Q QUESTIONS

[**1**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa1)**.**   Ravila is a new CISO in a healthcare organization. During strategy development, Ravila found that IT system administrators apply security patches when the security team sends them quarterly vulnerability scan reports. What is the most effective change that can be made in the vulnerability management process to make it more proactive versus reactive?

**A.**   Have IT system administrators run vulnerability scans on their own systems.

**B.**   No change is needed because this process is already working properly.

**C.**   Revise the patching process to ensure patches are applied on a defined process schedule based on the risk of the vulnerability. Leverage the quarterly scanning process as a QA.

**D.**   Run vulnerability scan reports monthly instead of quarterly.

[**2**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa2)**.**   An organization has outsourced most of its business applications and IT operations to software as a service (SaaS) providers and other service providers. Currently, the organization has no master list of service providers. Instead, IT, legal, procurement, and security have separate lists that are not in alignment. What is the first step that should take place?

**A.**   Implement a cloud access security broker (CASB) system to discover what other services providers are in use.

**B.**   Create a master list of service providers from the lists from IT, legal, procurement, and security.

**C.**   Develop a policy that requires that the security team assess all new service providers.

**D.**   Develop a policy that requires the legal team review all contracts with all new service providers.

[**3**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa3)**.**   An organization’s CISO is planning for the cybersecurity budget for the following year. One of the security analysts informed the CISO that she should add more licenses to the vulnerability scanning tool so that all of the organization’s networks can be scanned; currently, there are only enough licenses to scan the primary on-premises data center, but not the secondary data center, office networks, or external-facing assets. How should the CISO respond to this request?

**A.**   Acquire licenses for all internal and external networks.

**B.**   No additional licenses are needed, since only the data center network needs to be scanned.

**C.**   No additional licenses are needed, because the scanner can scan all networks but will not maintain records for them because of license limitations.

**D.**   Acquire licenses for the secondary data center.

[**4**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa4)**.**   A global manufacturing organization has decided to develop a SaaS solution in support of one of its products. What security-related resources will need to be acquired in support of this new endeavor?

**A.**   Functional requirements, source code control system, and IDEs

**B.**   Secure coding training, web content scanning tools, and a web application firewall

**C.**   Secure coding training, DAST and SAST tools, and a web application firewall

**D.**   Secure coding training, web application scanning tools, and a web application firewall

[**5**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa5)**.**   An organization has decided to improve its information security program by developing a full suite of policies, procedures, standards, and processes. Which of these must be developed first?

**A.**   Procedures

**B.**   Standards

**C.**   Processes

**D.**   Policies

[**6**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa6)**.**   What kind of statement is the following: “Passwords are to consist of upper- and lowercase letters, numbers, and symbols, and are to be at least 12 characters in length.”

**A.**   Standard

**B.**   Policy

**C.**   Guideline

**D.**   Procedure

[**7**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa7)**.**   What is the purpose of developing security awareness content in various forms?

**A.**   To provide unexpected messages that users are less likely to notice

**B.**   To maximize the value of security awareness training content licensing

**C.**   To relieve personnel of boredom from only one form of messaging

**D.**   In recognition that different people have different learning and cognition styles

[**8**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa8)**.**   The CISO in a venture capital firm wants the firm’s acquisition process to include a cybersecurity risk assessment prior to the acquisition of a new company, not after the acquisition, as has been done in the past. What is the best reason for this change?

**A.**   To discover compliance risks prior to the acquisition

**B.**   To discover cybersecurity-related risks that may impact the valuation of the company

**C.**   To get a head start on understanding risks that should be remediated

**D.**   To understand cybersecurity-related risks prior to connecting networks together

[**9**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa9)**.**   What is the purpose of sending security questionnaires to third parties at the start of the due diligence process?

**A.**   To determine the firewall rules required to connect to a third party

**B.**   To determine which controls need to be added or changed

**C.**   To address risks during contract negotiations

**D.**   To register the third party with regulatory authorities

[**10**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa10)**.**   A CISO has developed and is publishing a new metric entitled, “Percentage of patches applied within SLAs to servers supporting manufacturing.” What message does this metric convey to executives?

**A.**   The risk associated with SLAs and whether they are too long

**B.**   The amount of downtime in manufacturing while patches are being applied

**C.**   The amount of effort used to apply security patches to servers

**D.**   The risk of security incidents that could disrupt manufacturing operations

[**11**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa11)**.**   Which of the following reports is most appropriate to send to a board of directors?

**A.**   Quarterly high-level metrics and a list of security incidents

**B.**   Weekly detailed metrics

**C.**   Weekly detailed metrics and vulnerability scan reports

**D.**   Vulnerability scan reports and a list of security incidents

[**12**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa12)**.**   What is the best solution for protecting an SaaS application from a layer 7 attack?

**A.**   Advanced malware protection

**B.**   Cloud access security broker

**C.**   Web content filter

**D.**   Web application firewall

[**13**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa13)**.**   An organization’s CISO has examined statistics and metrics and has determined that the organization’s software development organization is producing a growing number of serious security vulnerabilities. What new control would be most effective at ensuring that production systems are free of these vulnerabilities?

**A.**   Implement an intrusion prevention system.

**B.**   Implement a web application firewall.

**C.**   Perform a security scan during the software build process and require that no critical or high-level vulnerabilities exist in software released to production.

**D.**   Administer secure code training to all developers once per year.

[**14**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa14)**.**   How does an acceptable use policy differ from an information security policy?

**A.**   They differ in name only; they are functionally the same.

**B.**   An acceptable use policy defines expected behavior from workers, while an information security policy details all of the business rules for cybersecurity.

**C.**   An information security policy defines expected behavior from workers, while an acceptable use policy details all of the business rules for cybersecurity.

**D.**   An acceptable use policy applies to nontechnical workers only, while an information security policy applies only to technical workers.

[**15**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa15)**.**   What is the name of the self-attestation that U.S.-based companies can use to express their compliance with the General Data Protection Regulation?

**A.**   Binding corporate rules

**B.**   Model clauses

**C.**   Safe Harbor

**D.**   Privacy Shield

[**16**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa16)**.**   What is the name of the provision that multinational organizations can adopt for the protection of PII of its internal personnel?

**A.**   Binding corporate rules

**B.**   Model clauses

**C.**   Safe Harbor

**D.**   Privacy Shield

[**17**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa17)**.**   What is the most effective way of ensuring that personnel are aware of an organization’s security policies?

**A.**   Require personnel to acknowledge compliance to security policies in writing annually.

**B.**   Require personnel to acknowledge compliance to security policies at the time of hire.

**C.**   Post information security policies on the organization’s intranet.

**D.**   Distribute hard copies of information security policies to all personnel.

[**18**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa18)**.**   Which certification is recognized for knowledge and experience on the examination of information systems and on information system protection?

**A.**   CGEIT

**B.**   CRISC

**C.**   CISA

**D.**   CISSP

[**19**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa19)**.**   What is the best method for determining whether employees understand an organization’s information security policy?

**A.**   Require employees to acknowledge information security policy in writing.

**B.**   Incorporate quizzes into security awareness training.

**C.**   Require employees to read the information security policy.

**D.**   Distribute copies of the information security policy to employees.

[**20**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa20)**.**   An access management process includes an access request procedure, an access review procedure, and an access termination procedure. In the access request procedure, an employee submits an access request; it is approved by the application owner, and it is provisioned by the IT service desk. Which party should periodically review access requests to ensure that records are complete and that accesses were properly provisioned?

**A.**   IT service desk

**B.**   Internal audit

**C.**   Application owner

**D.**   Employee’s manager

[**21**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa21)**.**   When is the best time for the legal department to review a contract with a third-party service provider?

**A.**   After a security questionnaire has been completed by the service provider

**B.**   At the start of the procurement process

**C.**   At the vendor selection stage

**D.**   Before a security questionnaire has been sent to the service provider

[**22**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa22)**.**   What aspects of security access reviews would best be reported to senior management?

**A.**   Number of accounts reviewed in security access reviews

**B.**   Number of security access reviews completed

**C.**   Number of security access reviews performed

**D.**   Number of exceptions identified during security access reviews

[**23**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa23)**.**   In an audit of the user account deprovisioning process for a financial application, three out of ten randomly selected samples indicated that user accounts were not terminated within the 24-hour control limit. How should the audit proceed from this point?

**A.**   Publish audit findings and declare the control as ineffective.

**B.**   Select another sample of ten records and publish audit findings based on the twenty samples.

**C.**   Test all remaining termination requests to see if more were missed.

**D.**   Publish audit findings and declare the control as effective.

[**24**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa24)**.**   The board of directors in a manufacturing company has asked for a report from the CISO that describes the state of the organization’s cybersecurity program. Which of the following is the best way for the CISO to fulfill this request?

**A.**   Meet with the board at its next scheduled meeting, provide a state of the state for the cybersecurity program, and answer questions by board members.

**B.**   Send the most recent penetration test to the board members.

**C.**   Send the most recent risk assessment to the board members.

**D.**   Send the risk register to the board members.

[**25**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa25)**.**   One of the objectives in the long-term strategy for an organization’s information security program states that a concerted effort at improving software development will be undertaken. Which of the following approaches will be *least* effective at reaching this objective?

**A.**   Enact financial compensation incentives for developers based on reductions in security defects.

**B.**   Implement web application firewalls (WAFs) and intrusion prevention systems (IPSs) to protect applications from attack.

**C.**   Enact a policy stating that new software release packages cannot be released until critical and high-level vulnerabilities are remediated.

**D.**   Provide mandatory secure development training for all software developers.

[**26**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa26)**.**   The human resources arm of a large multinational company is planning to consolidate its HR information systems (HRIS) onto a single platform. How can the information security function align its strategy to this development?

**A.**   Contractors and temporary workers can be managed in the new global HRIS.

**B.**   Workers in all countries can acknowledge compliance with the information security policy.

**C.**   Workers in all countries can be enrolled in security awareness training.

**D.**   The identity and access management function can be integrated with the new global HRIS.

[**27**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa27)**.**   The CISO in a 1000-employee organization wants to implement a 24/7/365 security monitoring function. There is currently no 24/7 IT operations in the organization. What is the best option for the CISO to implement a 24/7/365 security monitoring function?

**A.**   Outsource security monitoring to a managed security services provider (MSSP) that specializes in security event monitoring.

