Q QUESTIONS

[**1**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa1)**.**   Which of the following best describes information security governance?

**A.**   Information security policies.

**B.**   Information security policies along with audits of those policies.

**C.**   Management’s control of information security processes.

**D.**   Benchmarks of metrics as compared to similar organizations.

[**2**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa2)**.**   What is the best method for ensuring that an organization’s security program achieves adequate business alignment?

**A.**   Find and read the organization’s articles of incorporation.

**B.**   Understand the organization’s vision, mission statement, and objectives.

**C.**   Study the organization’s chart of management reporting (the “org chart”).

**D.**   Study the organization’s financial chart of accounts.

[**3**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa3)**.**   Robert has located his organization’s mission statement and a list of strategic objectives. What steps should Robert take to ensure that the information security program aligns with the business?

**A.**   Discuss strategic objectives with business leaders to understand better what they want to accomplish and what steps are being taken to achieve them.

**B.**   Develop a list of activities that will support the organization’s strategic objectives, and determine the cost of each.

**C.**   Select those controls from the organization’s control framework that align to each objective, and then ensure that those controls are effective.

**D.**   Select the policies from the organization’s information security policy that are relevant to each objective, and ensure that those policies are current.

[**4**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa4)**.**   Michael wants to improve the risk management process in his organization by creating guidelines that will help management understand when certain risks should be accepted and when certain risks should be mitigated. The policy that Michael needs to create is known as what?

**A.**   Security policy

**B.**   Control framework

**C.**   Risk appetite statement

**D.**   Control testing procedure

[**5**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa5)**.**   In a risk management process, who is the best person(s) to make a risk treatment decision?

**A.**   Chief risk officer (CRO)

**B.**   Chief information officer (CIO)

**C.**   Process owner who is associated with the risk

**D.**   Chief information security officer (CISO)

[**6**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa6)**.**   The ultimate responsibility for an organization’s cybersecurity program lies with whom?

**A.**   The board of directors

**B.**   The chief executive officer (CEO)

**C.**   The chief information officer (CIO)

**D.**   The chief information security officer (CISO)

[**7**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa7)**.**   In a U.S. public company, a CISO will generally report the state of the organization’s cybersecurity program to:

**A.**   The Treadway Commission

**B.**   Independent auditors

**C.**   The U.S. Securities and Exchange Commission

**D.**   The audit committee of the board of directors

[**8**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa8)**.**   A new CISO in an organization is building its cybersecurity program from the ground up. To ensure collaboration among business leaders and department heads in the organization, the CISO should form and manage which of the following?

**A.**   A risk committee of the board of directors

**B.**   A cybersecurity steering committee

**C.**   An audit committee of the board of directors

**D.**   Business-aligned security policy

[**9**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa9)**.**   Who is the best person or group to make cyber-risk treatment decisions?

**A.**   The chief information security officer (CISO)

**B.**   The audit committee of the board of directors

**C.**   The cybersecurity steering committee

**D.**   The chief risk officer (CRO)

[**10**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa10)**.**   Which is the best party to conduct access reviews?

**A.**   Users’ managers

**B.**   Information security manager

**C.**   IT service desk

**D.**   Department head

[**11**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa11)**.**   Which is the best party to make decisions about the purpose and function of business applications?

**A.**   Business department head

**B.**   IT business analyst

**C.**   Application developer

**D.**   End user

[**12**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa12)**.**   Which of the following is the best definition of custodial responsibility?

**A.**   Custodian protects assets based on customer’s defined interests

**B.**   Custodian protects assets based on its own defined interests

**C.**   Custodian makes decisions based on its own defined interests

**D.**   Custodian makes decisions based on customer’s defined interests

[**13**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa13)**.**   What is the primary risk of IT acting as custodian for a business owner?

**A.**   IT may not have enough interest to provide quality care for business applications.

**B.**   IT may not have sufficient staffing to care for business applications properly.

**C.**   IT may have insufficient knowledge of business operations to make good decisions.

**D.**   Business departments might not give IT sufficient access to manage applications properly.

[**14**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa14)**.**   An organization needs to hire an executive who will build a management program that will consider threats and vulnerabilities and determine controls needed to protect systems and work centers. What is the best job title for this position?

**A.**   CSO

**B.**   CRO

**C.**   CISO

**D.**   CIRO

[**15**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa15)**.**   An organization needs to hire an executive who will be responsible for ensuring that the organization’s policies, business processes, and information systems are compliant with laws and regulations concerning the proper collection, use, and protection of personally identifiable information. What is the best job title for the organization to use for this position?

**A.**   CSO

**B.**   CIRO

**C.**   CISO

**D.**   CPO

[**16**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa16)**.**   The Big Data Company is adjusting several position titles in its IT department to reflect industry standards. Included in consideration are two individuals: The first is responsible for the overall relationships and data flows among its internal and external information systems. The second is responsible for the overall health and management of systems containing information. Which two job titles are most appropriate for these two roles?

**A.**   Systems architect and database administrator

**B.**   Data architect and data scientist

**C.**   Data scientist and database administrator

**D.**   Data architect and database administrator

[**17**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa17)**.**   What is the primary distinction between a network engineer and a telecom engineer?

**A.**   A network engineer is primarily involved with networks and internal network media, while a telecom engineer is primarily involved with networks and external (carrier) network media.

**B.**   A network engineer is primarily involved with networks and external (carrier) network media, while a telecom engineer is primarily involved with networks and internal network media.

**C.**   A network engineer is primarily involved with layer 3 protocols and above, while a telecom engineer is primarily involved with layer 1 and layer 2 protocols.

**D.**   There is no distinction, as both are involved in all aspects of an organization’s networks.

[**18**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa18)**.**   An organization that is a U.S. public company is redesigning its access management and access review controls. What is the best role for internal audit in this redesign effort?

**A.**   Develop procedures

**B.**   Design controls

**C.**   Provide feedback on control design

**D.**   Develop controls and procedures

[**19**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa19)**.**   A security operations manager is proposing that engineers who design and manage information systems play a role in monitoring those systems. Is design and management compatible with monitoring? Why or why not?

**A.**   Personnel who design and manage systems should not perform a monitoring role because this is a conflict of interest.

**B.**   Personnel who design and manage systems will be more familiar with the reasons and steps to take when alerts are generated.

**C.**   Personnel who design and manage systems will not be familiar with response procedures when alerts are generated.

**D.**   Personnel who design and manage systems are not permitted access to production environments and should not perform monitoring.

[**20**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa20)**.**   What is the purpose of metrics in an information security program?

**A.**   To measure the performance and effectiveness of security controls

**B.**   To measure the likelihood of an attack on the organization

**C.**   To predict the likelihood of an attack on an organization

**D.**   To predict the method of an attack on an organization

[**21**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa21)**.**   Which security metric is best considered a leading indicator of an attack?

**A.**   Number of firewall rules triggered

**B.**   Number of security awareness training sessions completed

**C.**   Percentage of systems scanned

**D.**   Mean time to apply security patches

[**22**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa22)**.**   Steve, a CISO, has vulnerability management metrics and needs to build business-level metrics. Which of the following is the best leading indicator metric suitable for his organization’s board of directors?

**A.**   Average time to patch servers supporting manufacturing processes

**B.**   Frequency of security scans of servers supporting manufacturing processes

**C.**   Percentage of servers supporting manufacturing processes that are scanned by vulnerability scanning tools

**D.**   Number of vulnerabilities remediated on servers supporting manufacturing processes

[**23**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa23)**.**   The metric “percentage of systems with completed installation of advanced antimalware” is best described as what?

**A.**   Key operational indicator (KOI)

**B.**   Key performance indicator (KPI)

**C.**   Key goal indicator (KGI)

**D.**   Key risk indicator (KRI)

[**24**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa24)**.**   A member of the board of directors has asked Ravila, a CIRO, to produce a metric showing the reduction of risk as a result of the organization making key improvements to its security information and event management system. Which type of metric is most suitable for this purpose?

**A.**   KGI

**B.**   RACI

**C.**   KRI

**D.**   ROSI

[**25**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa25)**.**   A common way to determine the effectiveness of security and risk metrics is the SMART method. What does SMART stand for?

**A.**   Security Metrics Are Risk Treatment

**B.**   Specific, Measurable, Attainable, Relevant, Timely

**C.**   Specific, Measurable, Actionable, Relevant, Timely

**D.**   Specific, Manageable, Actionable, Relevant, Timely

[**26**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa26)**.**   The statement “Complete migration of flagship system to latest version of vendor-supplied software” is an example of what?

**A.**   Mission statement

**B.**   Vision statement

**C.**   Purpose statement

**D.**   Objective statement

[**27**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa27)**.**   Ernie, a CISO who manages a large security group, wants to create a mission statement for the CISO group. What is the best approach for creating this mission statement?

**A.**   Start with the organization’s mission statement.

**B.**   Start with Ernie’s most recent performance review.

**C.**   Start with the results of the most recent risk assessment.

**D.**   Start with the body of open items in the risk register.

[**28**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa28)**.**   Which of the following statements is the best description for the purpose of performing risk management?

**A.**   Identify and manage vulnerabilities that may permit security events to occur.

**B.**   Identify and address threats that are relevant to the organization.

**C.**   Assess the risks associated with third-party service providers.

**D.**   Assess and manage risks associated with doing business online.

[**29**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa29)**.**   Key metrics showing effectiveness of a risk management program would *not* include which of the following?

**A.**   Reduction in the number of security events

**B.**   Reduction in the impact of security events

**C.**   Reduction in the time to remediate vulnerabilities

**D.**   Reduction in the number of patches applied

[**30**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa30)**.**   Examples of security program performance include all of the following *except*:

**A.**   Time to detect security incidents

**B.**   Time to remediate security incidents

**C.**   Time to perform security scans

**D.**   Time to discover vulnerabilities

[**31**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa31)**.**   Two similar-sized organizations are merging. Paul will be the CISO of the new combined organization. What is the greatest risk that may occur as a result of the merger?

**A.**   Differences in practices that may not be understood

**B.**   Duplication of effort

**C.**   Gaps in coverage of key processes

**D.**   Higher tooling costs

[**32**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa32)**.**   What is the purpose of value delivery metrics?

**A.**   Long-term reduction in costs

**B.**   Reduction in ROSI

**C.**   Increase in ROSI

**D.**   Increase in net profit

[**33**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa33)**.**   Joseph, a CISO, is collecting statistics on several operational areas and needs to find a standard way of measuring and publishing information about the effectiveness of his program. Which of the following is the best approach to follow?

**A.**   Scaled Score

**B.**   NIST Cybersecurity Framework (CSF)

**C.**   Business Model for Information Security (BMIS)

**D.**   Balanced Scorecard (BSC)

[**34**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa34)**.**   Which of the following is the best description of the Business Model for Information Security (BMIS)?

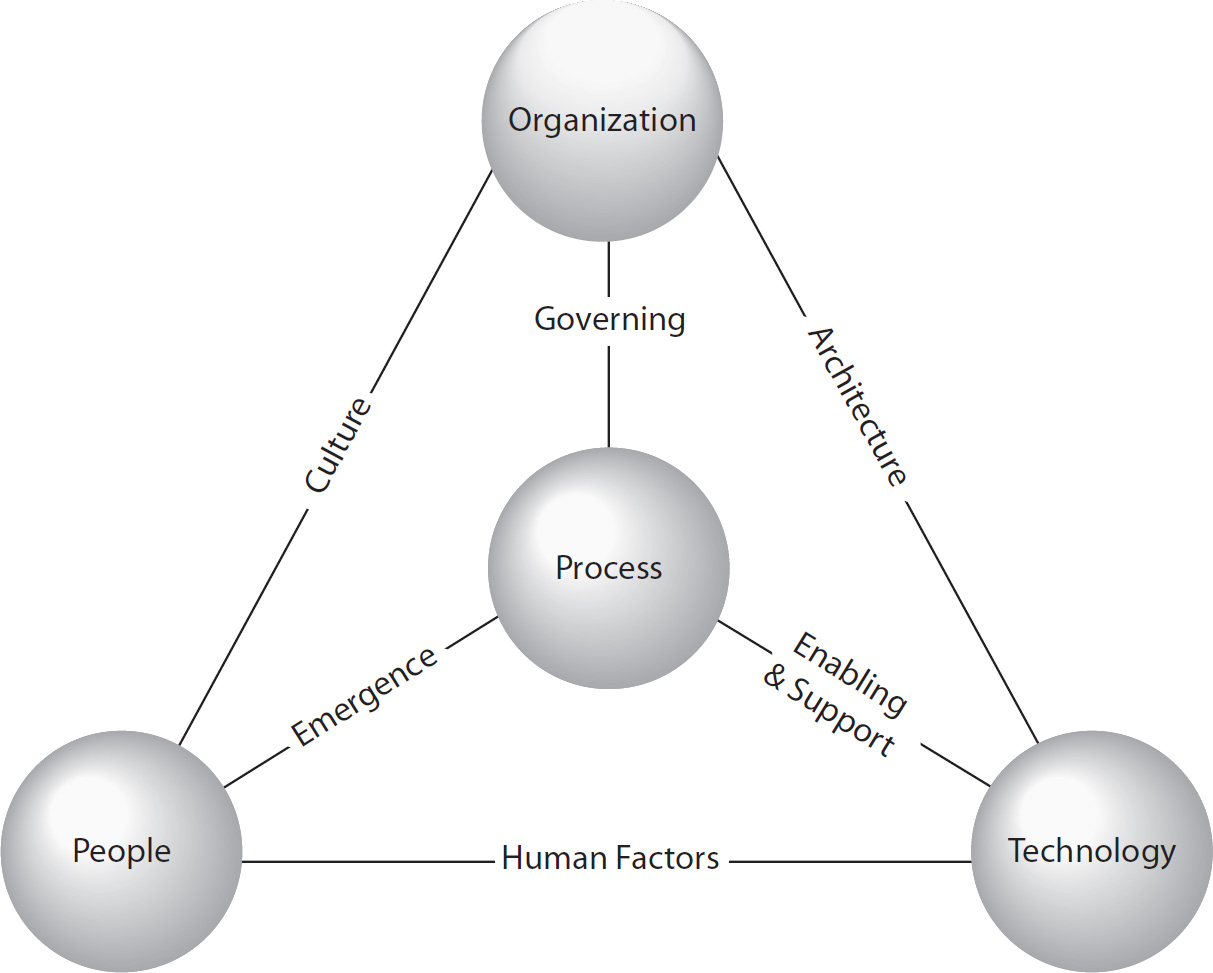
**A.**   It describes the relationships (as dynamic interconnections) between policy, people, process, and technology.

