prevent this situation by:
* periodically testing the incident response plans.
* regularly testing the intrusion detection system (IDS).
* establishing mandatory training of all personnel.
* periodically reviewing incident response procedures.

Section: INFORMATION RISK MANAGEMENT

Explanation:

Security incident response plans should be tested to find any deficiencies and improve existing processes.

Testing the intrusion detection system (IDS) is a good practice but would not have prevented this situation.

All personnel need to go through formal training to ensure that they understand the process, tools and methodology involved in handling security incidents. However, testing of the actual plans is more effective in ensuring the process works as intended.
Reviewing the response procedures is not enough; the security response plan needs to be tested on a regular basis.

NO.188 What should be an information security manager&#8217;s FIRST course of action when an organization is subject to a new regulatory requirement?
* Submit a business case to support compliance.
* Perform a gap analysis,
* Complete a control assessment.
* Update the risk register.

NO.189 The FIRST step in developing an information security management program is to:
* identify business risks that affect the organization.
* clarify organizational purpose for creating the program.
* assign responsibility for the program.
* assess adequacy of controls to mitigate business risks.

Section: INFORMATION SECURITY GOVERNANCE

Explanation:

In developing an information security management program, the first step is to clarify the organization&#8217;s purpose for creating the program. This is a business decision based more on judgment than on any specific quantitative measures. After clarifying the purpose, the other choices are assigned and acted upon.

NO.190 Which of the following would BEST address the risk of data leakage?
* File backup procedures

- Database integrity checks
- Acceptable use policies
- Incident response procedures

Acceptable use policies are the best measure for preventing the unauthorized disclosure of confidential information. The other choices do not address confidentiality of information.

NO.191 A risk assessment should be conducted:

- once a year for each business process and subprocess.
- every three to six months for critical business processes.
- by external parties to maintain objectivity.
- annually or whenever there is a significant change.

Section: INFORMATION RISK MANAGEMENT

Explanation:

Risks are constantly changing. Choice D offers the best alternative because it takes into consideration a reasonable time frame and allows flexibility to address significant change. Conducting a risk assessment once a year is insufficient if important changes take place. Conducting a risk assessment every three-to-six months for critical processes may not be necessary, or it may not address important changes in a timely manner. It is not necessary for assessments to be performed by external parties.

NO.192 Authorization can BEST be accomplished by establishing:

- whether users are who they say they are
- who users can do when they are granted system access.
- how users identify themselves to information systems.
- the ownership of the data

NO.193 Which of the following would be the BEST option to improve accountability for a system administrator who has security functions?

- Include security responsibilities in the job description
- Require the administrator to obtain security certification
- Train the system administrator on penetration testing and vulnerability assessment
- Train the system administrator on risk assessment

Explanation/Reference:

Explanation:

The first step to improve accountability is to include security responsibilities in a job description. This documents what is expected and approved by the organization. The other choices are methods to ensure that the system administrator has the training to fulfill the responsibilities included in the job description.

NO.194 An organization utilizes a third party to classify its customers&#8217; personally identifiable information (PII). What is the BEST way to hold the third party accountable for data leaks?

- Include detailed documentation requirements within the formal statement of work.
- Submit a formal request for proposal (RFP) containing detailed documentation of requirements.
- Ensure a nondisclosure agreement is signed by both parties&#8217; senior management.
- Require the service provider to sign off on the organization&#8217;s acceptable use policy.

NO.195 Information classification is a fundamental step in determining:

- whether risk analysis objectives are met.
- who has ownership of information.

* the type of metrics that should be captured.
* the security strategy that should be used.
Section: INCIDENT MANAGEMENT AND RESPONSE

NO.196 When performing a business impact analysis (BIA), which of the following should calculate the recovery time and cost estimates?
* Business continuity coordinator
* Information security manager
* Business process owners
* Industry averages benchmarks
Section: INCIDENT MANAGEMENT AND RESPONSE

Explanation:

Business process owners are in the best position to understand the true impact on the business that a system outage would create. The business continuity coordinator, industry averages and even information security will not be able to provide that level of detailed knowledge.

NO.197 Which of the following is the BEST way to improve the timely reporting of information security incidents?
* Perform periodic simulations with the incident response team.
* Regularly reassess and update the incident response plan.
* Integrate an intrusion detection system (IDS) in the DMZ
* Incorporate security procedures in help desk processes

NO.198 After a risk assessment study, a bank with global operations decided to continue doing business in certain regions of the world where identity theft is rampant. The information security manager should encourage the business to:
* increase its customer awareness efforts in those regions.
* implement monitoring techniques to detect and react to potential fraud.
* outsource credit card processing to a third party.
* make the customer liable for losses if they fail to follow the bank&#8217;s advice.
Explanation/Reference:

Explanation:

While customer awareness will help mitigate the risks, this is insufficient on its own to control fraud risk.

Implementing monitoring techniques which will detect and deal with potential fraud cases is the most effective way to deal with this risk. If the bank outsources its processing, the bank still retains liability. While making the customer liable for losses is a possible approach, nevertheless, the bank needs to be seen to be proactive in managing its risks.

NO.199 Following a significant change to the underlying code of an application, it is MOST important for the information security manager to:
* inform senior management
* update the risk assessment
* validate the user acceptance testing
* modify key risk indicators

NO.200 An information security manager at a global organization that is subject to regulation by multiple governmental jurisdictions with differing requirements should:
* bring all locations into conformity with the aggregate requirements of all governmental jurisdictions.

* establish baseline standards for all locations and add supplemental standards as required.
* bring all locations into conformity with a generally accepted set of industry best practices.
* establish a baseline standard incorporating those requirements that all jurisdictions have in common.

It is more efficient to establish a baseline standard and then develop additional standards for locations that must meet specific requirements. Seeking a lowest common denominator or just using industry best practices may cause certain locations to fail regulatory compliance. The opposite approach-forcing all locations to be in compliance with the regulations places an undue burden on those locations.

NO.201 Data owners must provide a safe and secure environment to ensure confidentiality, integrity and availability of the transaction. This is an example of an information security:

* baseline.
* strategy.
* procedure.
* policy.

Explanation/Reference:

Explanation:

A policy is a high-level statement of an organization&#8217;s beliefs, goals, roles and objectives. Baselines assume a minimum security level throughout an organization. The information security strategy aligns the information security program with business objectives rather than making control statements. A procedure is a step-by-step process of how policy and standards will be implemented.

NO.202 To mitigate a situation where one of the programmers of an application requires access to production data, the information security manager could BEST recommend to.

* create a separate account for the programmer as a power user.
* log all of the programmers&#8217; activity for review by supervisor.
* have the programmer sign a letter accepting full responsibility.
* perform regular audits of the application.

Explanation/Reference:

Explanation:

It is not always possible to provide adequate segregation of duties between programming and operations in order to meet certain business requirements. A mitigating control is to record all of the programmers&#8217; actions for later review by their supervisor, which would reduce the likelihood of any inappropriate action on the part of the programmer. Choices A, C and D do not solve the problem.

3. Information Security Program Development and Management ? 27% **The next area that you should learn will evaluate your knowledge base whether it contains the following or not:** - Knowledge and ability to implement the proper effectiveness and procedures of information security along with its policies;- Knowledge of the certifications, training, and

skills required for information security;- Knowledge and skills in managing, identifying, and defining the necessary requirements for internal and external resources;- Knowledge and skills in implementing the rules into contracts, agreements, and third-party management processes;- Knowledge of the techniques to communicate this program to the stakeholders.