**B.**   Staff up a 24/7/365 IT operations and security event monitoring function with permanent full-time staff.

**C.**   Staff up a 24/7/365 security event monitoring function with permanent full-time staff.

**D.**   Implement a security event monitoring platform and have events sent to existing 5x8 staff (a staff that works five days a week for eight hours per day) after hours.

[**28**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa28)**.**   Which of the following is the best regimen for managing security policy content?

**A.**   Develop policy that aligns with ISO, NIST, or CSC, and review annually.

**B.**   Develop policy that aligns with known standards and the business; review annually and when the organization undergoes significant changes.

**C.**   Outsource policy development to a consulting firm; have the consulting firm review annually according to industry changes.

**D.**   Develop policy that aligns with known standards and the business.

[**29**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa29)**.**   What is the most effective way to confirm overall compliance with security policy?

**A.**   Perform penetration tests of key systems and applications, and scan source code if applicable.

**B.**   Review test scores from security awareness training quizzes.

**C.**   Circulate questionnaires to process owners and ask them to attach evidence.

**D.**   Interview process owners and examine business records.

[**30**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa30)**.**   What is the purpose of phishing testing?

**A.**   Determine whether phishing messages can bypass phishing controls

**B.**   Determine whether the links in phishing messages can be confirmed

**C.**   Determine how many personnel can be tricked by phishing messages

**D.**   Determine how many actual phishing messages bypass antiphishing defenses

[**31**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa31)**.**   How are security requirements integrated into disaster recovery plans?

**A.**   Security requirements and controls are a part of the foundation of DR plans and capabilities.

**B.**   Management selects the most important security controls and requirements to be a part of DR.

**C.**   The purpose of DR is different from cybersecurity and the two are not related.

**D.**   Only those controls required by law are a part of DR plans and capabilities.

[**32**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa32)**.**   A security team has performed a risk assessment of a third-party service provider that hosts the organization’s financial accounting system. The risk assessment has identified some critical risks. How should the security team and its leader respond?

**A.**   Discuss the matter with the service provider to see what mitigations can be implemented.

**B.**   Enact controls to mitigate the critical risks.

**C.**   Negotiate a new agreement with the service provider.

**D.**   Select a different service provider based on the absence of these risks.

[**33**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa33)**.**   A new CISO in a manufacturing company has developed statistics and metrics on the industrial control systems supporting automated manufacturing and has found that more than one-third of the operating systems are many years out of support because the ICS software does not support newer versions of operating systems and newer versions of ICS software are not available. What is the best response in this situation?

**A.**   Switch to software vendors that provide modern, supported operating systems.

**B.**   Upgrade operating systems and install backward-compatible libraries.

**C.**   Virtualize outdated operating systems.

**D.**   Isolate ICS systems in hardened networks.

[**34**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa34)**.**   A new CISO in a manufacturing company has developed statistics and metrics on the industrial control systems supporting automated manufacturing and has found that more than one-third of the operating systems are many years out of support because the ICS software does not support newer versions of operating systems and newer versions of ICS software are not available. How should this situation be described to senior management?

**A.**   The organization needs to step up and modernize its industrial control systems.

**B.**   The organization needs to isolate and protect its industrial control systems.

**C.**   The organization needs to require its ICS vendors to support modern operating systems.

**D.**   The organization needs to outsource its ICS to an ICS cloud provider.

[**35**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa35)**.**   Which of the following is the best language for a security policy in a multinational software organization regarding background checks?

**A.**   Prior to hire, all employees must undergo background investigations where permitted by law.

**B.**   Prior to hire, all workers, whether they are employees, contractors, or consultants, must undergo background investigations.

**C.**   Prior to hire, all workers, whether they are employees, contractors, or consultants, must undergo background investigations where permitted by law.

**D.**   Prior to hire and annually thereafter, all employees must undergo background investigations.

[**36**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa36)**.**   What is the best time to identify security and privacy requirements in a project to identify and evaluate a software service provider?

**A.**   Just prior to implementation

**B.**   At the same time that business functional requirements are identified

**C.**   Post-implementation after the first penetration test

**D.**   Post-implementation before the first penetration test

[**37**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa37)**.**   What is the primary reason for discontinuing the use of SMS for two-factor authentication?

**A.**   SMS messages can be easily spoofed.

**B.**   SIM switching attacks can cause SMS messages to be sent elsewhere.

**C.**   SMS messages are not encrypted in transit.

**D.**   One-time passwords sent via SMS do not prove physical possession of a trusted device.

[**38**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa38)**.**   An organization recently experienced a security incident in which an employee leaked vital information via an unapproved cloud-based storage provider. The employee stated that she “did not know” that it was against policy to store company data in unapproved cloud-based services. What is the best administrative control to prevent this type of event in the future?

**A.**   Require employees to acknowledge compliance to security policy annually in writing.

**B.**   Implement a CASB system.

**C.**   Implement endpoint-based DLP.

**D.**   Implement a GPO to block the use of USB mass storage devices.

[**39**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa39)**.**   An organization recently experienced a security incident in which an employee leaked vital information via an unapproved cloud-based storage provider. The employee stated that she “did not know” that it was against policy to store company data in unapproved cloud-based services. What is the best automatic control to prevent this type of event in the future?

**A.**   Require employees to acknowledge compliance to security policy annually in writing.

**B.**   Implement a CASB system.

**C.**   Implement endpoint-based DLP.

**D.**   Implement a GPO to block the use of USB mass storage devices.

[**40**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa40)**.**   What control can best improve software security in a software as a service organization that currently undergoes quarterly penetration tests of its SaaS software?

**A.**   SAST scans as a part of the software build process

**B.**   Monthly penetration tests

**C.**   Mandatory secure development training for all developers

**D.**   Daily web application scans of the production environment

[**41**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa41)**.**   Which of the following is the best source for system and component hardening standards?

**A.**   Microsoft

**B.**   NIST

**C.**   SANS

**D.**   The Center for Internet Security

[**42**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa42)**.**   Which of the following is the best vulnerability management process?

**A.**   Proactive patching and hardening according to SLAs, and security scanning as a QA activity

**B.**   Security scanning reports initiate patching and hardening according to SLAs

**C.**   Proactive patching according to SLAs, and security scanning as a QA activity

**D.**   Security scanning reports initiate patching according to SLAs

[**43**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa43)**.**   An existing healthcare organization is developing a first-ever system and device hardening program and has chosen CIS Benchmarks as their industry standard. What is the best method for implementing CIS Benchmarks in server operating systems in production environments?

**A.**   Implement CIS Benchmark configurations all at once in test environments, and then in production environments.

**B.**   Implement CIS Benchmark configurations slowly in test environments, and then in production environments.

**C.**   Implement CIS Benchmark configurations all at once in production environments.

**D.**   Implement CIS Benchmark configurations slowly in production environments.

[**44**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa44)**.**   What is the best use for requiring security certifications when screening candidates for a security director position in a midsized financial services organization?

**A.**   Require CISSP or CISM, or similar certifications.

**B.**   Desire CISSP or CISM, and relevant experience.

**C.**   Require CISSP and CISM.

**D.**   Require CISSP or CISM, as well as an advanced degree.

[**45**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa45)**.**   What is the best advantage of implementing smaller units of security awareness training quarterly as opposed to all-at-once training annually?

**A.**   More straightforward recordkeeping for compliance purposes

**B.**   Less disruption to workers in an organization

**C.**   Decreased license costs from security awareness training content providers

**D.**   Keeping the topic of information security current through more frequent training

[**46**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa46)**.**   What is the purpose of periodically assessing risks at a third-party service provider?

**A.**   Periodic assessment of third parties is required by the PCI-DSS.

**B.**   Assessing a third party is wise when the business relationship changes or increases.

**C.**   Assessment helps with detection of changes in risk that may not have existed at the start of the third-party relationship.

**D.**   Assessment determines the need to perform penetration tests of specific third-party service providers.

[**47**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa47)**.**   In large organizations, what is the best technique for incorporating cybersecurity-related language into contracts with third-party service providers?

**A.**   Develop custom legal terms for each service provider based on questionnaires.

**B.**   Develop custom legal terms for each service provider based on risk.

**C.**   Develop templates of legal terms for various types of service providers.

**D.**   Develop templates of legal terms for various types of service providers, and tailor them as needed.

[**48**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa48)**.**   The security leader in an organization learned about a security breach at a strategic service provider that provides data storage services. What first step should the security leader take regarding the relationship with the service provider?

**A.**   Examine the agreement to see what the service provider’s obligations are.

**B.**   Terminate the contract if there is a breach exit clause.

**C.**   Request a copy of the security incident from the service provider.

**D.**   Perform a penetration test of the service provider’s service endpoints.

[**49**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa49)**.**   How could a statistic about security scanning be transformed into a metric meaningful to senior management?

**A.**   Avoid the use of technical jargon.

**B.**   Express the metric in business terms and potential business outcomes.

**C.**   Show the metric on an easily viewed dashboard.

**D.**   Describe the statistic in an executive summary narrative.

[**50**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa50)**.**   Which of the following is the best method for testing the following control: “Only authorized persons may approve user access requests”?

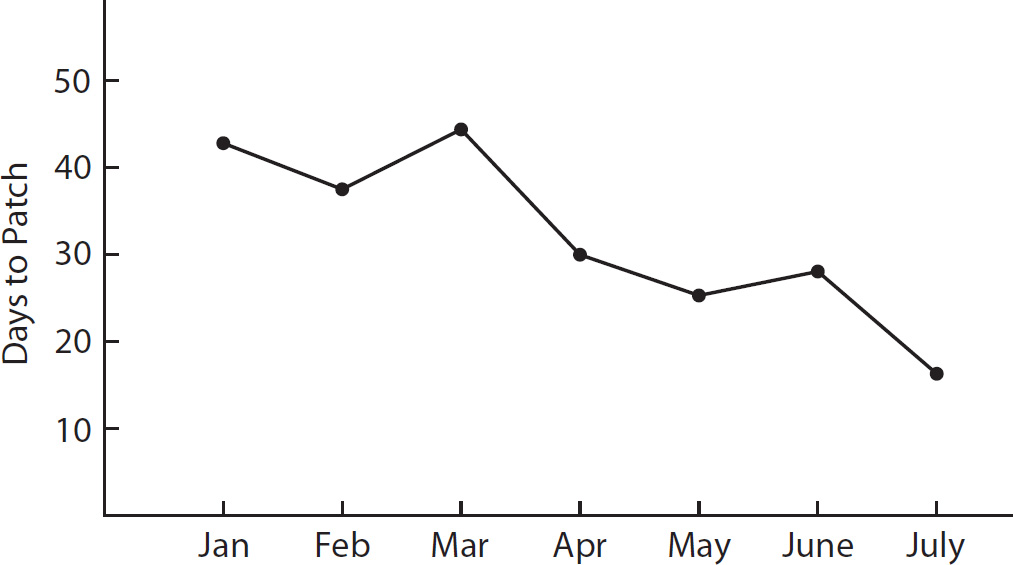
**A.**   Make some dummy access requests and see who approves them.