**B.**   It describes the relationships (as dynamic interconnections) between people, process, technology, and the organization.

**C.**   It describes the primary elements (people, process, and technology) in an organization.

**D.**   It describes the dynamic interconnections (people, process, and technology) in an organization.

[**35**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa35)**.**   What is the correct name for the following illustration?



**A.**   COBIT Model for Information Technology

**B.**   COBIT Model for Information Security

**C.**   Business Model for Information Security

**D.**   Business Model for Information Technology

[**36**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa36)**.**   Jacqueline, an experienced CISO, is reading the findings in a recent risk assessment that describes deficiencies in the organization’s vulnerability management process. How would Jacqueline use the Business Model for Information Security (BMIS) to analyze the deficiency?

**A.**   Identify the elements connected to the process DI.

**B.**   Identify the dynamic interconnections (DIs) connected to the process element.

**C.**   Identify the dynamic elements connected to human factors.

**D.**   Identify the dynamic elements connected to technology.

[**37**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa37)**.**   Which of the following would constitute an appropriate use of the Zachman enterprise framework?

**A.**   An IT service management model as an alternative to ITIL

**B.**   Identifying system components, followed by high-level design and business functions

**C.**   Development of business requirements, translated top-down into technical architecture

**D.**   IT systems described at a high level and then in increasing levels of detail

[**38**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa38)**.**   An IT architect needs to document the flow of data from one system to another, including external systems operated by third-party service providers. What kind of documentation does the IT architect need to develop?

**A.**   Data flow diagrams (DFDs)

**B.**   Entity relationship diagrams (EFDs)

**C.**   A Zachman architecture framework

**D.**   Visio diagrams showing information systems and data flows

[**39**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa39)**.**   Carole is a CISO in a new organization with a fledgling security program. Carole needs to identify and develop mechanisms to ensure desired outcomes in selected business processes. What is a common term used to define these mechanisms?

**A.**   Checkpoints

**B.**   Detective controls

**C.**   Controls

**D.**   Preventive controls

[**40**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa40)**.**   What is the best approach to developing security controls in a new organization?

**A.**   Start with a standard control framework and make risk-based adjustments as needed.

**B.**   Start from scratch and develop controls based on risk as needed.

**C.**   Start with NIST CSF and move up to ISO 27001, and then NIST 800-53 as the organization matures.

**D.**   Develop controls in response to an initial risk assessment.

[**41**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa41)**.**   Which of the following is the best description of the COBIT framework?

**A.**   A security process and controls framework that can be integrated with ITIL or ISO 20000

**B.**   An IT controls and process framework on which IT controls and processes can be added at an organization’s discretion

**C.**   An IT process framework with optional security processes when Extended COBIT is implemented

**D.**   An IT process framework that includes security processes that are interspersed throughout the framework

[**42**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa42)**.**   Name one distinct disadvantage of the ISO 27001 standard.

**A.**   The standard is costly (more than 100 U.S. dollars per copy).

**B.**   The standard is costly (a few thousand U.S. dollars per copy).

**C.**   The standard is available only for use in the United States.

**D.**   The standard is suitable only in large organizations.

[**43**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa43)**.**   Which of the following statements about ISO 27001 is correct?

**A.**   ISO 27001 consists primarily of a framework of security controls, followed by an appendix of security requirements for running a security management program.

**B.**   ISO 27001 consists primarily of a body of requirements for running a security management program, along with an appendix of security controls.

**C.**   ISO 27001 consists of a framework of information security controls.

**D.**   ISO 27001 consists of a framework of requirements for running a security management program.

[**44**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa44)**.**   What U.S. law regulates the protection of medical care–related data?

**A.**   PIPEDA

**B.**   HIPAA

**C.**   GLBA

**D.**   GDPR

[**45**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa45)**.**   The regulation “Security and Privacy Controls for Federal Information Systems and Organizations” is better known as what?

**A.**   ISO/IEC 27001

**B.**   ISO/IEC 27002

**C.**   NIST CSF

**D.**   NIST SP800-53

[**46**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa46)**.**   What is the best explanation for the Implementation Tiers in the NIST Cybersecurity Framework?

**A.**   Implementation Tiers are levels of risk as determined by the organization.

**B.**   Implementation Tiers are stages of implementation of controls in the framework.

**C.**   Implementation Tiers are likened to maturity levels.

**D.**   Implementation Tiers are levels of risk as determined by an external auditor or regulator.

[**47**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa47)**.**   Jeffrey is a CISO in an organization that performs financial services for private organizations as well as government agencies and U.S. federal agencies. Which is the best information security controls framework for this organization?

**A.**   CIS

**B.**   ISO 27001

**C.**   NIST CSF

**D.**   NIST-800-53

[**48**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa48)**.**   What is the scope of requirements of PCI-DSS?

**A.**   All systems that store, process, and transmit credit card numbers, as well as all other systems that can communicate with these systems

**B.**   All systems that store, process, and transmit credit card numbers

**C.**   All systems that store, process, and transmit unencrypted credit card numbers

**D.**   All systems in an organization where credit card numbers are stored, processed, and transmitted

[**49**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa49)**.**   Which of the following statements is true about controls in the Payment Card Industry Data Security Standard?

**A.**   Many controls are required, while some are “addressable,” or optional, based on risk.

**B.**   All controls are required, regardless of actual risk.

**C.**   Controls that are required are determined for each organization by the acquiring bank.

**D.**   In addition to core controls, each credit card brand has its own unique controls.

[**50**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa50)**.**   The PCI-DSS is an example of what?

**A.**   An industry regulation that is enforced with fines

**B.**   A private industry standard that is enforced with contracts

**C.**   A voluntary standard that, if used, can reduce cyber insurance premiums

**D.**   An international law enforced through treaties with member nations

[**51**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa51)**.**   What are three factors that a risk manager may consider when developing an information security strategy?

**A.**   Threats, risks, and solutions

**B.**   Prevention, detection, and response

**C.**   Risk levels, staff qualifications, and security tooling

**D.**   Risk levels, operating costs, and compliance levels

[**52**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa52)**.**   Jerome, a new CISO in a SaaS organization, has been asked to develop a long-term information security strategy. Which is the best first step for understanding the present state of the organization’s existing information security program?

**A.**   Perform a code review of the organization’s SaaS offerings.

**B.**   Study the contents of the risk register.

**C.**   Perform a baseline risk assessment.

**D.**   Commission a penetration test of internal and external networks.

[**53**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa53)**.**   Jerome, a new CISO in a SaaS organization, has been asked to develop a long-term information security strategy. Why would Jerome choose to perform a threat assessment prior to producing the strategy?

**A.**   Ensure that the organization is aware of everything that could reasonably go wrong.

**B.**   Ensure that preventive controls are effective.

**C.**   Ensure that there are no unidentified vulnerabilities.

**D.**   Ensure that there are no unidentified risks.

[**54**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa54)**.**   Jerome, a new CISO in a SaaS organization, has been asked to develop a long-term information security strategy. While examining the organization’s information security policy, and together with knowledge of the organization’s practices and controls, Jerome now realizes that the organization’s security policy is largely aspirational. What is the most important consequence of this on the organization?

**A.**   Confusion on the part of end users

**B.**   Appearance that the organization is not in control of its security practices

**C.**   Fines and sanctions from regulators

**D.**   Unmitigated risks and vulnerabilities

[**55**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa55)**.**   Jerome, a new CISO in a SaaS organization, has been asked to develop a long-term information security strategy. While examining the organization’s information security policy, and together with knowledge of the organization’s practices and controls, Jerome now realizes that the organization’s security policy is largely aspirational. What is the best first step Jerome should take next?

**A.**   Create an entry in the organization’s risk register.

**B.**   Withdraw the security policy and write a new one that’s closer to reality.

**C.**   Perform a gap analysis and determine actions to take to close the policy gaps.

**D.**   Consult with the organization’s general counsel to develop a plan of action.

[**56**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa56)**.**   Jerome, a new CISO in a SaaS organization, has identified a document that describes acceptable encryption protocols. What type of document is this?

**A.**   Policy

**B.**   Standard

**C.**   Practice

**D.**   Guideline

[**57**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa57)**.**   Jerome, a new CISO in a SaaS organization, has identified a document that describes suggested techniques for implementing encryption protocols. What type of document is this?

**A.**   Policy

**B.**   Standard

**C.**   Guideline

**D.**   Procedure

[**58**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa58)**.**   An organization is required by PCI to include several policies that are highly technical and not applicable to the majority of its employees. What is the best course of action for implementing these policies?

**A.**   Implement a technical security policy containing these required items, with a separate acceptable use policy for all workers.

**B.**   Incorporate all PCI-required policies in the organization’s information policy and let users figure out what is relevant to them.

**C.**   Include all PCI-related policies and indicate which are applicable to end users.

**D.**   Keep the PCI-related policies out of the overall security policy because it will confuse nontechnical end users.

[**59**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa59)**.**   Which of the following is the most likely result of an organization that lacks a security architecture function?

**A.**   Inconsistent security-related procedures

**B.**   Inconsistent application of standards

**C.**   Lower process maturity

**D.**   Added complication in vulnerability management tools

[**60**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa60)**.**   What is the main advantage of a security architecture function in a larger, distributed organization?

**A.**   Greater employee satisfaction

**B.**   Better results in vulnerability assessments

**C.**   Greater consistency in the use of tools and configurations

**D.**   Lower cost of operations

[**61**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa61)**.**   Which of the following statements about control frameworks is correct?

**A.**   Control frameworks are used only in regulated environments.

**B.**   All control frameworks are essentially the same, with different controls groups.

**C.**   It doesn’t matter which control framework is selected, as long as controls are operated effectively.

**D.**   Different control frameworks are associated with different industries.

[**62**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa62)**.**   Joel, a new CISO in an organization, has discovered that the server team applies security patches in response to the quarterly vulnerability scan reports created by the security team. What is the best process improvement Joel can introduce to this process?

**A.**   Server team proactively applies patches, and security scans confirm effective patching

**B.**   Server team proactively applies patches, and security scans confirm effective patching and identify other issues

**C.**   Security team increases the frequency of vulnerability scans from quarterly to monthly for internal scans and weekly for external scans

**D.**   Security team increases the frequency of vulnerability scans from quarterly to monthly

[**63**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa63)**.**   Which of the following is the best management-level metric for a vulnerability management process?

**A.**   Average time from availability of a patch to the successful application of a patch

**B.**   Average time from a vulnerability scan to the successful application of a patch

**C.**   Average time to apply a security patch successfully

**D.**   Number of security patches applied

[**64**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa64)**.**   A new CISO in a manufacturing company is gathering artifacts to understand the state of security in the organization. Which of the following would be the *least* valuable for determining risk posture?

**A.**   Security incident log

**B.**   Security awareness training records

**C.**   Penetration test results

**D.**   Report to the board of directors

[**65**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa65)**.**   Of what value is a business impact analysis (BIA) for a security leader in an organization?

**A.**   It provides a view of the criticality of IT systems in an organization.

**B.**   It provides a view of the criticality of business processes in an organization.

**C.**   It provides a view of the criticality of software applications in an organization.

**D.**   It provides no value to a security leader because it focuses on business continuity, not security.

[**66**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa66)**.**   Samuel is the CISO in an organization that is a U.S. public company. Samuel has noted that the organization’s internal audit function concentrates its auditing efforts on “financially relevant” applications and underlying IT systems and infrastructure. As an experienced CISO, what conclusion can Samuel draw from this?