**B.**   Interview at least two process SMEs and review business records.

**C.**   Interview process owners and ask who the approvers are.

**D.**   Review business records and see who approved access requests.

[**51**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa51)**.**   What does the following vulnerability management dashboard indicate to management?



**A.**   It takes more days to patch systems.

**B.**   It takes fewer days to patch systems.

**C.**   Risk is increasing over time.

**D.**   Risk is decreasing over time.

[**52**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa52)**.**   In an organization’s information security program, one of the strategy statements reads, “Improve security awareness outreach to company workers.” Which activities would best support this objective?

**A.**   Scan end-user workstations more frequently.

**B.**   Raise the minimum score required to complete security awareness training successfully.

**C.**   Publish a quarterly newsletter with security tips and articles.

**D.**   All of these are correct.

[**53**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa53)**.**   A company’s IT organization has decided to implement a single sign-on (SSO) portal in the coming year. What are the most important security-related considerations that should be included in advance planning for the SSO portal?

**A.**   SAML integration with applications

**B.**   Password quality and password reset

**C.**   Multifactor authentication

**D.**   HMAC integration

[**54**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa54)**.**   All of the following are advantages to outsourcing an IS audit function, *except* which one?

**A.**   Avoidance of hiring and retaining talent

**B.**   Cost savings of contractors versus full-time employees

**C.**   No need to find onsite workspace

**D.**   Cost savings for training and professional development

[**55**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa55)**.**   What is the best approach to the development of an organization’s security incident response plan?

**A.**   Developing separate security incident recordkeeping

**B.**   Developing a general IR plan and leaving the details to subject matter experts

**C.**   Developing detailed playbooks and relying on the organization’s crisis management plan

**D.**   Leveraging the organization’s crisis management plan

[**56**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa56)**.**   Which of the following statements about guidelines is correct?

**A.**   Guidelines are mandatory.

**B.**   Guidelines are optional and not required.

**C.**   Security policies are derived from guidelines.

**D.**   Security controls are derived from guidelines.

[**57**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa57)**.**   What is the purpose of a security awareness program?

**A.**   Helps personnel understand proper computer usage

**B.**   Informs personnel about security policy

**C.**   Helps personnel develop better judgment when handling company information

**D.**   Meets compliance requirements for PCI-DSS and SOX

[**58**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa58)**.**   What is meant by the term “move to the left” in the context of information security and systems development?

**A.**   Introduce security earlier in the development lifecycle.

**B.**   Introduce security later in the development lifecycle.

**C.**   Remediate security flaws more slowly.

**D.**   Remediate security flaws more quickly.

[**59**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa59)**.**   An online retail organization accepts credit card payments and is therefore required to comply with PCI-DSS. Which of the following statements is correct regarding the organization’s service providers that have access to the organization’s credit card payment information?

**A.**   The organization is required to verify each service provider’s PCI-DSS compliance annually.

**B.**   The organization is required to verify each service provider’s PCI-DSS compliance status annually.

**C.**   The organization is required to assess each service provider’s PCI-DSS compliance annually.

**D.**   The organization is required to verify each service provider’s PCI-DSS compliance quarterly.

[**60**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa60)**.**   An organization performs phishing testing on a monthly basis. Over the past year, the average of click-through rates has changed from 42 percent to 14 percent. What conclusion can be drawn from this trend?

**A.**   End users are more likely to click on actual phishing messages.

**B.**   Phishing messages are more likely to reach end users’ inboxes.

**C.**   End users are less likely to click on actual phishing messages.

**D.**   Phishing messages are less likely to reach end users’ inboxes.

[**61**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa61)**.**   Which of the following is the best approach for a “state of the security program” for the board of directors?

**A.**   Executive summary and details from an enterprise risk assessment

**B.**   Executive summary portion of an enterprise risk assessment

**C.**   Detailed workbook containing statistics and metrics for the past 12 months

**D.**   Short slide deck showing key risk indicators, accomplishments, and incidents

[**62**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa62)**.**   An organization has hired a new CISO to make strategic improvements to the information security program. As one of her first important tasks, the new CISO is going to write a program charter document that describes the organization’s security program, key roles and responsibilities, primary business processes, and relationships with key business stakeholders and external parties. What is the best approach to producing this charter document?

**A.**   Develop the charter document based upon ISO/IEC 27001.

**B.**   First identify and interview key business stakeholders to understand their cyber-risk needs and concerns.

**C.**   Develop the charter document based upon information security best practices.

**D.**   Develop the charter document based upon industry-sector best practices.

[**63**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa63)**.**   Approximately how many personnel would need to be identified to fully staff a 24/7/365 SOC, which can ensure shift coverage even during vacation and sick time?

**A.**   12

**B.**   3

**C.**   9

**D.**   24

[**64**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa64)**.**   What is the best approach for implementation of a DLP system in an organization’s e-mail environment?

**A.**   Develop a data classification policy, and implement active controls.

**B.**   Develop a data classification policy, train users, and perform scans of unstructured data stores.

**C.**   Develop a data classification policy, train users, and implement active controls.

**D.**   Develop a data classification policy, train users, and implement passive controls.

[**65**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa65)**.**   An organization has experienced numerous instances of unintended data exfiltration via its corporate e-mail system. All of the following approaches for solving this problem are valid *except* which one?

**A.**   Warn users who are sending e-mail to external recipients so they can double-check recipients.

**B.**   Automatically encrypt attachments in outgoing messages to external recipients.

**C.**   Disable e-mail recipient auto-complete.

**D.**   Warn users who are sending e-mail with attachments to external recipients so they can double-check recipients.

[**66**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa66)**.**   During the organization’s annual goal-setting session, the CISO was asked first to describe the security program’s goals for the new year. Why would the CISO prefer to wait until later?

**A.**   The CISO is unprepared and needs more time to establish goals.

**B.**   The CISO needs to know what goals the CIO will set before describing security goals.

**C.**   The CISO wants to get ideas from others so that security goals will be more credible.

**D.**   The CISO first needs to understand the organization’s overall goals, as well as those of business leaders.

[**67**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa67)**.**   The statement, “Passwords can be constructed from words, phrases, numbers, and special characters in a variety of ways that are easily remembered but not easily guessed,” is an example of what?

**A.**   A guideline

**B.**   A standard

**C.**   A policy

**D.**   A procedure

[**68**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa68)**.**   Which of the following statements is correct about PCI-DSS audits?

**A.**   An organization with a PCI-ISA (internal security assessor) does not have to undergo external PCI-DSS audits.

**B.**   An organization can be compliant with PCI-DSS if it completes the audit and has project plans for noncompliant controls.

**C.**   An organization must have all PCI-DSS controls in place to be compliant with PCI-DSS.

**D.**   An organization must complete a PCI-DSS audit to be compliant with PCI-DSS.

[**69**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa69)**.**   Which of the following is the most effective means for making information security policies, standards, and guidelines available to an organization’s workforce?

**A.**   Policies, standards, and guidelines should be on a “need to know” basis and not published or sent to personnel.

**B.**   Publish policies, standards, and guidelines on an intranet site where they can be easily found.

**C.**   E-mail policies, standards, and guidelines to the workforce once per year.

**D.**   Publish policies, standards, and guidelines in hard copy and have copies available at the security office.

[**70**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa70)**.**   What is the best approach in most organizations for ensuring that cybersecurity personnel remain current in their knowledge and skills?

**A.**   Security personnel can study on their own and do not require support from the organization.

**B.**   Build a library of books on various security topics that security personnel can check out and read.

**C.**   Provide at least one month of formal training per year.

**D.**   Provide at least one week of formal training per year.

[**71**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa71)**.**   In an organization with an established security culture, some personnel complain about the time required to undergo the annual eight-hour security awareness training, claiming that they are already proficient in the subject matter and that the organization would benefit more from their continuing their work duties. What is the best approach to address this matter?

**A.**   Permit personnel to skip security awareness training topics if they first pass tests on those topics.

**B.**   Permit those personnel to skip security awareness training.

**C.**   Permit personnel to skip security awareness training if they achieved good test scores in previous years.

**D.**   Require all personnel to undergo training because it is required by policy.

[**72**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa72)**.**   An organization undergoes quarterly phishing testing to see how proficient its workforce is in detecting phishing messages. What is the best approach to take for individuals who fail to detect test phishing messages and click on their contents?

**A.**   Post their names on a “wall of shame” as a way of ensuring that personnel work harder to detect phishing messages properly.

**B.**   Require that they undergo reinforcement training.

**C.**   Remove their access privileges for a period of time.

**D.**   Require that they write a short essay on the risk of phishing messages.

[**73**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa73)**.**   An organization is required, via a legal agreement, to perform account activity reviews. Which of the following best defines an account activity review?

**A.**   A review to see how many changes to users’ accounts are performed during a time period

**B.**   A review to see how frequently users log in to their accounts

**C.**   A review to see how busy users are when they log in to their accounts

**D.**   A review to see whether users have logged in to their accounts during a specific time period

[**74**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa74)**.**   A particular organization is a financial software as a service (SaaS) provider in the financial services industry. Many of the organization’s customers claim that they have a regulatory requirement to conduct audits of the SaaS provider. What remedy is available to the SaaS provider to minimize or eliminate these customer audits?

**A.**   Undertake an annual SOC2 Type 2 audit.

**B.**   Undertake an annual SOC2 Type 1 audit.

**C.**   Undertake an annual SOC1 Type 2 audit of relevant controls.

**D.**   Undertake an annual SOC1 Type 1 audit of relevant controls.

[**75**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa75)**.**   An organization provides training content to corporate customers via a SaaS platform. Because the organization’s SaaS platform includes some sensitive information about its customers, some of the customers want to perform audits of the SaaS organization. What can the SaaS organization do to reduce the number of such audit requests?