**A.**   The audits performed by internal audit on underlying IT systems and infrastructure are value-added activities.

**B.**   Internal audit’s scope is too narrow and must include all applications and IT systems.

**C.**   The scope of internal audit is of no consequence or value to the CISO.

**D.**   The scope of internal audit’s auditing activities is as expected for a U.S. public company.

[**67**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa67)**.**   Of what value is a third-party risk management (TPRM) process for a CISO who is developing a long-term security strategy for an organization?

**A.**   TPRM provides valuable insight into the security capabilities of critical service providers.

**B.**   TPRM provides valuable insight into the organization’s procurement process.

**C.**   TPRM provides a list of all service providers used by the organization.

**D.**   TPRM does not provide value to the CISO because it is concerned only with business processes.

[**68**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa68)**.**   Joseph, a new security leader in an online retail organization, is developing a long-term security strategy. Joseph has developed a detailed description of the future state of the security organization. What must Joseph do before developing a strategy to realize the future state?

**A.**   Perform an audit of existing security controls to understand their effectiveness.

**B.**   Understand the current state and perform a gap analysis to identify the differences.

**C.**   Perform a risk assessment to identify potential pitfalls in the strategy.

**D.**   Commission a penetration test to identify unknown vulnerabilities in critical systems.

[**69**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa69)**.**   Joseph, a new security leader in an online retail organization, is developing a long-term security strategy. In his research, Joseph is seeking documents describing the current security program. Which of the following documents would *not* provide the best value in this analysis?

**A.**   Security program charter

**B.**   Security team job descriptions

**C.**   Information security policy

**D.**   Meeting minutes for the cybersecurity steering committee

[**70**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa70)**.**   Quincy is a security leader who wants to formalize information security in his organization. What is the best first step to formalizing the program?

**A.**   Start an information security intranet site.

**B.**   Start an information security newsletter.

**C.**   Develop an information security policy.

**D.**   Develop an information security program charter.

[**71**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa71)**.**   Ravila, a security leader, has assessed the maturity of the information security capabilities in the organization using the CMMI model. The average maturity of business processes in the organization is 3.2. What should Ravila do next?

**A.**   Compare the current maturity levels to desired maturity levels and develop a strategy to achieve desired levels.

**B.**   Determine the steps necessary to raise process maturity to 5.

**C.**   Identify the processes with the lowest maturity and develop a strategy to raise them to the level of other processes.

**D.**   Perform a root cause analysis (RCA) to determine why business process maturity has fallen to this level.

[**72**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa72)**.**   An organization’s security leader, together with members of its information security steering committee, has decided to require that all encryption of data at rest must use AES-256 or better encryption. The organization needs to update what document?

**A.**   Policies

**B.**   Standards

**C.**   Guidelines

**D.**   Systems

[**73**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa73)**.**   A security leader has been asked to justify the need to implement a new strategy for information security. How should the security leader respond?

**A.**   Develop a project plan showing the personnel, tasks, timelines, and dependencies.

**B.**   Develop a risk matrix that includes the potential consequences if the strategy is not implemented.

**C.**   Develop a SWOT diagram showing strengths, weaknesses, opportunities, and threats.

**D.**   Develop a business case that includes success criteria, requirements, costs, and action plan.

[**74**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2sa74)**.**   What is the purpose of obtaining management commitment in support of a strategy?

**A.**   Improved enforcement of policy

**B.**   Approval for new hires

**C.**   Visible support to reinforce the importance of the strategy

**D.**   Approval of spending

QUICK ANSWER KEY

|  |  |  |  |
| --- | --- | --- | --- |
| [**1**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa1)**.**   C  [**2**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa2)**.**   B  [**3**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa3)**.**   A  [**4**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa4)**.**   C  [**5**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa5)**.**   C  [**6**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa6)**.**   A  [**7**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa7)**.**   D  [**8**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa8)**.**   B  [**9**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa9)**.**   C  [**10**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa10)**.**   D  [**11**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa11)**.**   A  [**12**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa12)**.**   D  [**13**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa13)**.**   C  [**14**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa14)**.**   B  [**15**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa15)**.**   D  [**16**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa16)**.**   D  [**17**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa17)**.**   A  [**18**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa18)**.**   C  [**19**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa19)**.**   B  [**20**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa20)**.**   A | [**21**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa21)**.**   D  [**22**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa22)**.**   A  [**23**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa23)**.**   C  [**24**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa24)**.**   C  [**25**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa25)**.**   B  [**26**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa26)**.**   D  [**27**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa27)**.**   A  [**28**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa28)**.**   B  [**29**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa29)**.**   D  [**30**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa30)**.**   C  [**31**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa31)**.**   A  [**32**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa32)**.**   A  [**33**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa33)**.**   D  [**34**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa34)**.**   B  [**35**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa35)**.**   C  [**36**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa36)**.**   B  [**37**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa37)**.**   D  [**38**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa38)**.**   A  [**39**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa39)**.**   C  [**40**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa40)**.**   A | [**41**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa41)**.**   D  [**42**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa42)**.**   A  [**43**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa43)**.**   B  [**44**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa44)**.**   B  [**45**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa45)**.**   D  [**46**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa46)**.**   C  [**47**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa47)**.**   D  [**48**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa48)**.**   A  [**49**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa49)**.**   B  [**50**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa50)**.**   B  [**51**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa51)**.**   D  [**52**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa52)**.**   C  [**53**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa53)**.**   A  [**54**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa54)**.**   B  [**55**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa55)**.**   D  [**56**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa56)**.**   B  [**57**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa57)**.**   C  [**58**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa58)**.**   A  [**59**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa59)**.**   B  [**60**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa60)**.**   C | [**61**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa61)**.**   D  [**62**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa62)**.**   B  [**63**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa63)**.**   A  [**64**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa64)**.**   D  [**65**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa65)**.**   B  [**66**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa66)**.**   D  [**67**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa67)**.**   A  [**68**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa68)**.**   B  [**69**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa69)**.**   B  [**70**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa70)**.**   D  [**71**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa71)**.**   A  [**72**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa72)**.**   B  [**73**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa73)**.**   D  [**74**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2qa74)**.**   C |

### A ANSWERS

[**1**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q1)**.**   Which of the following best describes information security governance?

**A.**   Information security policies.

**B.**   Information security policies along with audits of those policies.

**C.**   Management’s control of information security processes.

**D.**   Benchmarks of metrics as compared to similar organizations.

Images  **C**. ISACA defines governance as a set of processes that “[e]nsures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives.”

Images  **A**, **B**, and **D** are incorrect. **A** is incorrect because, although information security policies are an essential part of information security governance, there are several other components to governance as well. **B** is incorrect because security policies and activities (such as audits) to measure their effectiveness are only one component of information security governance. **D** is incorrect because the comparison of metrics to other organizations is not a significant part of a governance program. Indeed, many organizations forego benchmarking entirely.

[**2**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q2)**.**   What is the best method for ensuring that an organization’s security program achieves adequate business alignment?

**A.**   Find and read the organization’s articles of incorporation.

**B.**   Understand the organization’s vision, mission statement, and objectives.

**C.**   Study the organization’s chart of management reporting (the “org chart”).

**D.**   Study the organization’s financial chart of accounts.

Images  **B**. The best way to align an information security program to the business is to find and understand the organization’s vision statement, mission statement, goals, and objectives. Many organizations develop and publish one or more of these statements. Others take a simpler approach and develop strategic objectives for a calendar or fiscal year. Whatever can be found is valuable: once a security manager understands these statements, then he or she can prioritize resources and activities in the information security program to support the vision, mission, goals, or other strategic statements.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because an organization’s articles of incorporation do not provide sufficient information about an organization’s mission or objectives. **C** is incorrect because the org chart reveals little about what the organization wants to accomplish. **D** is incorrect because the organization’s financial chart of accounts reveals little or nothing about the organization’s strategic objectives.

[**3**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q3)**.**   Robert has located his organization’s mission statement and a list of strategic objectives. What steps should Robert take to ensure that the information security program aligns with the business?

**A.**   Discuss strategic objectives with business leaders to understand better what they want to accomplish and what steps are being taken to achieve them.

**B.**   Develop a list of activities that will support the organization’s strategic objectives, and determine the cost of each.

**C.**   Select those controls from the organization’s control framework that align to each objective, and then ensure that those controls are effective.

**D.**   Select the policies from the organization’s information security policy that are relevant to each objective, and ensure that those policies are current.

Images  **A**. The best first step to aligning an information security program to the organization’s strategic objectives is to understand those objectives fully, including the resources and activities that will be employed to achieve them.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because, without a dialogue with business leaders, simply identifying supporting activities is likely to miss important details. **C** is incorrect because proper alignment of an information security program does not generally begin with the selection or implementation of controls. In fact, the implementation of controls may play only a minor part (if any) in support of strategic objectives. **D** is incorrect because proper alignment of an information security program does not generally involve identifying relevant security policies. This may be a minor supporting activity but would not be a primary activity when aligning a program to the business.

[**4**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q4)**.**   Michael wants to improve the risk management process in his organization by creating guidelines that will help management understand when certain risks should be accepted and when certain risks should be mitigated. The policy that Michael needs to create is known as what?

**A.**   Security policy

**B.**   Control framework

**C.**   Risk appetite statement

**D.**   Control testing procedure

Images  **C**. A risk appetite statement (sometimes known as a risk tolerance statement or risk capacity statement) provides guidance on the types of risk and the amount of risk that an organization may be willing to accept, versus what risks an organization may instead prefer to mitigate, avoid, or transfer. Risk appetite statements are most often created in financial services organizations, although they are used in other types of organizations as well. They help management seek a more consistent approach to risk treatment decisions. In part, this can help management avoid the appearance of being biased or preferential through the use of objective or measurable means for risk treatment decisions.

Images  **A**, **B**, and **D** are incorrect. **A** is incorrect because a security policy is not a primary means for making risk treatment decisions. **B** is incorrect because an organization’s controls framework is not typically used for making risk treatment decisions. **D** is incorrect because control testing procedures are not related to risk treatment decisions.

[**5**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q5)**.**   In a risk management process, who is the best person(s) to make a risk treatment decision?

**A.**   Chief risk officer (CRO)

**B.**   Chief information officer (CIO)

**C.**   Process owner who is associated with the risk

**D.**   Chief information security officer (CISO)

Images  **C**. The department head (or division head or business owner, as appropriate) associated with the business activity regarding the risk treatment decision should be the person making the risk treatment decision. This is because a risk treatment decision is a business decision that should be made by the person who is responsible for the business function.

Images  **A**, **B**, and **D** are incorrect. **A** is incorrect because the chief risk officer (CRO) should not be making business function risk decisions on behalf of department heads or business owners. At best, the CRO should be facilitating discussions leading to risk treatment decisions. **B** is incorrect because the CIO should not be making business function risk decisions on behalf of department heads or business owners. **D** is incorrect because the CISO should not be making risk treatment decisions. Instead, the CISO should, at best, be facilitating discussions that lead to risk treatment decisions made by department heads or business owners.

[**6**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q6)**.**   The ultimate responsibility for an organization’s cybersecurity program lies with whom?

**A.**   The board of directors

**B.**   The chief executive officer (CEO)

**C.**   The chief information officer (CIO)

**D.**   The chief information security officer (CISO)

Images  **A**. The ultimate responsibility for everything in an organization, including its cybersecurity program, lies with its board of directors. Various laws and regulations define board member responsibilities, particularly in publicly traded organizations in the United States and in other countries.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect, except in unusual cases when an organization does not have a board of directors. **C** is incorrect because this is about ultimate responsibility, which lies with the board of directors. **D** is incorrect because the CISO’s role should be one of a facilitator, wherein other members of executive management, as well as board members, make business decisions (including cybersecurity-related decisions) on behalf of the organization.

[**7**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q7)**.**   In a U.S. public company, a CISO will generally report the state of the organization’s cybersecurity program to:

**A.**   The Treadway Commission

**B.**   Independent auditors

**C.**   The U.S. Securities and Exchange Commission

**D.**   The audit committee of the board of directors

Images  **D**. In most U.S. publicly traded companies, the CISO will report the state of the organization’s cybersecurity program to members of the audit committee of the board of directors. Although this is the best answer, in some organizations, the CIO or CEO may instead report on the cybersecurity program.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because an organization would not report anything to the Treadway Commission. **B** is incorrect because the CISO would typically not report the state of the cybersecurity program to independent auditors. In public companies, however, the CISO and independent auditors will periodically meet to discuss the cybersecurity program. **C** is incorrect because the CISO would not be reporting to the U.S. Securities and Exchange Commission (SEC). An organization’s internal auditor or CFO will, however, submit reports about the organization’s financial results to the SEC, although these filings will rarely include information about cybersecurity, unless there has been a security incident that had material impact on the organization.

[**8**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q8)**.**   A new CISO in an organization is building its cybersecurity program from the ground up. To ensure collaboration among business leaders and department heads in the organization, the CISO should form and manage which of the following?

**A.**   A risk committee of the board of directors

**B.**   A cybersecurity steering committee

**C.**   An audit committee of the board of directors

**D.**   Business-aligned security policy

Images  **B**. A cybersecurity steering committee, consisting of senior executives, business unit leaders, and department heads, when properly facilitated by the CISO, can discuss organization-wide issues related to cybersecurity and make strategic decisions about cyber risk.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because the CISO will not be involved in the formation and management of a board of directors risk committee. **C** is incorrect because a CISO would not be involved in the formation or management of a board of directors audit committee. **D** is incorrect because a business-aligned security policy, while important, would not significantly foster collaboration among business leaders.