**A.**   Undergo an annual penetration test of its SaaS application.

**B.**   Undergo an annual penetration test of its infrastructure.

**C.**   Undergo an annual SOC2 Type 1 audit.

**D.**   Undergo an annual SOC2 Type 2 audit.

[**76**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa76)**.**   A CISO is turning her attention to the organization’s third-party risk management process, which has risk classification tiers into which each third party is classified. The CISO is concerned with “scope creep” among its third parties. In this context, what does this mean?

**A.**   Third parties that, over time, provide additional services that should elevate them into higher-risk tiers

**B.**   Third parties whose security programs degrade over time

**C.**   Third parties that outsource more and more of their operations to fourth parties

**D.**   Third parties that improve their security programs over time

[**77**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa77)**.**   Of what value are metrics about dropped packets on firewalls?

**A.**   These metrics are a measure of security breaches that have been avoided.

**B.**   These metrics are of operational value only.

**C.**   These metrics are a measure of DDoS attacks that have been blocked.

**D.**   These metrics are of no value.

[**78**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa78)**.**   When in an audit is it acceptable to use a sample instead of an entire population?

**A.**   When the entire population is too large to test

**B.**   When automation is in place to ensure consistency

**C.**   When logging is in place to measure results

**D.**   When alerting is in place to notify personnel of exceptions

[**79**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa79)**.**   An audit of a privileged user account has turned up a high number of exceptions from the sample. What is the appropriate next step?

**A.**   Notify management that there has been a breach.

**B.**   Stop the audit.

**C.**   Select additional samples.

**D.**   Complete the audit report.

[**80**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4sa80)**.**   James, a CISO in a software company, is preparing a report for the board of directors prior to an upcoming board meeting. What is the best method for James to deliver this report to board members?

**A.**   E-mail the report to board members.

**B.**   Orally deliver the report to the board members during the board meeting.

**C.**   Provide hard copies of the report to board members during the board meeting discussion.

**D.**   Securely send the report to board members in advance of the board meeting, and then review and discuss the report at the board meeting.

|  |  |  |  |
| --- | --- | --- | --- |
| [**1**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa1)**.**   C  [**2**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa2)**.**   B  [**3**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa3)**.**   A  [**4**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa4)**.**   C  [**5**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa5)**.**   D  [**6**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa6)**.**   A  [**7**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa7)**.**   D  [**8**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa8)**.**   B  [**9**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa9)**.**   C  [**10**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa10)**.**   D  [**11**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa11)**.**   A  [**12**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa12)**.**   D  [**13**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa13)**.**   C  [**14**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa14)**.**   B  [**15**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa15)**.**   D  [**16**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa16)**.**   A  [**17**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa17)**.**   A  [**18**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa18)**.**   C  [**19**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa19)**.**   B  [**20**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa20)**.**   B | [**21**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa21)**.**   A  [**22**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa22)**.**   D  [**23**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa23)**.**   C  [**24**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa24)**.**   C  [**25**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa25)**.**   B  [**26**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa26)**.**   D  [**27**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa27)**.**   A  [**28**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa28)**.**   B  [**29**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa29)**.**   D  [**30**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa30)**.**   C  [**31**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa31)**.**   A  [**32**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa32)**.**   A  [**33**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa33)**.**   D  [**34**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa34)**.**   B  [**35**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa35)**.**   C  [**36**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa36)**.**   B  [**37**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa37)**.**   D  [**38**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa38)**.**   A  [**39**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa39)**.**   B  [**40**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa40)**.**   A | [**41**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa41)**.**   D  [**42**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa42)**.**   A  [**43**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa43)**.**   B  [**44**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa44)**.**   B  [**45**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa45)**.**   D  [**46**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa46)**.**   C  [**47**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa47)**.**   D  [**48**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa48)**.**   A  [**49**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa49)**.**   B  [**50**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa50)**.**   B  [**51**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa51)**.**   D  [**52**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa52)**.**   C  [**53**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa53)**.**   A  [**54**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa54)**.**   B  [**55**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa55)**.**   D  [**56**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa56)**.**   B  [**57**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa57)**.**   C  [**58**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa58)**.**   A  [**59**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa59)**.**   B  [**60**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa60)**.**   C | [**61**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa61)**.**   D  [**62**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa62)**.**   B  [**63**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa63)**.**   A  [**64**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa64)**.**   D  [**65**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa65)**.**   B  [**66**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa66)**.**   D  [**67**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa67)**.**   A  [**68**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa68)**.**   C  [**69**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa69)**.**   B  [**70**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa70)**.**   D  [**71**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa71)**.**   A  [**72**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa72)**.**   B  [**73**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa73)**.**   D  [**74**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa74)**.**   C  [**75**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa75)**.**   D  [**76**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa76)**.**   A  [**77**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa77)**.**   B  [**78**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa78)**.**   A  [**79**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa79)**.**   C  [**80**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4qa80)**.**   D |

QUICK ANSWER KEY

ANSW

ERS A

[**1**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q1)**.**   Ravila is a new CISO in a healthcare organization. During strategy development, Ravila found that IT system administrators apply security patches when the security team sends them quarterly vulnerability scan reports. What is the most effective change that can be made in the vulnerability management process to make it more proactive versus reactive?

**A.**   Have IT system administrators run vulnerability scans on their own systems.

**B.**   No change is needed because this process is already working properly.

**C.**   Revise the patching process to ensure patches are applied on a defined process schedule based on the risk of the vulnerability. Leverage the quarterly scanning process as a QA.

**D.**   Run vulnerability scan reports monthly instead of quarterly.

Images  **C**. In an effective vulnerability management process, engineers proactively apply security patches and other configuration changes according to a process that may include analysis of new available patches, as well as a regimen of testing to ensure that patches do not introduce new problems. Then vulnerability scans serve as a QA (quality assurance) check to ensure that all systems and devices are configured and patched within established timelines.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because this change does not get at the root of the problem of IT system administrators patching only when they are given a scan report. **B** is incorrect because the vulnerability management process as described is not working properly but is reactive instead. **D** is incorrect because patching will still be reactive, although this still may result in security patches being applied earlier. This option would reduce risk but is not the best answer.

[**2**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q2)**.**   An organization has outsourced most of its business applications and IT operations to software as a service (SaaS) providers and other service providers. Currently, the organization has no master list of service providers. Instead, IT, legal, procurement, and security have separate lists that are not in alignment. What is the first step that should take place?

**A.**   Implement a cloud access security broker (CASB) system to discover what other services providers are in use.

**B.**   Create a master list of service providers from the lists from IT, legal, procurement, and security.

**C.**   Develop a policy that requires that the security team assess all new service providers.

**D.**   Develop a policy that requires the legal team review all contracts with all new service providers.

Images  **B**. The best first step is to create a master list of all known service providers that combines information available from legal (because they manage contracts), IT (because they manage network connections), procurement (because they acquire new vendors and service provider relationships), and security (because they manage or audit firewalls). Many other steps need to follow so that the organization will have a sound third-party management program that ensures that all stakeholders (IT, legal, procurement, security, and possibly others) are involved and can perform their functions as needed.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because this is not the best available answer. However, implementing a CASB or similar capability will provide information about additional service providers that may be used. **C** and **D** are incorrect because neither is the best next step. However, the organization will need to develop policy and a process regarding the use of third-party service providers. The best first step is one of discovery, through the combining of lists of service providers.

[**3**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q3)**.**   An organization’s CISO is planning for the cybersecurity budget for the following year. One of the security analysts informed the CISO that she should add more licenses to the vulnerability scanning tool so that all of the organization’s networks can be scanned; currently, there are only enough licenses to scan the primary on-premises data center, but not the secondary data center, office networks, or external-facing assets. How should the CISO respond to this request?

**A.**   Acquire licenses for all internal and external networks.

**B.**   No additional licenses are needed, since only the data center network needs to be scanned.

**C.**   No additional licenses are needed, because the scanner can scan all networks but will not maintain records for them because of license limitations.

**D.**   Acquire licenses for the secondary data center.

Images  **A**. The CISO should expand licensing for the vulnerability scanning tool to include all internal and external networks. Many vulnerability scanning tools maintain databases that track the history of vulnerabilities for each asset; expanding licensing to include all networks will enable this feature to be used.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because licenses should be increased to include all internal and external networks and not just the primary data center. **C** is incorrect because the licensing limitation will mean that reconfiguring the scanning tool to scan various internal networks will destroy valuable scanning and remediation history, depriving the security team of the history of scans, vulnerabilities, and remediation for every asset. **D** is incorrect because the addition of the secondary data center, though a move in the right direction, is insufficient; the scanning tool should be licensed to scan all assets in all internal and external networks.

[**4**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q4)**.**   A global manufacturing organization has decided to develop a SaaS solution in support of one of its products. What security-related resources will need to be acquired in support of this new endeavor?

**A.**   Functional requirements, source code control system, and IDEs

**B.**   Secure coding training, web content scanning tools, and a web application firewall

**C.**   Secure coding training, DAST and SAST tools, and a web application firewall

**D.**   Secure coding training, web application scanning tools, and a web application firewall

Images  **C**. To support security-related needs of the new SaaS endeavor, the organization needs to acquire secure coding training for its developers, dynamic application scanning tools (DAST) and static application scanning tools (SAST) to discover security defects in its software, and a web application firewall to block layer 7 attacks on its SaaS system. Different organizations will need different combinations of security tools and capabilities, depending upon several factors not addressed in this question.

Images  **A**, **B**, and **D** are incorrect. **A** is incorrect because these items are not security-related resources. **B** is incorrect because web content scanning tools are used to prevent internal users from the hazards encountered when visiting websites with their browsers, not for protecting web applications. **D** is incorrect because this is not the best available answer.

[**5**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q5)**.**   An organization has decided to improve its information security program by developing a full suite of policies, procedures, standards, and processes. Which of these must be developed first?

**A.**   Procedures

**B.**   Standards

**C.**   Processes

**D.**   Policies

Images  **D**. Policies, which are business rules governing behavior in an organization, should be developed first. Then, processes and procedures that align with policy can be developed next. Standards, which specify how policies are to be implemented, can be developed alongside processes and procedures. Next, guidelines, which offer suggestions on the implementation of policies and standards, can be developed.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because procedures should not be created until policies are first developed, followed by processes. **B** is incorrect because standards should not be created until policies are first developed. **C** is incorrect because processes should not be developed until policies are in place.

[**6**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q6)**.**   What kind of statement is the following: “Passwords are to consist of upper- and lowercase letters, numbers, and symbols, and are to be at least 12 characters in length.”

**A.**   Standard

**B.**   Policy

**C.**   Guideline

**D.**   Procedure

Images  **A**. The statement is a standard. Detailed specifications on any topic should appear in a standard, not in a policy.

Images  **B**, **C**, and **D** are incorrect. **B** is incorrect because the statement is too detailed to be a policy. **C** is incorrect because a guideline on passwords would offer suggestions and ideas on the topic of “good” passwords. **D** is incorrect because the statement is not a step-by-step procedure, but instead a list of configuration specifications.

[**7**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q7)**.**   What is the purpose of developing security awareness content in various forms?

**A.**   To provide unexpected messages that users are less likely to notice

**B.**   To maximize the value of security awareness training content licensing

**C.**   To relieve personnel of boredom from only one form of messaging

**D.**   In recognition that different people have different learning and cognition styles

Images  **D**. The most effective security awareness training programs include content in various forms (including but not limited to computer-based training, newsletters, e-mail messages, poster, flyers, and promotional items) in recognition of the fact that people have different learning and cognition styles. Workers are more likely to be receptive to messages when they appear in different forms.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because security awareness training is not trying to surprise people or send unexpected messages; it is intended to keep the topic of a secure culture on the minds of workers through a variety of messages. **B** is incorrect because a variety of media types and product licenses have little, if anything, to do with one another. **C** is incorrect because creating messages in a variety of different forms is an attempt to reach people in the most effective way, not to relieve their boredom.

[**8**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q8)**.**   The CISO in a venture capital firm wants the firm’s acquisition process to include a cybersecurity risk assessment prior to the acquisition of a new company, not after the acquisition, as has been done in the past. What is the best reason for this change?

**A.**   To discover compliance risks prior to the acquisition

**B.**   To discover cybersecurity-related risks that may impact the valuation of the company

**C.**   To get a head start on understanding risks that should be remediated

**D.**   To understand cybersecurity-related risks prior to connecting networks together

Images  **B**. The identification of cybersecurity-related risks prior to the acquisition of a company will, at times, affect the true value of the company being acquired. For instance, if serious vulnerabilities were identified and evidence of a breach was discovered, this would have significant impact on the value of the company.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because, although compliance risks would be useful to know, this is not the best answer. **C** is incorrect because this is not the best answer. **D** is incorrect because venture capital firms do not typically connect their networks to companies they acquire. But even if they do, this is still not the best available answer.

[**9**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q9)**.**   What is the purpose of sending security questionnaires to third parties at the start of the due diligence process?

**A.**   To determine the firewall rules required to connect to a third party

**B.**   To determine which controls need to be added or changed

**C.**   To address risks during contract negotiations

**D.**   To register the third party with regulatory authorities

Images  **C**. The purpose of sending a questionnaire to a third-party service provider early in the process is to understand the risks involved that would be related to a business relationship with a third party. Better organizations send questionnaires not just to the selected third party, but to other candidate third parties, to help the business make a sound selection that takes cyber risks into account. By sending out questionnaires early, any issues identified can be addressed during contract negotiations.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because the determination of firewall rules is a minor matter that can be addressed during the onboarding process. **B** is incorrect because this is not the best answer, even though it may be necessary to make changes to the control environment based upon a third party, the services it provides, and any risks that have been identified through questionnaires and other means. **D** is incorrect because only in narrow circumstances does an organization need to register the use of a third party with regulatory authorities.

[**10**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q10)**.**   A CISO has developed and is publishing a new metric entitled, “Percentage of patches applied within SLAs to servers supporting manufacturing.” What message does this metric convey to executives?

**A.**   The risk associated with SLAs and whether they are too long

**B.**   The amount of downtime in manufacturing while patches are being applied

**C.**   The amount of effort used to apply security patches to servers

**D.**   The risk of security incidents that could disrupt manufacturing operations

Images  **D**. The metric in this case helps management understand the risk of a security incident or breach. If the percentage trends down, it’s taking longer for servers to get patched, which means an intrusion and potential disruptions to manufacturing would be more likely to occur.

Images  **A**, **B**, and **C** are incorrect. **A** is incorrect because this metric does not address the risk with the SLA itself, but with the organization’s performance to the SLA. **B** is incorrect because the metric does not directly reveal any downtime information. **C** is incorrect because the amount of effort to patch servers is not revealed by this metric.

[**11**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q11)**.**   Which of the following reports is most appropriate to send to a board of directors?

**A.**   Quarterly high-level metrics and a list of security incidents

**B.**   Weekly detailed metrics

**C.**   Weekly detailed metrics and vulnerability scan reports

**D.**   Vulnerability scan reports and a list of security incidents

Images  **A**. A board of directors is going to be interested in high-level information about a security program, usually in summary form.

Images  **B**, **C**, and **D**are incorrect. **B** and **C** are incorrect because weekly detailed metrics are far too detailed and voluminous for consumption by a board of directors. **D** is incorrect because a board of directors is not going to be interested in vulnerability scan reports.

[**12**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q12)**.**   What is the best solution for protecting an SaaS application from a layer 7 attack?

**A.**   Advanced malware protection

**B.**   Cloud access security broker

**C.**   Web content filter

**D.**   Web application firewall

Images  **D**. A web application firewall is the best solution for protecting an SaaS application from layer 7 attacks such as script injection, buffer overflow, and reflected cross-site scripting.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because advanced malware protection is a solution used on endpoints to detect and block exploits from malware. **B** is incorrect because a cloud access security broker (CASB) does not protect web applications from threats. Instead, a CASB is used to control end users’ access to Internet web sites in order to manage the use of external service providers and control sensitive content. **C** is incorrect because a web content filter is a solution used to protect endpoints from malicious websites and to control the categories of websites that users are permitted to visit.

[**13**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q13)**.**   An organization’s CISO has examined statistics and metrics and has determined that the organization’s software development organization is producing a growing number of serious security vulnerabilities. What new control would be most effective at ensuring that production systems are free of these vulnerabilities?

**A.**   Implement an intrusion prevention system.

**B.**   Implement a web application firewall.

**C.**   Perform a security scan during the software build process and require that no critical or high-level vulnerabilities exist in software released to production.

**D.**   Administer secure code training to all developers once per year.

Images  **C**. Control and remediation of security-related software defects is not a simple undertaking. Performing vulnerability scans during a nightly build process will identify any new vulnerabilities. Requiring that software releases contain no critical or high-level vulnerabilities can be a successful control, particularly if it is measured to see how effective it is. This control works only when both of these mechanisms are implemented: scans during nightly builds will inform developers of defects, and the control permitting no release of critical or high-level vulnerabilities is achievable because the nightly scans inform them of vulnerabilities that must be fixed.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because, although an intrusion prevention system (IPS) may be at least partially effective at protecting applications, the question asks what controls will result in the application being free of serious vulnerabilities. **B** is incorrect because a web application firewall may be effective in protecting applications, but the question asks what controls will result in the application being free of serious vulnerabilities. **D** is incorrect because, although secure code training may help reduce the number of new security-related software defects over time, it will not have an immediate effect on existing vulnerabilities.

[**14**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q14)**.**   How does an acceptable use policy differ from an information security policy?

**A.**   They differ in name only; they are functionally the same.

**B.**   An acceptable use policy defines expected behavior from workers, while an information security policy details all of the business rules for cybersecurity.

**C.**   An information security policy defines expected behavior from workers, while an acceptable use policy details all of the business rules for cybersecurity.

**D.**   An acceptable use policy applies to nontechnical workers only, while an information security policy applies only to technical workers.

Images  **B**. An acceptable use policy (AUP) defines expected behavior for all workers in an organization. An information security policy, which also applies to everyone, defines cybersecurity-related business rules on many topics, including some that are not relevant to nontechnical workers (for example, policy on secure software development).

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because an acceptable use policy and an information security policy are distinctly different from one another. **C** is incorrect because the definitions are reversed. **D** is incorrect because an AUP applies to all workers, while an information security policy generally applies only to technical workers.

[**15**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q15)**.**   What is the name of the self-attestation that U.S.-based companies can use to express their compliance with the General Data Protection Regulation?

**A.**   Binding corporate rules

**B.**   Model clauses

**C.**   Safe Harbor

**D.**   Privacy Shield

Images  **D**. Privacy Shield is used by U.S.-based organizations that choose to self-attest their compliance to GDPR.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because binding corporate rules are used in multinational organizations’ compliance to GDPR for the protection of internally transferred PII, which is typically HR information about its internal employees. **B** is incorrect because model clauses are contract language used among organizations to hold one another accountable to GDPR. **C** is incorrect because Safe Harbor is no longer in use.

[**16**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q16)**.**   What is the name of the provision that multinational organizations can adopt for the protection of PII of its internal personnel?

**A.**   Binding corporate rules

**B.**   Model clauses

**C.**   Safe Harbor

**D.**   Privacy Shield

Images  **A**. Binding corporate rules are the provisions used by multinational organizations for ensuring privacy protections for internally transferred PII. Generally, this is limited to PII of internal personnel.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because model clauses are contract language to be used among organizations to hold one another accountable to GDPR. **C** is incorrect because Safe Harbor was used for a different purpose. **D** is incorrect because Privacy Shield is used for a different purpose.

[**17**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q17)**.**   What is the most effective way of ensuring that personnel are aware of an organization’s security policies?

**A.**   Require personnel to acknowledge compliance to security policies in writing annually.

**B.**   Require personnel to acknowledge compliance to security policies at the time of hire.

**C.**   Post information security policies on the organization’s intranet.

**D.**   Distribute hard copies of information security policies to all personnel.

Images  **A**. Requiring annual written acknowledgement of security policies is the best choice here. Better still is requiring written acknowledgement at the time of hire AND annually thereafter.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because new workers are often overwhelmed with a lot of information at the time of hire, and there is a possibility they will not recall this acknowledgment, particularly when it is not required ever again. **C** is incorrect because posting security policies on an intranet site does not ensure that personnel will be aware of them. **D** is incorrect because there is no assurance that personnel will read or understand security policies; further, the absence of written acknowledgment may mean that workers will not take the policies seriously.