[**9**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q9)**.**   Who is the best person or group to make cyber-risk treatment decisions?

**A.**   The chief information security officer (CISO)

**B.**   The audit committee of the board of directors

**C.**   The cybersecurity steering committee

**D.**   The chief risk officer (CRO)

Images  **C**. The cybersecurity steering committee, which should consist of senior executives, business unit leaders, and department heads, should openly discuss, collaborate, and decide on most risk treatment issues in an organization. If decisions are made by individuals such as the CISO or CRO, then business leaders may be less likely to support those decisions, as they may not have had a part in decision-making.

Images  **A**, **B**, and **D** are incorrect. **A** is incorrect because the CISO unilaterally making risk treatment decisions for the organization is less likely to get buy-in from other business leaders, who may feel they did not have a voice in making these decisions. **B** is incorrect because audit committee members rarely get involved in risk treatment decision-making. **D** is incorrect because the CRO unilaterally making risk treatment decisions will result in less buy-in and support from business leaders than if they participated in these decisions.

[**10**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q10)**.**   Which is the best party to conduct access reviews?

**A.**   Users’ managers

**B.**   Information security manager

**C.**   IT service desk

**D.**   Department head

Images  **D**. The persons who are responsible for business activities should be the ones who review users’ access to applications that support their business activities. All too often, however, access reviews are performed by persons less qualified to make decisions about which persons should have access (and at what levels or capabilities) to systems and applications critical to their business processes. Commonly, IT personnel perform these reviews as a proxy for business owners, but often IT personnel do not have as much knowledge about business operations and are therefore less qualified to make quality decisions about user access. IT personnel can perform a user access review only if they have a sound understanding of user roles; but even then, business owners should be informed of user access reviews and their outcome.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because the managers of users with access to systems and applications are not the best parties to review access. **B** is incorrect because information security managers have insufficient knowledge about business operations and the persons using them. **C** is incorrect because IT service desk personnel have insufficient knowledge about business operations and the persons using them. More often, IT service personnel are the ones who carry out access changes. Since they are the ones carrying out changes (in most cases), they should not also be the party reviewing who has access, because they would be reviewing their own work.

[**11**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q11)**.**   Which is the best party to make decisions about the purpose and function of business applications?

**A.**   Business department head

**B.**   IT business analyst

**C.**   Application developer

**D.**   End user

Images  **A**. As the party who is responsible for the ongoing operations and success of business operations and business processes, a business department head is the best party to determine the behavior of business applications supporting business processes.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because IT business analysts are not responsible for decisions about business unit operations. That said, the IT business analyst’s role may include facilitation of discussions concerning the configuration and function of business applications, and in some cases he or she may make configuration changes. **C** is incorrect because application developers are not responsible for decisions about business unit operations. In some cases, however, application developers may have intimate knowledge of the internal workings of business applications and may provide insight into the function of applications. Thus, they may provide information in support of decisions made by business department heads. **D** is incorrect because end users are generally not responsible for decisions about business unit operations.

[**12**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q12)**.**   Which of the following is the best definition of custodial responsibility?

**A.**   Custodian protects assets based on customer’s defined interests

**B.**   Custodian protects assets based on its own defined interests

**C.**   Custodian makes decisions based on its own defined interests

**D.**   Custodian makes decisions based on customer’s defined interests

Images  **D**. A custodian is charged with a potentially wide range of decisions regarding the care of an asset. Decisions are based upon the customer’s defined interests. A germane example is an IT department that builds and maintains information systems on behalf of internal customers; the IT department will make various decisions about the design and operation of an information system so that the system will best meet customers’ needs.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because protection of an asset is only a part of the scope of responsibility of a custodian. **B** is incorrect because a custodian does not protect assets based on its own interests, but on its customers’ interest. **C** is incorrect because a custodian does not make decisions based on its own interests, but instead on its customers’ interest.

[**13**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q13)**.**   What is the primary risk of IT acting as custodian for a business owner?

**A.**   IT may not have enough interest to provide quality care for business applications.

**B.**   IT may not have sufficient staffing to care for business applications properly.

**C.**   IT may have insufficient knowledge of business operations to make good decisions.

**D.**   Business departments might not give IT sufficient access to manage applications properly.

Images  **C**. IT personnel tend to focus their thoughts on the technology supporting business departments rather than on the business operations occurring in the business departments they support. Often, IT departments are observed to make too many assumptions about the needs of their customers, and they do not work hard enough to understand their users’ needs to ensure that business applications will support them properly.

Images  **A**, **B**, and **D** are incorrect. **A** and **B** are incorrect because they are not the best answers. **D** is incorrect because business units are not generally in a position to restrict IT departments from administrative access to business applications.

[**14**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q14)**.**   An organization needs to hire an executive who will build a management program that will consider threats and vulnerabilities and determine controls needed to protect systems and work centers. What is the best job title for this position?

**A.**   CSO

**B.**   CRO

**C.**   CISO

**D.**   CIRO

Images  **B**. The CRO (chief risk officer) is responsible for managing risk for multiple types of assets, commonly information assets, as well as physical assets and/or workplace safety. In financial services organizations, the CRO will also manage risks associated with financial transactions or financial asset portfolios.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because the CSO (chief security officer) is not necessarily responsible for risk management, but is instead responsible for the design, deployment, and operation of protective controls, commonly for information systems as well as other assets such as equipment or work centers. **C** is incorrect because the CISO (chief information security officer) is typically responsible for protection of only information assets and not other types of assets such as property, plant, and equipment. **D** is incorrect because the CIRO (chief information risk officer) is typically responsible for risk management and protection of information assets but not other types of assets, such as property, plant, and equipment.

[**15**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q15)**.**   An organization needs to hire an executive who will be responsible for ensuring that the organization’s policies, business processes, and information systems are compliant with laws and regulations concerning the proper collection, use, and protection of personally identifiable information. What is the best job title for the organization to use for this position?

**A.**   CSO

**B.**   CIRO

**C.**   CISO

**D.**   CPO

Images  **D**. The chief privacy officer (CPO) is the best title for a position in which the executive ensures that the organization’s policies, practices, controls, and systems ensure the proper collection, use, and protection of personally identifiable information (PII).

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because the chief security officer (CSO) is typically not responsible for privacy-related activities concerning the collection and use of PII. **B** is incorrect because the chief information risk officer (CIRO) is typically not responsible for privacy-related activities concerning the collection and use of PII. **C** is incorrect because the chief information security officer (CISO) is typically not responsible for privacy-related activities concerning the collection and use of PII.

[**16**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q16)**.**   The Big Data Company is adjusting several position titles in its IT department to reflect industry standards. Included in consideration are two individuals: The first is responsible for the overall relationships and data flows among its internal and external information systems. The second is responsible for the overall health and management of systems containing information. Which two job titles are most appropriate for these two roles?

**A.**   Systems architect and database administrator

**B.**   Data architect and data scientist

**C.**   Data scientist and database administrator

**D.**   Data architect and database administrator

Images  **D**. Data architect is the best position title for someone who is responsible for the overall relationships and data flows among the organization’s information systems. Database administrator (DBA) is the best position title for someone who is responsible for maintaining the database management systems (DBMSs) throughout the organization.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because systems architect is not the best title for someone who is responsible for the overall relationships and data flows among the organization’s information systems. **B** is incorrect because data scientist is not the best title for someone who is responsible for the overall health and management of systems containing information. **C** is incorrect because data scientist is not the best title for someone who is responsible for the overall relationships and data flows among its internal and external information systems.

[**17**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q17)**.**   What is the primary distinction between a network engineer and a telecom engineer?

**A.**   A network engineer is primarily involved with networks and internal network media, while a telecom engineer is primarily involved with networks and external (carrier) network media.

**B.**   A network engineer is primarily involved with networks and external (carrier) network media, while a telecom engineer is primarily involved with networks and internal network media.

**C.**   A network engineer is primarily involved with layer 3 protocols and above, while a telecom engineer is primarily involved with layer 1 and layer 2 protocols.

**D.**   There is no distinction, as both are involved in all aspects of an organization’s networks.

Images  **A**. A network engineer is primarily involved with networks and internal network media (including cabling and internal wireless networks such as Wi-Fi), while a telecom engineer is primarily involved with networks and external (carrier) network media such as Multiprotocol Label Switching (MPLS), Frame Relay, and dark fibre.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because the definitions in this answer are swapped. **C** is incorrect because the distinction between a network engineer and a telecom engineer are not strictly about protocol layers. **D** is incorrect because there is a distinction between the network engineer and telecom engineer position titles.

[**18**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q18)**.**   An organization that is a U.S. public company is redesigning its access management and access review controls. What is the best role for internal audit in this redesign effort?

**A.**   Develop procedures

**B.**   Design controls

**C.**   Provide feedback on control design

**D.**   Develop controls and procedures

Images  **C**. Any internal audit function should not design or implement controls or procedures other than those in their own department. Internal audit cannot play a design role in any process or control that it may later be required to audit.

Images  **A**, **B**, and **D** are incorrect. **A** is incorrect because internal audit should not develop procedures that it may later be required to audit. Instead, internal audit can provide feedback on procedures developed by others. Internal audit can never be in a position to audit its own work. **B** is incorrect because internal audit should not develop controls that it may later be required to audit. Internal audit can provide feedback on controls designed by others. Internal audit can never be in a position to audit its own work. **D** is incorrect because internal audit should not develop controls or procedures. This is because internal audit may be required to audit these controls and/or procedures; internal audit can never be in a position to audit its own work.

[**19**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q19)**.**   A security operations manager is proposing that engineers who design and manage information systems play a role in monitoring those systems. Is design and management compatible with monitoring? Why or why not?

**A.**   Personnel who design and manage systems should not perform a monitoring role because this is a conflict of interest.

**B.**   Personnel who design and manage systems will be more familiar with the reasons and steps to take when alerts are generated.

**C.**   Personnel who design and manage systems will not be familiar with response procedures when alerts are generated.

**D.**   Personnel who design and manage systems are not permitted access to production environments and should not perform monitoring.

Images  **B**. Personnel who design and manage information systems are more likely to be familiar with the nature of alerts as well as procedures for responding to them.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because there would normally not be any conflict of interest between design, management, and monitoring. **C** is incorrect because personnel who design and manage information systems are in a position to understand how those systems work and would be more likely to know how to respond to alerts. **D** is incorrect because personnel who manage information systems would be permitted to access them in production environments.

[**20**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q20)**.**   What is the purpose of metrics in an information security program?

**A.**   To measure the performance and effectiveness of security controls

**B.**   To measure the likelihood of an attack on the organization

**C.**   To predict the likelihood of an attack on an organization

**D.**   To predict the method of an attack on an organization

Images  **A**. The purpose of metrics is to measure the performance and effectiveness of security controls. The meaning and usefulness of specific metrics will depend upon the context and measurement method of specific controls.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because metrics do not necessarily foretell of an attack on an organization. **C** is incorrect because metrics are not always used to predict an attack on an organization. **D** is incorrect because metrics do not necessarily predict the method used for an attack on an organization.

[**21**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q21)**.**   Which security metric is best considered a leading indicator of an attack?

**A.**   Number of firewall rules triggered

**B.**   Number of security awareness training sessions completed

**C.**   Percentage of systems scanned

**D.**   Mean time to apply security patches

Images  **D**. There is a strong correlation between the absence of security patches and the likelihood and success of attacks on systems. Information systems patched soon after patches are available are far less likely to be successfully attacked, whereas systems without security patches (and those in which the organization takes many months to apply patches) are easy targets for intruders.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because this is not the best answer. Although the number of firewall rules triggered may signal the level of unwanted network activity, there is not necessarily a strong correlation between this and the likelihood of an attack. This is because the likelihood of a successful attack is more dependent on other conditions such as patch levels and login credentials. **B** is incorrect because this is not the best answer. Although a higher percentage of completion of security awareness training may indicate a workforce that is more aware of social engineering techniques, other factors such as patch levels are usually more accurate indicators. **C** is incorrect because the percentage of systems scanned is not a reliable attack indicator. This is still a valuable metric, however, because it contributes to an overall picture of vulnerability management process effectiveness.

[**22**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q22)**.**   Steve, a CISO, has vulnerability management metrics and needs to build business-level metrics. Which of the following is the best leading indicator metric suitable for his organization’s board of directors?

**A.**   Average time to patch servers supporting manufacturing processes

**B.**   Frequency of security scans of servers supporting manufacturing processes

**C.**   Percentage of servers supporting manufacturing processes that are scanned by vulnerability scanning tools

**D.**   Number of vulnerabilities remediated on servers supporting manufacturing processes

Images  **A**. This is the best metric that serves as a leading indicator. This metric portrays the average time that critical servers are potentially exposed to new security threats. A metric is considered a leading indicator if it foretells future events.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because the number of scans provides no information about vulnerabilities and, therefore, risk of successful attack. Frequency of security scans is a good operational metric, although a better one would be percentage of critical servers scanned. **C** is incorrect because the percentage of critical systems scanned reveals little about vulnerabilities and their remediation. This is, however, a good operational metric that helps the CISO understand the effectiveness of the vulnerability management process. **D** is incorrect because a raw number, such as number of vulnerabilities remediated, tells board members little or nothing useful to them.