[**18**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q18)**.**   Which certification is recognized for knowledge and experience on the examination of information systems and on information system protection?

**A.**   CGEIT

**B.**   CRISC

**C.**   CISA

**D.**   CISSP

Images  **C**. CISA, or Certified Information Systems Auditor, is recognized for its requirement for experience in information systems audit and information systems protection.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because CGEIT (Certified in the Governance of Enterprise IT) is not related to information systems audit or protection. **B** is incorrect because CRISC (Certified in Risk and Information Systems Control) is related to risk management. **D** is incorrect because CISSP (Certified Information Systems Security Professional) is a general-purpose security certification.

[**19**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q19)**.**   What is the best method for determining whether employees understand an organization’s information security policy?

**A.**   Require employees to acknowledge information security policy in writing.

**B.**   Incorporate quizzes into security awareness training.

**C.**   Require employees to read the information security policy.

**D.**   Distribute copies of the information security policy to employees.

Images  **B**. Incorporating quizzes into security awareness training establishes a record of employees’ knowledge about information security policy and acceptable use policy, particularly when quiz scores are retained for each employee. Quizzes help to reinforce learning, and they also deter nonrepudiation: an employee who violated policy cannot later claim they did not remember their security awareness training when confronted with records showing they correctly answered questions about policy.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because requiring employees to acknowledge information security policy in writing does not mean they read, understood, or retained knowledge about the contents of the policy. **C** is incorrect because requiring employees to read the policy does not ensure they will retain the information. **D** is incorrect because distributing hard copies to employees does not ensure that they will read or retain knowledge about it.

[**20**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q20)**.**   An access management process includes an access request procedure, an access review procedure, and an access termination procedure. In the access request procedure, an employee submits an access request; it is approved by the application owner, and it is provisioned by the IT service desk. Which party should periodically review access requests to ensure that records are complete and that accesses were properly provisioned?

**A.**   IT service desk

**B.**   Internal audit

**C.**   Application owner

**D.**   Employee’s manager

Images  **B**. Internal audit is the best party to perform the access review.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because the IT service desk would be reviewing its own work, and this would represent a conflict of interest. **C** is incorrect, although the application owner may want to participate in such a review. **D** is incorrect, because employees’ managers could be numerous, and they may not be in a position to review accesses if they are unfamiliar with business processes associated with the system being reviewed.

[**21**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q21)**.**   When is the best time for the legal department to review a contract with a third-party service provider?

**A.**   After a security questionnaire has been completed by the service provider

**B.**   At the start of the procurement process

**C.**   At the vendor selection stage

**D.**   Before a security questionnaire has been sent to the service provider

Images  **A**. The best time for the legal department to perform contract review is after a service provider has completed and returned a security questionnaire. Any issues identified in the questionnaire can be mitigated during contract negotiations. For example, if the service provider says that they do not undergo penetration testing, the contract can require the service provider to start undergoing periodic penetration tests.

Images  **B**, **C**, and **D**are incorrect. **B** and **C** are incorrect because there is insufficient information available at these early stages in the process. **D** is incorrect because if the contract is finalized before a security questionnaire is completed and returned by a service provider, it will be too late to address any issues identified in the questionnaire.

[**22**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q22)**.**   What aspects of security access reviews would best be reported to senior management?

**A.**   Number of accounts reviewed in security access reviews

**B.**   Number of security access reviews completed

**C.**   Number of security access reviews performed

**D.**   Number of exceptions identified during security access reviews

Images  **D**. The number of exceptions identified during security access reviews is the best operational metric to report to senior management. This metric provides an indication of the quality of the access request and provisioning process. A higher number of exceptions would indicate that personnel are either violating business rules or not paying attention to detail. A low number of exceptions would indicate that employees understand and follow the rules and are paying attention to their work.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because the number of accounts reviewed provides little insight into how well the access request and provisioning process is performing and whether controls are effective. **B** and **C** are incorrect because the number of reviews performed and completed also provides little insight into the effectiveness of the access request and provisioning process.

[**23**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q23)**.**   In an audit of the user account deprovisioning process for a financial application, three out of ten randomly selected samples indicated that user accounts were not terminated within the 24-hour control limit. How should the audit proceed from this point?

**A.**   Publish audit findings and declare the control as ineffective.

**B.**   Select another sample of ten records and publish audit findings based on the twenty samples.

**C.**   Test all remaining termination requests to see if more were missed.

**D.**   Publish audit findings and declare the control as effective.

Images  **C**. With three out of ten samples failing, this important control is clearly ineffective. Because of the importance of the user account deprovisioning process, it’s not enough to publish audit results at this point; instead, all records must be examined so that a more thorough understanding of the control failure can be determined and to deprovision all accounts that were missed.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because this is not the best course of action. Although it is true that the control is ineffective, all remaining records should be examined better to understand why the control is in such a poor state of effectiveness. **B** is incorrect because this is not the best course of action. Although pulling another sample will help the auditor better understand what has happened, the gravity of the situation calls for more drastic action—namely the examination of all records. **D** is incorrect because the control is not effective. This option is the worst course of action because a determination that this control is effective is wrong.

[**24**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q24)**.**   The board of directors in a manufacturing company has asked for a report from the CISO that describes the state of the organization’s cybersecurity program. Which of the following is the best way for the CISO to fulfill this request?

**A.**   Meet with the board at its next scheduled meeting, provide a state of the state for the cybersecurity program, and answer questions by board members.

**B.**   Send the most recent penetration test to the board members.

**C.**   Send the most recent risk assessment to the board members.

**D.**   Send the risk register to the board members.

Images  **C**. The best available option is for the CISO to send the most recent risk assessment. That said, none of the four options is entirely adequate. A better response by the CISO would be to send a report containing some key risk indicators (KRIs), a list of significant security incidents (if any), and short narratives on recent accomplishments and future projects.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because the board asked for a report, not simply airtime with the CISO in their meeting. The board wants something to read that explains the state of security in the organization. **B** is incorrect because a penetration test is not appropriate content for a board of directors: it’s too detailed and too narrow in focus. **D** is incorrect because the contents of the risk register will not tell the board enough about what is going on. This would be a good second choice, however.

[**25**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q25)**.**   One of the objectives in the long-term strategy for an organization’s information security program states that a concerted effort at improving software development will be undertaken. Which of the following approaches will be *least* effective at reaching this objective?

**A.**   Enact financial compensation incentives for developers based on reductions in security defects.

**B.**   Implement web application firewalls (WAFs) and intrusion prevention systems (IPSs) to protect applications from attack.

**C.**   Enact a policy stating that new software release packages cannot be released until critical and high-level vulnerabilities are remediated.

**D.**   Provide mandatory secure development training for all software developers.

Images  **B**. While implementing a WAF and an IPS to protect applications from attack will be effective at reducing the probability and impact of layer 7 attacks, this approach is least effective and only serves to cover up what could be sloppy development practices with regard to the reduction of security defects.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because financial incentives, when implemented correctly, can be a powerful means for helping a development organization focus on the reduction of security defects. **C** is incorrect because a policy forbidding the release of software containing critical and high-level security defects can help reduce the number of exploitable defects in production applications. **D** is incorrect because secure development training can help developers better understand how to avoid producing security defects in their code.

[**26**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q26)**.**   The human resources arm of a large multinational company is planning to consolidate its HR information systems (HRIS) onto a single platform. How can the information security function align its strategy to this development?

**A.**   Contractors and temporary workers can be managed in the new global HRIS.

**B.**   Workers in all countries can acknowledge compliance with the information security policy.

**C.**   Workers in all countries can be enrolled in security awareness training.

**D.**   The identity and access management function can be integrated with the new global HRIS.

Images  **D**. The best alignment opportunity lies in the potential to integrate the new global HRIS to the organization’s identity and access management platform. Although this may be a challenge in an organization with many identity systems and many HRISs, the consolidation to single platforms should greatly simplify identity and access management processes and technologies.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because the organization may already be managing contractors and temporary workers in some or all of its HRIS platforms. Many organizations’ HR departments resist having anything to do with contractors and temporary workers, but better organizations’ HR departments fully embrace their mission to manage information for all workers, regardless of employment status (full time, part time, contractor, consultant, temporary worker, and so on). **B** is incorrect because acknowledgement of compliance to policies, while important, is a minor consideration. **C** is incorrect because the management of security awareness training, while important, is not as important an opportunity as is the alignment of a global HRIS platform with a global identity and access management platform.

[**27**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q27)**.**   The CISO in a 1000-employee organization wants to implement a 24/7/365 security monitoring function. There is currently no 24/7 IT operations in the organization. What is the best option for the CISO to implement a 24/7/365 security monitoring function?

**A.**   Outsource security monitoring to a managed security services provider (MSSP) that specializes in security event monitoring.

**B.**   Staff up a 24/7/365 IT operations and security event monitoring function with permanent full-time staff.

**C.**   Staff up a 24/7/365 security event monitoring function with permanent full-time staff.

**D.**   Implement a security event monitoring platform and have events sent to existing 5x8 staff (a staff that works five days a week for eight hours per day) after hours.

Images  **A**. The CISO’s best option is to outsource security event monitoring to an MSSP. The main advantage of an MSSP is cost: an MSSP’s fees for 24/7/365 monitoring will be a fraction of the cost of hiring and equipping a full-time staff capable of fully covering 21 shifts per week with coverage for vacation, sick days, and training.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because staffing an IT and security monitoring function is cost-prohibitive compared to outsourcing IT and security ops to an MSSP. **C** is incorrect because staffing and equipping a 24/7/365 security event monitoring function is cost-prohibitive. **D** is incorrect because alerts reaching 5x8 staff at night and on weekends will bring out fatigue, burnout, and turnover.

[**28**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q28)**.**   Which of the following is the best regimen for managing security policy content?

**A.**   Develop policy that aligns with ISO, NIST, or CSC, and review annually.

**B.**   Develop policy that aligns with known standards and the business; review annually and when the organization undergoes significant changes.

**C.**   Outsource policy development to a consulting firm; have the consulting firm review annually according to industry changes.

**D.**   Develop policy that aligns with known standards and the business.

Images  **B**. The best initial security policy is one that harmonizes with the organization and is structured on an appropriate standard such as ISO 27001, NIST 800-53, CSC 20, or another relevant standard. Policy should be reviewed at least annually and approved by management. If the organization undergoes significant changes, policy should be reviewed and altered at that time if needed.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because this choice does not state that policy needs to align with the business, nor does it state the need for policy to be reviewed when the organization undergoes significant changes. **C** is incorrect because, although outsourcing policy development can be a good move if the organization doesn’t have that expertise in house, this choice states that the outsourced firm should perform the review; even if an organization outsources the initial creation of its security policy, the organization itself should perform the annual review. If the firm lacks someone with sufficient experience to conduct the review, the outsourced firm can facilitate a review with representatives from the organization. **D** is incorrect because this choice lacks an annual review as well as a review when significant changes occur in the business.

[**29**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q29)**.**   What is the most effective way to confirm overall compliance with security policy?

**A.**   Perform penetration tests of key systems and applications, and scan source code if applicable.

**B.**   Review test scores from security awareness training quizzes.

**C.**   Circulate questionnaires to process owners and ask them to attach evidence.

**D.**   Interview process owners and examine business records.

Images  **D**. The most effective way to confirm compliance to security policy is to perform audits of controls: interview control owners, examine process documents, and look over business records and other evidence. And because resources are often limited, it’s common for an organization to audit the higher-risk controls rather than all controls.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because penetration tests and code reviews will measure only a small portion of an organization’s overall policy—and perhaps not even its most important parts! **B** is incorrect because test scores from security awareness training reveal only the workers’ understanding of policy, not whether policies are being carried out. **C** is incorrect because questionnaires and evidence are not an effective means for gathering information about processes. However, for a risk-based approach, it would be appropriate to interview control owners for the highest-risk controls and to use questionnaires and requests for evidence for low-risk controls.

[**30**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q30)**.**   What is the purpose of phishing testing?

**A.**   Determine whether phishing messages can bypass phishing controls

**B.**   Determine whether the links in phishing messages can be confirmed

**C.**   Determine how many personnel can be tricked by phishing messages

**D.**   Determine how many actual phishing messages bypass antiphishing defenses

Images  **C**. The purpose of phishing testing is to determine what proportion of the workforce is potentially susceptible to actual phishing campaigns. Phishing testing consists of the creation of e-mail messages that resemble phishing messages and are released into the workforce. Typically, phishing testing tools track each user’s response to test phishing messages and gather statistics on the percentage of the workforce that is successfully tricked by these test phishing messages. In a proper security awareness program, the results of phishing testing help management understand the effectiveness of end-user training on recognizing actual phishing messages and responding appropriately.

Images  **A**, **B**, and **D**are incorrect. The purpose of phishing test messages is not to bypass phishing controls, determine whether links are confirmable, or to test antiphishing defenses.

[**31**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q31)**.**   How are security requirements integrated into disaster recovery plans?

**A.**   Security requirements and controls are a part of the foundation of DR plans and capabilities.

**B.**   Management selects the most important security controls and requirements to be a part of DR.

**C.**   The purpose of DR is different from cybersecurity and the two are not related.

**D.**   Only those controls required by law are a part of DR plans and capabilities.

Images  **A**. All of an organization’s security policies, requirements, and controls apply equally to all environments, whether they are normal production environments or disaster recover environments. At any time, an organization may be compelled to shift its processing from its primary processing facilities to a disaster recovery processing facility, making the DR facility the new (but usually temporary) primary facility. All controls for security and privacy apply to all systems in all locations.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because security requirements and controls cannot be “cherry picked” to be included in DR sites based on management’s wishes. Instead, all requirements and controls apply to all information processing facilities, whether they are primary or recovery facilities. **C** is incorrect because security requirements and controls apply to all information processing facilities, whether they are primary or recovery facilities. **D** is incorrect because an organization may have requirements and controls in addition to those required by law that should be applicable to all information processing facilities.

[**32**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q32)**.**   A security team has performed a risk assessment of a third-party service provider that hosts the organization’s financial accounting system. The risk assessment has identified some critical risks. How should the security team and its leader respond?

**A.**   Discuss the matter with the service provider to see what mitigations can be implemented.

**B.**   Enact controls to mitigate the critical risks.

**C.**   Negotiate a new agreement with the service provider.

**D.**   Select a different service provider based on the absence of these risks.

Images  **A**. When an organization has performed a risk assessment of a third-party service provider, the best course of action is for the organization to engage with the service provider to understand these risks better and to determine what actions (in the form of additions or changes to existing controls or the enactment of new controls) can be taken that will partially or completely mitigate the identified risks.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because an organization cannot simply enact new controls in another organization. Only the third-party organization can make changes to its operations, including changes to existing controls and the enactment of new controls. **C** is incorrect because the initiation of contract negotiations during the term of a contract is often not fruitful. However, if a contract is about to expire and be renewed, that may be a good opportunity to bring new language into the agreement between the organization and its third-party service provider. **D** is incorrect because the discovery of new risks is rarely enough cause to compel an organization to change service providers. Terminating a relationship with a service provider is usually an action of last resort.

[**33**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q33)**.**   A new CISO in a manufacturing company has developed statistics and metrics on the industrial control systems supporting automated manufacturing and has found that more than one-third of the operating systems are many years out of support because the ICS software does not support newer versions of operating systems and newer versions of ICS software are not available. What is the best response in this situation?

**A.**   Switch to software vendors that provide modern, supported operating systems.

**B.**   Upgrade operating systems and install backward-compatible libraries.

**C.**   Virtualize outdated operating systems.

**D.**   Isolate ICS systems in hardened networks.

Images  **D**. Many organizations face the problem of being “marooned” on old versions of ICS software, subsystems, and computer operating systems, because the old versions of ICS software are not supported on newer operating systems. Often, newer versions of ICS software are prohibitively expensive or simply not available. The best response is to isolate ICS environments in separate, hardened networks with very tight access controls so that common threats are greatly reduced in both probability and impact.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because switching software vendors is often prohibitively expensive—and sometimes not available at all. **B** is incorrect because of the scarcity of libraries in newer operating systems to mimic older operating systems. **C** is incorrect because virtualizing older OSs does not alter the fact that an older and potentially vulnerable OS is still present.

[**34**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q34)**.**   A new CISO in a manufacturing company has developed statistics and metrics on the industrial control systems supporting automated manufacturing and has found that more than one-third of the operating systems are many years out of support because the ICS software does not support newer versions of operating systems and newer versions of ICS software are not available. How should this situation be described to senior management?

**A.**   The organization needs to step up and modernize its industrial control systems.

**B.**   The organization needs to isolate and protect its industrial control systems.

**C.**   The organization needs to require its ICS vendors to support modern operating systems.

**D.**   The organization needs to outsource its ICS to an ICS cloud provider.

Images  **B**. The best message to senior management is one of mitigation through protective isolation of its industrial control systems. Even ICS environments with modern, supported operating systems should be isolated from the rest of the organization’s networks.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because modernization of its ICS environment will probably be prohibitively expensive—in fact, this is probably the highest-cost option. **C** is incorrect because simply requiring ICS vendors to support newer operating systems is probably a nonstarter: in some cases, the ICS vendors are no longer in business; in other cases, upgrades to newer ICSs are possible but include a costly upgrade of ICS equipment in addition to ICS software. **D** is incorrect because the matter of unsupported ICS software is usually coupled with unsupported ICS hardware, and the two must sometimes be upgraded together—a costly option.

[**35**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q35)**.**   Which of the following is the best language for a security policy in a multinational software organization regarding background checks?

**A.**   Prior to hire, all employees must undergo background investigations where permitted by law.

**B.**   Prior to hire, all workers, whether they are employees, contractors, or consultants, must undergo background investigations.

**C.**   Prior to hire, all workers, whether they are employees, contractors, or consultants, must undergo background investigations where permitted by law.

**D.**   Prior to hire and annually thereafter, all employees must undergo background investigations.

Images  **C**. Background investigations, sometimes called background checks, are an essential safeguard in organizations. However, background checks, such as those performed in the United States, are not permitted in many countries. The best language here, “as permitted by law,” requires background investigations to be performed where they are permitted. Also, it is essential that not only full-time employees but also part-time employees, contractors, temporary workers, and consultants undergo background investigations—where permitted by law.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because this language excludes background investigations for part-time workers, temporary workers, contractors, and consultants. All of them should also have background investigations done prior to their having access to information systems and data. **B** is incorrect because background investigations are not permitted in many countries. The language here is inflexible and would result in the need for policy exceptions. **D** is incorrect because this language excludes all other types of workers: part-time, temporary, contractor, and consultant. Also, this language excludes “as permitted by law” that recognizes that background investigations are not permitted in every country.

[**36**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q36)**.**   What is the best time to identify security and privacy requirements in a project to identify and evaluate a software service provider?

**A.**   Just prior to implementation

**B.**   At the same time that business functional requirements are identified

**C.**   Post-implementation after the first penetration test

**D.**   Post-implementation before the first penetration test

Images  **B**. The best time to identify security requirements is at the earliest possible phase in the project—typically when business requirements and other requirements are also identified.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because the identification of security requirements just prior to implementation removes the opportunity to select a software service provider based upon its security capabilities (alongside all of its other capabilities). This also removes the opportunity to implement security controls and features in the service, since “just prior to implementation” implies that controls, features, and capabilities have already been determined. **C** and **D** are incorrect because post-implementation is far too late to identify security requirements. When security requirements have not been identified until after implementation, there is a high probability that the service will have been implemented with numerous security weaknesses.

[**37**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q37)**.**   What is the primary reason for discontinuing the use of SMS for two-factor authentication?

**A.**   SMS messages can be easily spoofed.

**B.**   SIM switching attacks can cause SMS messages to be sent elsewhere.

**C.**   SMS messages are not encrypted in transit.

**D.**   One-time passwords sent via SMS do not prove physical possession of a trusted device.

Images  **D**. SMS messages are not as secure as they used to be, and several methods are available (cellular carrier websites and services such as Google Voice) for users to obtain SMS messages without having their mobile device (the second factor), with just a user ID and password.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because SMS spoofing alone would not pose a threat to two-factor authentication. **B** is incorrect because this is not the best answer, although SIM switching attacks are a threat. **C** is incorrect because encryption of SMS messages does take place at lower layers.