[**23**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q23)**.**   The metric “percentage of systems with completed installation of advanced antimalware” is best described as what?

**A.**   Key operational indicator (KOI)

**B.**   Key performance indicator (KPI)

**C.**   Key goal indicator (KGI)

**D.**   Key risk indicator (KRI)

Images  **C**. An installation completion metric is most likely associated with a strategic goal, in this case, the installation of advanced antimalware on systems. This metric could arguably be a KRI as well, because this may also indicate risk reduction on account of an improved capability.

Images  **A**, **B**, and **D** are incorrect. **A** is incorrect because key operational indicator is not an industry standard term. Still, this type of metric is not operational in nature, but more associated with the completion of a strategic objective. **B** is incorrect because KPI is not the best description of this type of metric, and this activity of completion of software installations is not typically associated with performance (except, possibly, the performance of the team performing the installations). **D** is incorrect because this metric is a better KGI than it is a KRI. However, this metric could also be considered a KRI if the installation of advanced antimalware can be shown to help reduce risk.

[**24**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q24)**.**   A member of the board of directors has asked Ravila, a CIRO, to produce a metric showing the reduction of risk as a result of the organization making key improvements to its security information and event management system. Which type of metric is most suitable for this purpose?

**A.**   KGI

**B.**   RACI

**C.**   KRI

**D.**   ROSI

Images  **C**. The most suitable metric is a key risk indicator (KRI). Still, this will be a challenge because high-impact events usually occur rarely.

Images  **A**, **B**, and **D** are incorrect. **A** is incorrect because a key goal indicator is not the best indicator of risk. **B** is incorrect because the answer is a distractor. RACI stands for Responsible, Accountable, Consulted, and Informed and is used to assign roles and responsibilities. **D** is incorrect as return on security investment (ROSI) is not a suitable metric because significant events occur rarely.

[**25**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q25)**.**   A common way to determine the effectiveness of security and risk metrics is the SMART method. What does SMART stand for?

**A.**   Security Metrics Are Risk Treatment

**B.**   Specific, Measurable, Attainable, Relevant, Timely

**C.**   Specific, Measurable, Actionable, Relevant, Timely

**D.**   Specific, Manageable, Actionable, Relevant, Timely

Images  **B**. SMART, in the context of metrics, stands for Specific, Measurable, Attainable, Relevant, and Timely.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because the answer Security Metrics Are Risk Treatment is a distractor. **C** and **D** are incorrect because these are not definitions of SMART in the context of metrics.

[**26**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q26)**.**   The statement “Complete migration of flagship system to latest version of vendor-supplied software” is an example of what?

**A.**   Mission statement

**B.**   Vision statement

**C.**   Purpose statement

**D.**   Objective statement

Images  **D**. The statement is a strategic objective.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because the statement is too specific to be a mission statement. **B** is incorrect because the statement is not typical of a vision statement. **C** is incorrect because the statement is not typical of a purpose statement.

[**27**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q27)**.**   Ernie, a CISO who manages a large security group, wants to create a mission statement for the CISO group. What is the best approach for creating this mission statement?

**A.**   Start with the organization’s mission statement.

**B.**   Start with Ernie’s most recent performance review.

**C.**   Start with the results of the most recent risk assessment.

**D.**   Start with the body of open items in the risk register.

Images  **A**. The best way to manage a security organization is to align it with the business it is supporting. When creating a security organization mission statement, a good start is to look at the overall organization’s mission statement; this way, the security team’s mission is more likely to align with the overall organization. If the overall organization lacks a mission statement, the CISO can use what he knows about the organization’s purpose to build a security team mission statement that is sure to support the organization.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because it is not the best answer. Still, it is possible that the CISO’s performance review may be well aligned with the overall business and may be a useful reference for creating a CISO team mission statement. **C** is incorrect because, by itself, a risk assessment report, though it may be an indicator of the nature of the work that the CISO organization may be undertaking in the future, will not provide much information about the overall business’s purpose. **D** is incorrect because the risk register’s open items will not provide much information about the organization’s overall purpose. Although the risk register’s open items may be an indicator of the types of work that the CISO organization will be working on, this does not provide sufficient information to develop the CISO organization’s mission, because the CISO’s mission is more than just solving short-term problems.

[**28**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q28)**.**   Which of the following statements is the best description for the purpose of performing risk management?

**A.**   Identify and manage vulnerabilities that may permit security events to occur.

**B.**   Identify and address threats that are relevant to the organization.

**C.**   Assess the risks associated with third-party service providers.

**D.**   Assess and manage risks associated with doing business online.

Images  **B**. The purpose of risk management is to identify threats that, if they occurred, would cause some sort of harm to the organization. Persons running the risk management process would identify threats (and other risks), perform analysis on them, and collaborate with others to obtain agreement on the right risk treatment strategy.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because the management of vulnerabilities is only a single facet of risk management. A sound risk management program will, however, consider vulnerabilities within each risk assessment and risk analysis to help in the identification of risk treatment options. **C** is incorrect because the scope of risk management encompasses the entire organization, not only its third-party service providers. That said, it is important for an organization’s overall risk management program to identify and manage risks associated with third-party service providers. **D** is incorrect because the scope of risk management is far broader than just an organization’s online business, even if the organization’s entire business operation consists of doing business online. Even then, there will be other business activities that should be a part of its risk management program.

[**29**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q29)**.**   Key metrics showing effectiveness of a risk management program would not include which of the following?

**A.**   Reduction in the number of security events

**B.**   Reduction in the impact of security events

**C.**   Reduction in the time to remediate vulnerabilities

**D.**   Reduction in the number of patches applied

Images  **D**. The number of patches applied is not a metric that indicates a risk management program’s effectiveness, nor the effectiveness of a vulnerability management program.

Images  **A**, **B**, and **C** are incorrect. They are all incorrect because each of them is potentially a useful risk management program metric.

[**30**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q30)**.**   Examples of security program performance include all of the following except:

**A.**   Time to detect security incidents

**B.**   Time to remediate security incidents

**C.**   Time to perform security scans

**D.**   Time to discover vulnerabilities

Images  **C**. The time required to perform security scans is not a good example of a security program performance metric.

Images  **A**, **B**, and **D** are incorrect. **A** is incorrect because time to detect security incidents is a good example of a security program performance metric. **B** is incorrect because time to remediate security incidents is a good example of a security program performance metric. **D** is incorrect because time to discover vulnerabilities is a good example of a security program performance metric.

[**31**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q31)**.**   Two similar-sized organizations are merging. Paul will be the CISO of the new combined organization. What is the greatest risk that may occur as a result of the merger?

**A.**   Differences in practices that may not be understood

**B.**   Duplication of effort

**C.**   Gaps in coverage of key processes

**D.**   Higher tooling costs

Images  **A**. A merger of two organizations typically results in the introduction of new practices that are not always understood. The CISO may specify directives to the new combined security organization that could result in an increase in one or more risks. For example, the combining of two different organizations’ device hardening standards could result in a new standard that results in new and unforeseen vulnerabilities.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because duplication of effort is not the greatest risk. **C** is incorrect because coverage gaps are a potential risk, but they are not the greatest risk. **D** is incorrect because higher tooling costs, if managed properly, are a short-term spending matter that should not result in increased risk.

[**32**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q32)**.**   What is the purpose of value delivery metrics?

**A.**   Long-term reduction in costs

**B.**   Reduction in ROSI

**C.**   Increase in ROSI

**D.**   Increase in net profit

Images  **A**. Value delivery metrics are most often associated with the long-term reduction in costs, in proportion to other measures such as the number of employees and assets.

Images  **B**, **C**, and **D** are incorrect. **B** and **C** are incorrect because value delivery metrics are not usually associated with return on security investment (ROSI). **D** is incorrect because value delivery metrics are not associated with profit.

[**33**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q33)**.**   Joseph, a CISO, is collecting statistics on several operational areas and needs to find a standard way of measuring and publishing information about the effectiveness of his program. Which of the following is the best approach to follow?

**A.**   Scaled Score

**B.**   NIST Cybersecurity Framework (CSF)

**C.**   Business Model for Information Security (BMIS)

**D.**   Balanced Scorecard (BSC)

Images  **D**. The Balanced Scorecard is a well-known framework that is used to measure the performance and effectiveness of an organization. The Balanced Scorecard framework is used to determine how well an organization can fulfill its mission and strategic objectives and how well it is aligned with overall organizational objectives.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because a scaled score is not a method used to publish metrics. **B** is incorrect because the NIST CSF is not typically used as a framework for publishing security program metrics. **C** is incorrect, as the Business Model for Information Security (BMIS), while valuable for understanding the relationships between people, process, technology, and the organization, is not used for publishing metrics.

[**34**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q34)**.**   Which of the following is the best description of the Business Model for Information Security (BMIS)?

**A.**   It describes the relationships (as dynamic interconnections) between policy, people, process, and technology.

**B.**   It describes the relationships (as dynamic interconnections) between people, process, technology, and the organization.

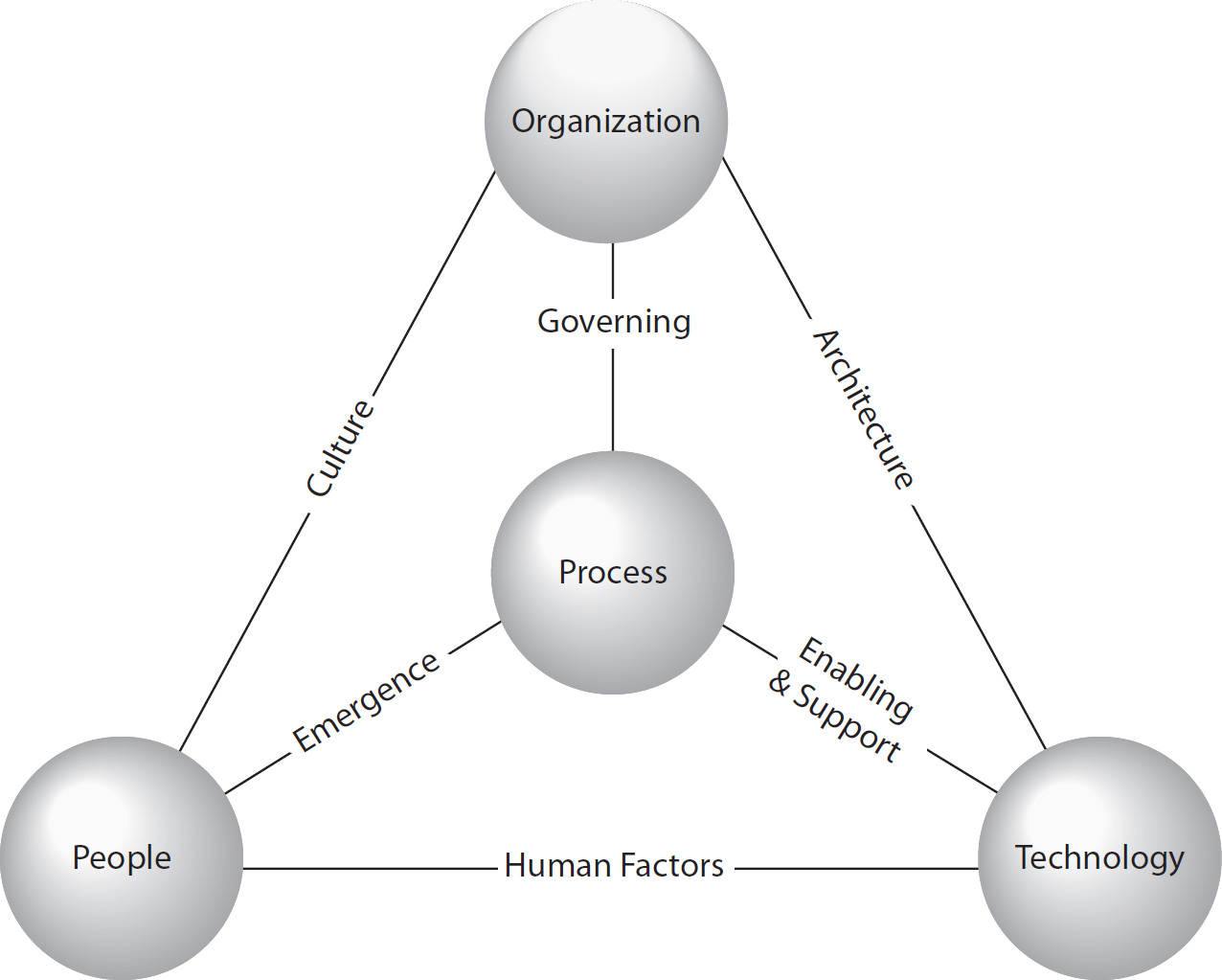
**C.**   It describes the primary elements (people, process, and technology) in an organization.

**D.**   It describes the dynamic interconnections (people, process, and technology) in an organization.

Images  **B**. The Business Model for Information Security (BMIS) describes the dynamic interconnections between the four elements of an organization: people, process, technology, and the organization itself. The dynamic interconnections describe the relationship between each of the relationship pairs. For example, the dynamic interconnection between people and technology, known as human factors, describes the relationship between people and technology.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because the organization element of BMIS is missing in this answer. **C** is incorrect because there are four primary elements in an organization: people, process, technology, and the organization itself. **D** is incorrect because people, process, and technology are not the labels for the dynamic interconnections. Instead, the dynamic interconnections are human factors (between people and technology), emergence (between people and process), enabling and support (between process and technology), culture (between people and organization), architecture (between technology and organization), and governing (between process and organization).

[**35**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q35)**.**   What is the correct name for the following illustration?



**A.**   COBIT Model for Information Technology

**B.**   COBIT Model for Information Security

**C.**   Business Model for Information Security

**D.**   Business Model for Information Technology

Images  **C**. This illustration depicts the Business Model for Information Security (BMIS), which was developed by ISACA to help individuals better understand the nature of the relationships between people, process, technology, and the organization itself.

Images  **A**, **B**, and **D** are incorrect. These answers are all distractors.

[**36**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q36)**.**   Jacqueline, an experienced CISO, is reading the findings in a recent risk assessment that describes deficiencies in the organization’s vulnerability management process. How would Jacqueline use the Business Model for Information Security (BMIS) to analyze the deficiency?

**A.**   Identify the elements connected to the process DI.

**B.**   Identify the dynamic interconnections (DIs) connected to the process element.

**C.**   Identify the dynamic elements connected to human factors.

**D.**   Identify the dynamic elements connected to technology.

Images  **B**. The deficiency was identified in the vulnerability management process. The CISO would see what dynamic interconnections (DIs) are connected to the process element. They are emergence (connecting to people), enabling and support (connecting to technology), and governing (connecting to organization). A description of the deficiency in the vulnerability management process should lead Jacqueline to one of the dynamic interconnections, emergence, enabling & support, and governing. In this case, the process deficiency is related to the frequency of scans, which is most likely the governing DI. Further investigation reveals that policy permits vulnerability scans only during small service windows, which are not enough time for scans to be completed. The solution to this deficiency is likely a process or policy change so that scans will be permitted to run through to completion.

Images  **A**, **C**, and **D** are incorrect. They are all distractors.

[**37**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q37)**.**   Which of the following would constitute an appropriate use of the Zachman enterprise framework?

**A.**   An IT service management model as an alternative to ITIL

**B.**   Identifying system components, followed by high-level design and business functions

**C.**   Development of business requirements, translated top-down into technical architecture

**D.**   IT systems described at a high level and then in increasing levels of detail

Images  **D**. Zachman is an IT enterprise framework that describes IT systems at a high level and in increasing levels of detail, down to individual components.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because Zachman is not an IT service management framework. **B** is incorrect because Zachman is a top-down framework, not a bottom-up framework as described. **C** is incorrect because Zachman does not start with business requirements, but describes only the IT architecture itself.

[**38**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q38)**.**   An IT architect needs to document the flow of data from one system to another, including external systems operated by third-party service providers. What kind of documentation does the IT architect need to develop?

**A.**   Data flow diagrams (DFDs)

**B.**   Entity relationship diagrams (EFDs)

**C.**   A Zachman architecture framework

**D.**   Visio diagrams showing information systems and data flows

Images  **A**. The IT architect needs to develop data flow diagrams, which are visual depictions showing information systems (and information system components, optionally) and the detailed nature of data flowing among them. DFDs are sometimes accompanied by documents that describe metadata, such as system specifications and descriptions.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because an entity relationship diagram (ERD) does not depict data flows among and between information systems. Instead, ERDs describe entities (for instance, information systems) and the relationships between them. ERDs are often depicted visually. **C** is incorrect because a Zachman framework describes the architecture of an IT environment in detail, but not necessarily the flows of data between systems in an environment. **D** is incorrect because this is a vague description. Although it is true that a DFD may be composed in Visio (or other graphical drawing tool), this is not the best answer because it is unspecific.

[**39**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q39)**.**   Carole is a CISO in a new organization with a fledgling security program. Carole needs to identify and develop mechanisms to ensure desired outcomes in selected business processes. What is a common term used to define these mechanisms?

**A.**   Checkpoints

**B.**   Detective controls

**C.**   Controls

**D.**   Preventive controls

Images  **C**. “Controls” is the best term describing the mechanisms designed to ensure desired outcomes in business processes.

Images  **A**, **B**, and **D** are incorrect. **A** is incorrect because “checkpoints” is not the term that describes these mechanisms. **B** is incorrect because there will not only be detective controls but also preventive controls, administrative controls, and perhaps even compensating and recovery controls. **D** is incorrect because there will not only be preventive controls but also detective controls, administrative controls, and perhaps even compensating and recovery controls.

[**40**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q40)**.**   What is the best approach to developing security controls in a new organization?

**A.**   Start with a standard control framework and make risk-based adjustments as needed.

**B.**   Start from scratch and develop controls based on risk as needed.

**C.**   Start with NIST CSF and move up to ISO 27001, and then NIST 800-53 as the organization matures.

**D.**   Develop controls in response to an initial risk assessment.

Images  **A**. Starting with a standard control framework is the best approach, particularly if an appropriate, business-relevant framework is selected. In a proper risk management framework, risk assessment and risk treatment will result in adjustments to the framework (removing, improving, and adding controls) over time.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because, although technically this approach will work, too much time may elapse while waiting for the initial set of controls to be developed. In most organizations, over several years, the resulting control framework will not be that different from a standard, industry-relevant framework. **C** is incorrect because there is little to be gained by changing from one control framework to another. Because this approach is not risk based, there is a chance that some risks will result in never having appropriate controls developed to compensate for those risks. **D** is incorrect because this approach implies that only an initial risk assessment takes place. Instead, the accepted approach is one where risk assessments are performed periodically, resulting in periodic adjustments to the control framework in response to newly discovered risks.

[**41**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q41)**.**   Which of the following is the best description of the COBIT framework?

**A.**   A security process and controls framework that can be integrated with ITIL or ISO 20000

**B.**   An IT controls and process framework on which IT controls and processes can be added at an organization’s discretion

**C.**   An IT process framework with optional security processes when Extended COBIT is implemented

**D.**   An IT process framework that includes security processes that are interspersed throughout the framework

Images  **D**. COBIT is an IT process framework with security processes that appear throughout the framework. Developed by ISACA and now in its fifth major release, COBIT’s four domains are plan and organize, acquire and implement, deliver and support, and monitor and evaluate. IT and security processes are contained in each of these domains.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because COBIT is not strictly a security controls framework. **B** is incorrect because the security processes are not considered optional in COBIT. **C** is incorrect because there is no such thing as Extended COBIT.

[**42**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q42)**.**   Name one distinct disadvantage of the ISO 27001 standard.

**A.**   The standard is costly (more than 100 U.S. dollars per copy).

**B.**   The standard is costly (a few thousand U.S. dollars per copy).

**C.**   The standard is available only for use in the United States.

**D.**   The standard is suitable only in large organizations.

Images  **A**. Single copies of the ISO 27001 standard (as well as virtually all other ISO standards) cost more than U.S. $100 each. This prevents widespread adoption of the standard, as organizations are somewhat less likely to implement it, since the standard is expensive to download and difficult to understand. Further, students are unlikely to learn about the standard in school because of its cost. Contrast this with most other standards, which are free to download and use.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because the ISO 27001 standard does not cost thousands of dollars per copy. **C** is incorrect because there are no restrictions on where ISO 27001 (and virtually all other standards) can be used. **D** is incorrect because ISO 27001 is suitable for organizations of all sizes, from very large to very small and everything in between.

[**43**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q43)**.**   Which of the following statements about ISO 27001 is correct?

**A.**   ISO 27001 consists primarily of a framework of security controls, followed by an appendix of security requirements for running a security management program.

**B.**   ISO 27001 consists primarily of a body of requirements for running a security management program, along with an appendix of security controls.

**C.**   ISO 27001 consists of a framework of information security controls.

**D.**   ISO 27001 consists of a framework of requirements for running a security management program.

Images  **B**. ISO 27001’s main focus is the body of requirements (sometimes known as clauses) that describe all of the required activities and business records needed to run an information security management program. ISO 27001 also includes an Annex A, containing a list of information security controls. The controls here are described briefly; the ISO 27002 standard contains the same control framework, but with longer explanations, as well as implementation guidance for each control.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because the main focus of ISO 27001 is the requirements for running a security management program, not the security controls. **C** is incorrect because ISO 27001’s main focus is the requirements for running a security management program. **D** is incorrect because ISO 27001 does not contain only the requirements for running a security management program but also includes an appendix of security controls also contained in ISO 27002, where they are fully explained.

[**44**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q44)**.**   What U.S. law regulates the protection of medical care–related data?

**A.**   PIPEDA

**B.**   HIPAA

**C.**   GLBA

**D.**   GDPR

Images  **B**. HIPAA, the Health Insurance Portability and Accountability Act, comprises a Privacy Rule and a Security Rule. The Privacy Rule limits what healthcare organizations are permitted to do with electronic patient healthcare information (EPHI), while the Security Rule stipulates various required processes and tooling for the protection of EPHI.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because PIPEDA is the Canadian Personal Information Protection and Electronic Documents Act that is the federal privacy law for private-sector organizations. It sets out the ground rules for how businesses must handle personal information in the course of commercial activity. **C** is incorrect because GLBA is the Gramm-Leach-Bliley Act, which established requirements for the protection of personal information in the U.S. financial services industry. Generally, organizations subject to GLBA are banks, credit unions, insurance companies, and securities trading firms. **D** is incorrect because GDPR is the European Union General Data Protection Regulation, the law that regulates the protection and use of personally identifiable information for European residents.

[**45**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q45)**.**   The regulation “Security and Privacy Controls for Federal Information Systems and Organizations,” is better known as what?

**A.**   ISO/IEC 27001

**B.**   ISO/IEC 27002

**C.**   NIST CSF

**D.**   NIST SP800-53

Images  **D**. NIST SP800-53, also known as NIST 800-53, is the security controls framework developed by the U.S. National Institute for Standards and Technology and published in its Special Publication number 800 library. NIST 800-53 is required of all branches of the U.S. federal government and has also been widely adopted by other government agencies and private industry in the United States and around the world. NIST 800-53 is available from <https://csrc.nist.gov/publications/sp>.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because ISO/IEC 27001 is known as “Information technology – Security techniques – Information security management systems – Requirements.” **B** is incorrect because ISO/IEC 27002 is known as “Information technology – Security techniques – Code of practice for information security controls.” **C** is incorrect because NIST CSF is known as the U.S. National Institute of Standards and Technology: Cybersecurity Framework.

[**46**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q46)**.**   What is the best explanation for the Implementation Tiers in the NIST Cybersecurity Framework?

**A.**   Implementation Tiers are levels of risk as determined by the organization.

**B.**   Implementation Tiers are stages of implementation of controls in the framework.

**C.**   Implementation Tiers are likened to maturity levels.

**D.**   Implementation Tiers are levels of risk as determined by an external auditor or regulator.

Images  **C**. Although the CSF states that Implementation Tiers are not strictly maturity levels, they are very similar to maturity levels.

Images  **A**, **B**, and **D** are incorrect. **A** and **D** are incorrect because Implementation Tiers are not risk levels. **B** is incorrect because Implementation Tiers are not related to the progress of implementation of controls.

[**47**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q47)**.**   Jeffrey is a CISO in an organization that performs financial services for private organizations as well as government agencies and U.S. federal agencies. Which is the best information security controls framework for this organization?

**A.**   CIS

**B.**   ISO 27001

**C.**   NIST CSF

**D.**   NIST-800-53

Images  **D**. As a service provider for the U.S. federal government, Jeffrey’s organization is required to adopt the NIST 800-53 controls framework.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because, although CIS is a high-quality controls framework, service providers that perform information-related services to the U.S. federal government are required to adopt the NIST 800-53 controls framework. **B** is incorrect because, although ISO 27001 is a high-quality information security controls framework, it is not required for service providers that provide services to agencies of the U.S. federal government. **C** is incorrect because, although NIST CSF (Cybersecurity Framework) is a good methodology for building an information security program, it is not a controls framework.

[**48**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q48)**.**   What is the scope of requirements of PCI-DSS?

**A.**   All systems that store, process, and transmit credit card numbers, as well as all other systems that can communicate with these systems

**B.**   All systems that store, process, and transmit credit card numbers

**C.**   All systems that store, process, and transmit unencrypted credit card numbers

**D.**   All systems in an organization where credit card numbers are stored, processed, and transmitted

Images  **A**. The systems that are in scope for PCI-DSS are all those that store, process, or transmit credit card numbers, as well as all other systems that can communicate with those systems.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because the scope of PCI-DSS is not limited to just those systems that store, process, or transmit credit card numbers, but also all other systems that can communicate with those systems. **C** is incorrect because the scope of PCI-DSS includes those systems that store, process, or transmit credit card numbers, even if encrypted. **D** is incorrect because the scope of PCI-DSS is not necessarily all systems in an organization where credit card numbers are stored, processed, or transmitted. If the organization has implemented effective network segmentation (that is, if systems that store, process, or transmit credit card numbers are isolated on subnets or VLANs where firewalls or ACLs have severely restricted communications to and from in-scope systems), then the systems not in the subnetworks or VLANs where credit card data resides are not in scope.

[**49**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q49)**.**   Which of the following statements is true about controls in the Payment Card Industry Data Security Standard?

**A.**   Many controls are required, while some are “addressable,” or optional, based on risk.

**B.**   All controls are required, regardless of actual risk.

**C.**   Controls that are required are determined for each organization by the acquiring bank.

**D.**   In addition to core controls, each credit card brand has its own unique controls.

Images  **B**. All controls are required for all organizations. There are additional controls required for service providers.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because no controls are optional. **C** is incorrect because acquiring banks do not make determinations of applicability of controls. **D** is incorrect because individual card brands do not impose additional controls. Individual card brands do, however, impose specific requirements for compliance reporting.

[**50**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q50)**.**   The PCI-DSS is an example of what?

**A.**   An industry regulation that is enforced with fines

**B.**   A private industry standard that is enforced with contracts

**C.**   A voluntary standard that, if used, can reduce cyber insurance premiums

**D.**   An international law enforced through treaties with member nations

Images  **B**. PCI-DSS was developed by a consortium of the major credit card brands in the world: Visa, MasterCard, American Express, Discover, and JCB. PCI is enforced through credit card brands’ operating rules, as well as by acquiring banks.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because PCI-DSS is not a law or regulation. **C** is incorrect because PCI-DSS is not voluntary for merchants and service providers that store, process, or transmit credit card numbers. Compliance with PCI-DSS may influence the cost of premiums for cyber-insurance premiums. **D** is incorrect because PCI-DSS is not an international law.

[**51**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q51)**.**   What are three factors that a risk manager may consider when developing an information security strategy?

**A.**   Threats, risks, and solutions

**B.**   Prevention, detection, and response

**C.**   Risk levels, staff qualifications, and security tooling

**D.**   Risk levels, operating costs, and compliance levels

Images  **D**. When developing a long-term strategy for an information security program, the best three factors are risk levels, operating costs, and compliance levels. One of these factors may be more important than others in any given organization and for a variety of reasons. Generally, a long-term strategy is being developed to improve the state of one of these: reduction of risk, reduction of cost, or improvement of compliance.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because this is not the best answer. These are factors that may be considered in some circumstances. **B** is incorrect because these are information security program capabilities. **C** is incorrect because this is not the best answer.

[**52**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q52)**.**   Jerome, a new CISO in a SaaS organization, has been asked to develop a long-term information security strategy. Which is the best first step for understanding the present state of the organization’s existing information security program?

**A.**   Perform a code review of the organization’s SaaS offerings.

**B.**   Study the contents of the risk register.

**C.**   Perform a baseline risk assessment.

**D.**   Commission a penetration test of internal and external networks.

Images  **C**. The best first step for understanding the current state of an organization’s information security program is to perform a comprehensive risk assessment. This is the best answer because a risk assessment takes the broadest assessment of the state of information risk, along with the state of any existing controls.

Images  **A**, **B**, and **D** are incorrect. **A** is incorrect because a code review is a consideration of a very narrow portion of the overall state of the organization’s information security program. At best, a code review will assess the state of the organization’s secure-by-design practices, as well as the effectiveness of safe development training for its developers. Virtually every other aspect of the organization’s information security program is ignored. **B** is incorrect because, although the risk register may indeed contain valuable information about many risks in the organization, it is not a good indicator of the state of existing security tooling and processes in the organization. Indeed, the risk register itself may be woefully incomplete, it may be out of date, or it may be inaccurate. **D** is incorrect because a penetration test provides a narrow viewpoint of the overall state of the organization’s information security program. Although a penetration test may be a good assessment of an organization’s vulnerability management and system hardening practices, it completely overlooks the majority of activities needed in today’s information security programs.

[**53**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q53)**.**   Jerome, a new CISO in a SaaS organization, has been asked to develop a long-term information security strategy. Why would Jerome choose to perform a threat assessment prior to producing the strategy?

**A.**   Ensure that the organization is aware of everything that could reasonably go wrong.

**B.**   Ensure that preventive controls are effective.

**C.**   Ensure that there are no unidentified vulnerabilities.

**D.**   Ensure that there are no unidentified risks.

Images  **A**. The purpose of a threat assessment is to identify and study internal and external threat scenarios involving key assets, including threats from any and all types of threat actors that can have the most significant impact to the organization based on the most likely scenarios that could reasonably occur.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because a threat assessment takes a different, and broader, view than preventive controls. For instance, it’s possible that there are reasonable threat scenarios for which no controls exist to reduce those threats’ impact or probability of occurrence. **C** is incorrect because a threat assessment does not take a vulnerability-centric approach. A threat assessment starts with threat actors and various scenarios. Once a threat assessment has been completed, the vulnerabilities can be identified and remediated. **D** is incorrect because this is not the best answer. Although it is true that a threat assessment’s role is to identify risks, a threat assessment does not identify all risks.

[**54**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q54)**.**   Jerome, a new CISO in a SaaS organization, has been asked to develop a long-term information security strategy. While examining the organization’s information security policy, and together with knowledge of the organization’s practices and controls, Jerome now realizes that the organization’s security policy is largely aspirational. What is the most important consequence of this on the organization?

**A.**   Confusion on the part of end users

**B.**   Appearance that the organization is not in control of its security practices

**C.**   Fines and sanctions from regulators

**D.**   Unmitigated risks and vulnerabilities

Images  **B**. An organization with a largely aspirational security policy (that is, the organization is not in compliance with most of its security policies) will have the appearance of not being in control of its practices. Were the organization to enter into cybersecurity-related legal proceedings in such a state, the organization’s information security policy would be a liability and would give the appearance that the organization does not take information security seriously.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because it is not the best answer. Though end users may indeed be confused by the dichotomy between stated policies and actual practices, this is an important consequence, but not the most important one. **C** is incorrect because it is not the best answer. There may be cases where fines may be levied by regulators because of an organization not being in compliance with its policies, but this is not the most important consequence. **D** is incorrect because it is not the best answer. It may, however, be true that the aspirational policy may result in unmitigated risks, but this is not the most important consequence.

[**55**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q55)**.**   Jerome, a new CISO in a SaaS organization, has been asked to develop a long-term information security strategy. While examining the organization’s information security policy, and together with knowledge of the organization’s practices and controls, Jerome now realizes that the organization’s security policy is largely aspirational. What is the best first step Jerome should take next?

**A.**   Create an entry in the organization’s risk register.

**B.**   Withdraw the security policy and write a new one that’s closer to reality.

**C.**   Perform a gap analysis and determine actions to take to close the policy gaps.

**D.**   Consult with the organization’s general counsel to develop a plan of action.

Images  **D**. Consulting counsel is the best first step. A security policy that is largely aspirational (meaning the organization is not in compliance with the majority of its policies) introduces legal liability upon the organization, which is best handled by the organization’s general counsel. Although a CISO is in the best position to describe the nature and type of gaps in an organization’s security policy, the precise course of action is best decided by the general counsel.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because this is not the best answer. Although putting an entry in the risk register is appropriate, this answer does not indicate the best substantial step to take. **B** is incorrect because withdrawing the information security policy would leave the organization in a state of having no information security policy at all. If an organization were to change its policy, it should keep the existing policy in place, then fully develop a new policy, and then “switch” the policies. **C** is incorrect, because this is not the best answer. This is, however, a step that may need to be taken so that the organization’s security policy may eventually be corrected.

[**56**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q56)**.**   Jerome, a new CISO in a SaaS organization, has identified a document that describes acceptable encryption protocols. What type of document is this?

**A.**   Policy

**B.**   Standard

**C.**   Practice

**D.**   Guideline

Images  **B**. A document that describes tools, products, or protocols is a standard.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because a policy would not typically specify tools or protocols. **C** is incorrect because a list of tools, products, or protocols is not a practice. **D** is incorrect because a guideline is a document that provides suggestions on the implementation of policies and standards.

[**57**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q57)**.**   Jerome, a new CISO in a SaaS organization, has identified a document that describes suggested techniques for implementing encryption protocols. What type of document is this?

**A.**   Policy

**B.**   Standard

**C.**   Guideline

**D.**   Procedure

Images  **C**. A document that provides suggestions on the implementation or use of a policy or standard is known as a guideline.

Images  **A**, **B**, and **D** are incorrect. **A** is incorrect because a policy document does not specify tools, techniques, protocols, or implementation guidance for any of these. **B** is incorrect because a standard is typically used to specify protocols to use, not how to implement them. **D** is incorrect because a procedure is a document that describes the steps to take to accomplish a task.

[**58**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q58)**.**   An organization is required by PCI to include several policies that are highly technical and not applicable to the majority of its employees. What is the best course of action for implementing these policies?

**A.**   Implement a technical security policy containing these required items, with a separate acceptable use policy for all workers.

**B.**   Incorporate all PCI-required policies in the organization’s information policy and let users figure out what is relevant to them.

**C.**   Include all PCI-related policies and indicate which are applicable to end users.

**D.**   Keep the PCI-related policies out of the overall security policy because it will confuse nontechnical end users.

Images  **A**. The best approach in an organization in scope for PCI is to segregate its policy content into separate documents: a technical or mandate-specific security policy document for technical workers that includes all PCI-related policies and a separate acceptable use policy (AUP) that contains security policy content for all end users.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because a bulky information security policy that contains numerous technical policies and technical jargon is not likely to be effective for end users, who would have trouble understanding much of it and who would fail to comply with the other policy statements applicable to them. **C** is incorrect because this is not the best answer. This approach, however, may be viable in organizations that desire to have all security policy content in a single document. It would be more complicated for end users to consume than a lightweight AUP written expressly for end users. **D** is incorrect because this approach is likely to cause the organization to fail to comply with PCI, which is explicit in its requirements for specific policies in an organization.

[**59**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q59)**.**   Which of the following is the most likely result of an organization that lacks a security architecture function?

**A.**   Inconsistent security-related procedures

**B.**   Inconsistent application of standards

**C.**   Lower process maturity

**D.**   Added complication in vulnerability management tools

Images  **B**. In an organization lacking a security architecture function, there is a greater likelihood that standards are going to be applied inconsistently. A security architecture function would likely include “reference architectures,” which are documents that define in detail how technology is implemented, configured, and even managed in an organization.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because, although inconsistent technology might also drive inconsistency in procedures, this is not the most direct result. **C** is incorrect because the lack of security architecture may or may not be a bellwether indicator of process maturity overall. **D** is incorrect because, although it may be true that lack of security architecture will result in complication in vulnerability management tools (because of inconsistencies in the environment), this is not the best answer.

[**60**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q60)**.**   What is the main advantage of a security architecture function in a larger, distributed organization?

**A.**   Greater employee satisfaction

**B.**   Better results in vulnerability assessments

**C.**   Greater consistency in the use of tools and configurations

**D.**   Lower cost of operations

Images  **C**. The main benefit of a security architecture is consistency in approach for all instances in the organization. For example, in a retail organization with dozens, hundreds, or thousands of locations, the use of a “reference architecture” as a part of a security architecture function would help ensure that equipment in all locations was configured identically. In another example, a reference architecture for access management would specify that SAML 2.0 would be used for single sign-on for all business applications. In the absence of a security architecture function, security tools and protocols might be inconsistently implemented and configured. Complexity is the enemy of security, it is said, and a large environment implemented inconsistently would be unnecessarily complex.

Images  **A**, **B**, and **D** are incorrect. **A** is incorrect because this is not the best answer. That said, employee satisfaction has little to do with security architecture, other than the consideration of engineers’ workloads in large environments that are inconsistent and unnecessarily complex. **B** is incorrect because this is not the best answer. However, in an environment with a security architecture function, it may be expected that vulnerability assessment results would be more consistent. **D** is incorrect because this is not the best answer. Still, in an environment that is highly consistent, there could be a somewhat lower cost incurred to operate it.

[**61**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q61)**.**   Which of the following statements about control frameworks is correct?

**A.**   Control frameworks are used only in regulated environments.

**B.**   All control frameworks are essentially the same, with different controls groups.

**C.**   It doesn’t matter which control framework is selected, as long as controls are operated effectively.

**D.**   Different control frameworks are associated with different industries.

Images  **D**. Different control frameworks are indeed associated with different industries. For instance, PCI controls are used in organizations that store, process, or transmit credit card information, and NIST 800-53 controls are used in U.S. federal government agencies and organizations that provide information services to those agencies.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because control frameworks are used in both regulated and unregulated environments. For example, many larger SaaS organizations use the ISO 27002 or NIST 800-53 control framework. **B** is incorrect because control frameworks can be said to be similar, but not identical, even when accounting for differences in their structure. **C** is incorrect because different control frameworks do have their differences, which in some cases could be significant.

[**62**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q62)**.**   Joel, a new CISO in an organization, has discovered that the server team applies security patches in response to the quarterly vulnerability scan reports created by the security team. What is the best process improvement Joel can introduce to this process?

**A.**   Server team proactively applies patches, and security scans confirm effective patching

**B.**   Server team proactively applies patches, and security scans confirm effective patching and identify other issues

**C.**   Security team increases the frequency of vulnerability scans from quarterly to monthly for internal scans and weekly for external scans

**D.**   Security team increases the frequency of vulnerability scans from quarterly to monthly

Images  **B**. The best improvement is the fundamental change from patching being reactive to being proactive and scanning serving as a QA to ensure that patching is working effectively. Further, security scanning can identify other issues besides patching—namely, security configuration problems as well as the presence of outdated or unsupported software.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because this is not the best answer. Scanning can identify not only missing security patches but also configuration problems and outdated software. **C** is incorrect because this answer still results in server patching that is reactive (to scan reports) instead of being proactive. The higher scan frequency in this answer is a needed improvement but not the best one. **D** is incorrect because this answer still results in server patching that is reactive (to scan reports) instead of being proactive. The higher scan frequency in this answer is a needed improvement but not the best one.

[**63**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q63)**.**   Which of the following is the best management-level metric for a vulnerability management process?

**A.**   Average time from availability of a patch to the successful application of a patch

**B.**   Average time from a vulnerability scan to the successful application of a patch

**C.**   Average time to apply a security patch successfully

**D.**   Number of security patches applied

Images  **A**. This is the most meaningful metric for management. This tells the story about how long servers are unprotected by security patches, which equates to exposure and risk of an intrusion and breach that pose potentially damaging impacts to the organization.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because this measures time from the vulnerability scan instead of from the time that the patch is available. **C** is incorrect because the time required to apply a patch has little relevance to the business. **D** is incorrect because the number of patches applied tells management little about the effectiveness of the process. This is, however, a potentially useful metric for measuring personnel workload.

[**64**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q64)**.**   A new CISO in a manufacturing company is gathering artifacts to understand the state of security in the organization. Which of the following would be the least valuable for determining risk posture?

**A.**   Security incident log

**B.**   Security awareness training records

**C.**   Penetration test results

**D.**   Report to the board of directors

Images  **D**. A report to the board of directors is the only one of the answers that represents secondary information that may have been filtered, edited, and/or biased. The other answers (security incident log, security awareness training records, and penetration test results) are more valuable records that are less subject to bias.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because a security incident log would be of particular value to a new CISO, particularly if this record contains data generated by a SIEM. **B** is incorrect because security awareness training records would indicate the degree of participation in security awareness training (itself an indicator of executive commitment to security awareness training and security overall), as well as competency test scores if they are a part of the record. **C** is incorrect because penetration test results are useful indicators of certain aspects of security in the organization. The number and type of vulnerabilities identified would be indicators of maturity in a secure systems development lifecycle (whether the penetration test targeted software applications or infrastructure) as well as the organization’s vulnerability management process.

[**65**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q65)**.**   Of what value is a business impact analysis (BIA) for a security leader in an organization?

**A.**   It provides a view of the criticality of IT systems in an organization.

**B.**   It provides a view of the criticality of business processes in an organization.

**C.**   It provides a view of the criticality of software applications in an organization.

**D.**   It provides no value to a security leader because it focuses on business continuity, not security.

Images  **B**. The purpose of a business impact analysis (BIA) is to provide a concise view of the criticality of business processes in an organization. From there, dependencies on information systems (that is, software applications and supporting infrastructure) can be determined.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because the primary purpose of a BIA is to determine critical business processes. The criticality of IT systems can be derived from a BIA after further analysis. **C** is incorrect because the primary purpose of a BIA is to determine critical business processes. The criticality of software applications can be derived from a BIA after further analysis. **D** is incorrect because the BIA does provide value to a security leader by indicating which business processes are most important in an organization. This knowledge has several benefits: it helps prioritize IT disaster recovery planning efforts, and it helps security understand which information systems warrant the most protection.

[**66**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q66)**.**   Samuel is the CISO in an organization that is a U.S. public company. Samuel has noted that the organization’s internal audit function concentrates its auditing efforts on “financially relevant” applications and underlying IT systems and infrastructure. As an experienced CISO, what conclusion can Samuel draw from this?

**A.**   The audits performed by internal audit on underlying IT systems and infrastructure are value-added activities.

**B.**   Internal audit’s scope is too narrow and must include all applications and IT systems.

**C.**   The scope of internal audit is of no consequence or value to the CISO.

**D.**   The scope of internal audit’s auditing activities is as expected for a U.S. public company.

Images  **D**. In a U.S. public company, an internal audit function is required to audit the financially relevant business processes and their supporting business applications and IT infrastructure to provide reasonable assurances about the integrity of financial reports produced by the organization to its shareholders. This is required because in 2002, Congress passed the Sarbanes-Oxley Act (SOX) to protect shareholders and the general public from accounting errors and fraudulent practices in enterprises and to improve the accuracy of corporate disclosures. The act sets deadlines for compliance and publishes rules on requirements.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because internal audits in a U.S. public company are required to audit the systems and infrastructures that support financially relevant business applications. This is not a value-added (not required) activity. **B** is incorrect because internal audit is not required to audit all of an organization’s applications and IT systems. However, in some organizations, internal audit’s scope surpasses what is required of U.S. public companies to provide assurances of the integrity of other processes and systems. **C** is incorrect because internal audit would be considered a business partner of a CISO in most organizations. This is because internal audit analyzes security controls in parts of IT, and this provides the CISO with valuable information on the effectiveness of at least some of the security controls in the organization.

[**67**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q67)**.**   Of what value is a third-party risk management (TPRM) process for a CISO who is developing a long-term security strategy for an organization?

**A.**   TPRM provides valuable insight into the security capabilities of critical service providers.

**B.**   TPRM provides valuable insight into the organization’s procurement process.

**C.**   TPRM provides a list of all service providers used by the organization.

**D.**   TPRM does not provide value to the CISO because it is concerned only with business processes.

Images  **A**. An effective TPRM program captures and archives detailed information about security controls in third-party service-provider organizations. This helps a CISO better understand the overall world of risk with regard to the protection of critical data and capabilities.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because TPRM provides little, if any, insight into procurement. This is because TPRM does not include activities such as competitive analysis, suitability of services, or pricing, which are among the matters of focus by procurement. **C** is incorrect because a TPRM process does not necessarily provide a list of all of an organization’s service providers. This is because individuals and groups may still procure low-cost or free services and “fly under the radar” of IT, security, legal, and procurement processes and put the organization at risk. **D** is incorrect because a TPRM process focuses on information security risk in third-party service-provider organizations, which is a high-value concern for a CISO.

[**68**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q68)**.**   Joseph, a new security leader in an online retail organization, is developing a long-term security strategy. Joseph has developed a detailed description of the future state of the security organization. What must Joseph do before developing a strategy to realize the future state?

**A.**   Perform an audit of existing security controls to understand their effectiveness.

**B.**   Understand the current state and perform a gap analysis to identify the differences.

**C.**   Perform a risk assessment to identify potential pitfalls in the strategy.

**D.**   Commission a penetration test to identify unknown vulnerabilities in critical systems.

Images  **B**. When developing a strategy, it is first necessary to develop the desired end state, understand the current state, and understand the gaps between the two. The strategy, then, will consist of work required to close those gaps, transforming the organization into the desired end state.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because, although it is important to perform audits of controls to understand their effectiveness, this question is focused on the proper method for developing a strategy: develop the desired end state, determine the current state, and perform a gap analysis to determine the work required to realize the end state. **C** is incorrect because, although it is important to perform risk assessments, this question is focused on the proper method for developing a strategy: develop the desired end state, determine the current state, and perform a gap analysis to determine the work required to realize the end state. **D** is incorrect because, although it is important to perform penetration tests to identify potentially critical vulnerabilities in information systems and applications, this question is focused on the proper method for developing a strategy: develop the desired end state, determine the current state, and perform a gap analysis to determine the work required to realize the end state.

[**69**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q69)**.**   Joseph, a new security leader in an online retail organization, is developing a long-term security strategy. In his research, Joseph is seeking documents describing the current security program. Which of the following documents would not provide the best value in this analysis?

**A.**   Security program charter

**B.**   Security team job descriptions

**C.**   Information security policy

**D.**   Meeting minutes for the cybersecurity steering committee

Images  **B**. Of these four sets of information, job descriptions for security team members would provide the least valuable insight. In part this is because workers’ regular activities sometimes stray away from statements in a job description. At best, a job description describes desired or expected activities at a point in time in the past.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because a security program charter would provide considerable insight into the mission and vision for an information security program. **C** is incorrect because an information security policy would provide insight into the security-related expectations in an organization. That said, a security leader would need to explore the policy further to determine the degree of compliance. **D** is incorrect because meeting minutes for a cybersecurity steering committee are of potentially high value to a security leader. This, of course, depends upon the purpose of the steering committee and the nature of its proceedings and decisions.

[**70**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q70)**.**   Quincy is a security leader who wants to formalize information security in his organization. What is the best first step to formalizing the program?

**A.**   Start an information security intranet site.

**B.**   Start an information security newsletter.

**C.**   Develop an information security policy.

**D.**   Develop an information security program charter.

Images  **D**. An information security program charter describes the mission and vision for an information security program, defines roles and responsibilities, and describes its engagement with others in the organization as well as external parties such as customers or regulators.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because, although an intranet site can help others in the organization be better informed about the information security program, a charter is the best choice. **B** is incorrect because, although a newsletter can help others in the organization be better informed about the information security program, a charter is the best choice. **C** is incorrect because an organization needs to have an information security policy, whether its information security program is formal or not.

[**71**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q71)**.**   Ravila, a security leader, has assessed the maturity of the information security capabilities in the organization using the CMMI model. The average maturity of business processes in the organization is 3.2. What should Ravila do next?

**A.**   Compare the current maturity levels to desired maturity levels and develop a strategy to achieve desired levels.

**B.**   Determine the steps necessary to raise process maturity to 5.

**C.**   Identify the processes with the lowest maturity and develop a strategy to raise them to the level of other processes.

**D.**   Perform a root cause analysis (RCA) to determine why business process maturity has fallen to this level.

Images  **A**. The best answer here is to determine any gaps between current and future maturity levels so that any processes needing improvement can be improved and measured.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because level 5 is not necessarily a realistic goal for maturity in an organization. An average maturity between 2.5 and 4 is acceptable and appropriate in many organizations. **C** is incorrect because it is normal and acceptable for some processes to have lower maturity levels than others. **D** is incorrect because there is no indication here that the maturity of any processes has declined. RCA, however, may be a reasonable activity to undertake if the maturity of a specific process has declined in order to understand how to mitigate it.

[**72**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q72)**.**   An organization’s security leader, together with members of its information security steering committee, has decided to require that all encryption of data at rest must use AES-256 or better encryption. The organization needs to update what document?

**A.**   Policies

**B.**   Standards

**C.**   Guidelines

**D.**   Systems

Images  **B**. A standards document is the correct type of document for identifying specific protocols, configurations, and algorithms for use in an organization.

Images  **A**, **C**, and **D** are incorrect. **A** is incorrect because a policy should not include details such as protocols, configurations, and algorithms for use in an organization. Instead, a standard should be used. **C** is incorrect because a guideline is generally considered a suggestion for implementation of a policy or standard, but it does not carry the rule of law that is needed in this case. **D** is incorrect because, although it may be true that the organization needs to update some information systems to align with this recent decision, the best answer here is that the organization must first update its standards.

[**73**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q73)**.**   A security leader has been asked to justify the need to implement a new strategy for information security. How should the security leader respond?

**A.**   Develop a project plan showing the personnel, tasks, timelines, and dependencies.

**B.**   Develop a risk matrix that includes the potential consequences if the strategy is not implemented.

**C.**   Develop a SWOT diagram showing strengths, weaknesses, opportunities, and threats.

**D.**   Develop a business case that includes success criteria, requirements, costs, and action plan.

Images  **D**. A business case is the best method for justifying a project or initiative to support the company’s strategy. A well-formed business case includes a problem statement, current and desired states, resources required, requirements, a plan, and success criteria.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because a project plan is not designed to justify the need for a strategy. Instead, a project plan is used to document how a plan will be executed and by whom. **B** is incorrect because a risk matrix is not designed to justify the need for a strategy. It may, however, be useful to understand the risks involved in current and desired future states. **C** is incorrect because a SWOT (strengths, weaknesses, opportunities, and threats) diagram is not used to justify a strategy.

[**74**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch2.xhtml#ch2q74)**.**   What is the purpose of obtaining management commitment in support of a strategy?

**A.**   Improved enforcement of policy

**B.**   Approval for new hires

**C.**   Visible support to reinforce the importance of the strategy

**D.**   Approval of spending

Images  **C**. Management commitment in the form of messaging, availability of resources, and leadership by example/actions helps the organization achieve its strategies.

Images  **A**, **B**, and **D** are incorrect. **A** is incorrect because enforcement of policy is not a primary purpose of management commitment. **B** is incorrect because approval for new hires is only a part of what is needed for a successful strategy. **D** is incorrect because approval for spending is only a part of what is needed for a successful strategy.