[**38**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q38)**.**   An organization recently experienced a security incident in which an employee leaked vital information via an unapproved cloud-based storage provider. The employee stated that she “did not know” that it was against policy to store company data in unapproved cloud-based services. What is the best administrative control to prevent this type of event in the future?

**A.**   Require employees to acknowledge compliance to security policy annually in writing.

**B.**   Implement a CASB system.

**C.**   Implement endpoint-based DLP.

**D.**   Implement a GPO to block the use of USB mass storage devices.

Images  **A**. Requiring employees to acknowledge compliance to security policy is the best option. This answer is the only administrative control of the four answers available.

Images  **B**, **C**, and **D**are incorrect. Although these may be effective automatic controls, they are not administrative controls, as the question stated.

[**39**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q39)**.**   An organization recently experienced a security incident in which an employee leaked vital information via an unapproved cloud-based storage provider. The employee stated that she “did not know” that it was against policy to store company data in unapproved cloud-based services. What is the best automatic control to prevent this type of event in the future?

**A.**   Require employees to acknowledge compliance to security policy annually in writing.

**B.**   Implement a CASB system.

**C.**   Implement endpoint-based DLP.

**D.**   Implement a GPO to block the use of USB mass storage devices.

Images  **B**. A cloud access security broker (CASB) system is specifically designed to provide visibility and control into the use of cloud-based services. This is the best available option of those listed.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because signing an acknowledgment of policy is not an automatic control, but an administrative control. **C** is incorrect because endpoint DLP, while potentially effective, is not as effective as a CASB solution. **D** is incorrect because restriction of USB mass storage does not address the use of cloud-based storage.

[**40**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q40)**.**   What control can best improve software security in a software as a service organization that currently undergoes quarterly penetration tests of its SaaS software?

**A.**   SAST scans as a part of the software build process

**B.**   Monthly penetration tests

**C.**   Mandatory secure development training for all developers

**D.**   Daily web application scans of the production environment

Images  **A**. SAST (static application security testing) integration into the SaaS product build environment is the best solution. Modern organizations, particularly SaaS providers, are moving toward DevOps and away from waterfall development cycles. To improve security, DevOps is giving way to DevSecOps, where security such as SAST and DAST tools are integrated into software automation.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because an increase in the frequency of penetration tests is not the best available option. **C** is incorrect because security development training, while important, produces only gradual improvement in software security, and it rarely, if ever, results in the complete absence of exploitable security defects. **D** is incorrect because daily scans, while effective in detecting many (but not all) security defects, is not as effective as a SAST solution. It is important that organizations move security controls “to the left” (earlier in the development cycle).

[**41**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q41)**.**   Which of the following is the best source for system and component hardening standards?

**A.**   Microsoft

**B.**   NIST

**C.**   SANS

**D.**   The Center for Internet Security

Images  **D**. The Center for Internet Security, commonly known as CIS, has a comprehensive library of hardening standards for server operating systems, endpoint operating systems, mobile device operating systems, network devices, and numerous software subsystems including database management systems and application platforms. CIS controls are highly respected and kept up to date.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because Microsoft, while a reliable source for hardening techniques for its own products, is not a source for hardening for leading operating systems, subsystems, and network devices. **B** is incorrect because NIST is not the best source for hardening information for a wide variety of hardware and software products. **C** is incorrect because SANS is not the best source for hardening standards.

[**42**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q42)**.**   Which of the following is the best vulnerability management process?

**A.**   Proactive patching and hardening according to SLAs, and security scanning as a QA activity

**B.**   Security scanning reports initiate patching and hardening according to SLAs

**C.**   Proactive patching according to SLAs, and security scanning as a QA activity

**D.**   Security scanning reports initiate patching according to SLAs

Images  **A**. The best vulnerability management process is one in which system and device patching and hardening are proactively performed according to established SLAs, and where security scanning (and examination of hardening activities) is a quality assurance (QA) activity to confirm that proactive patching and hardening activities are effective.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because vulnerability scanning should not be the driving force for patching and hardening. **C** is incorrect because vulnerability management should also include proactive system hardening according to established local standards that are based upon accepted industry standards. **D** is incorrect because this method relies on vulnerability scanning that drives patching; hardening, another important aspect of vulnerability management, is not even mentioned in this option.

[**43**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q43)**.**   An existing healthcare organization is developing a first-ever system and device hardening program and has chosen CIS Benchmarks as their industry standard. What is the best method for implementing CIS Benchmarks in server operating systems in production environments?

**A.**   Implement CIS Benchmark configurations all at once in test environments, and then in production environments.

**B.**   Implement CIS Benchmark configurations slowly in test environments, and then in production environments.

**C.**   Implement CIS Benchmark configurations all at once in production environments.

**D.**   Implement CIS Benchmark configurations slowly in production environments.

Images  **B**. The CIS Benchmarks are highly detailed and voluminous, particularly for server operating systems. There are dozens of configuration settings, which should be applied gradually rather than all at once. Implementing these changes of configuration in test environments first ensures that configuration changes do not adversely affect production systems.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because implementing all of the configuration changes in CIS Benchmarks all at once is likely to result in server or application malfunctions that may be difficult to troubleshoot, since so many changes will have been made at one time. **C** and **D** are incorrect because it is not a good practice to implement server configuration changes in production environments without first testing those changes in test environments.

[**44**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q44)**.**   What is the best use for requiring security certifications when screening candidates for a security director position in a midsized financial services organization?

**A.**   Require CISSP or CISM, or similar certifications.

**B.**   Desire CISSP or CISM, and relevant experience.

**C.**   Require CISSP and CISM.

**D.**   Require CISSP or CISM, as well as an advanced degree.

Images  **B**. Relevant experience is the most important characteristic in a security director candidate. Certifications such as CISSP and CISM are great additions. Today, many organizations are excessively requiring advanced certifications such as CISSP and CISM, not only for leadership positions but also for individual contributor positions. This in part is a cause of the perceived shortage of qualified personnel.

Images  **A**, **C**, and **D**are incorrect. **A** and **C** are incorrect because requiring advanced security certifications alone is vastly insufficient for a security leader candidate. **D** is incorrect because requiring an advanced security certification such as CISSP and CISM, as well as requiring an advanced degree, will result in many candidates—including potentially the most qualified candidates—not being considered.

[**45**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q45)**.**   What is the best advantage of implementing smaller units of security awareness training quarterly as opposed to all-at-once training annually?

**A.**   More straightforward recordkeeping for compliance purposes

**B.**   Less disruption to workers in an organization

**C.**   Decreased license costs from security awareness training content providers

**D.**   Keeping the topic of information security current through more frequent training

Images  **D**. The primary purpose for conducting smaller units of security awareness training several times per year, versus a single larger session once per year, is to keep the topic of information current and to keep security awareness on the minds of workers in an organization.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because recordkeeping for security awareness training is already straightforward; maintaining training records for annual or quarterly training events is not burdensome. **B** is incorrect; although training may be seen as disruptive, security awareness training courses are generally limited to a few hours or a day. **C** is incorrect because license cost differences between quarterly and annual training should be minimal or insignificant.

[**46**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q46)**.**   What is the purpose of periodically assessing risks at a third-party service provider?

**A.**   Periodic assessment of third parties is required by the PCI-DSS.

**B.**   Assessing a third party is wise when the business relationship changes or increases.

**C.**   Assessment helps with detection of changes in risk that may not have existed at the start of the third-party relationship.

**D.**   Assessment determines the need to perform penetration tests of specific third-party service providers.

Images  **C**. Periodic assessments of risk in third-party service providers is needed because business conditions in any given third-party service provider can change in ways that influence risk for better or for worse.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because this is too narrow a position; although PCI-DSS does require that organizations confirm the ongoing compliance status, this fails to address the phenomenon of changing risk in service provider organizations. **B** is incorrect because risk assessments are *also* needed when a relationship with a third-party service provider relationship changes, but this does not address the need for periodic assessments while the relationship does not change. **D** is incorrect because the outcome of a risk assessment of a third party will not ordinarily determine the need for penetration tests. Rather, the level of inherent risk and the specific role of a third-party service provider will together determine the need for a penetration test.

[**47**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q47)**.**   In large organizations, what is the best technique for incorporating cybersecurity-related language into contracts with third-party service providers?

**A.**   Develop custom legal terms for each service provider based on questionnaires.

**B.**   Develop custom legal terms for each service provider based on risk.

**C.**   Develop templates of legal terms for various types of service providers.

**D.**   Develop templates of legal terms for various types of service providers, and tailor them as needed.

Images  **D**. Large organizations with better security programs develop templates of security terms and conditions for various types of situations. Then, for each third party, specific changes are made as needed.

Images  **A**, **B**, and **C**are incorrect. **A** and **B** are incorrect because the development of purely custom security terms and conditions is too time consuming. **C** is incorrect; although the use of a template is a good starting point, each contract will need specific changes based on several factors, including the nature of the business relationship and specific risks that are identified through questionnaires and other means.

[**48**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q48)**.**   The security leader in an organization learned about a security breach at a strategic service provider that provides data storage services. What first step should the security leader take regarding the relationship with the service provider?

**A.**   Examine the agreement to see what the service provider’s obligations are.

**B.**   Terminate the contract if there is a breach exit clause.

**C.**   Request a copy of the security incident from the service provider.

**D.**   Perform a penetration test of the service provider’s service endpoints.

Images  **A**. Before the security leader can take action, he needs to first understand what security-breach-related activities the service provider is obligated to perform. Knowing this will help the security leader take the right steps as a part of his organization’s response to the breach.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because a contract termination should be an action of last resort, not the first action to take, even in the event of a breach. Further, it is rarely the security leader’s decision to terminate a contract; instead, the security leader may offer his or her opinion regarding such remedies. **C** is incorrect because this may or may not be applicable or available. First, the agreement needs to be examined to see what obligations, if any, are included. **D** is incorrect because a penetration test may not be permitted or appropriate.

[**49**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q49)**.**   How could a statistic about security scanning be transformed into a metric meaningful to senior management?

**A.**   Avoid the use of technical jargon.

**B.**   Express the metric in business terms and potential business outcomes.

**C.**   Show the metric on an easily viewed dashboard.

**D.**   Describe the statistic in an executive summary narrative.

Images  **B**. A statistic or metric that is operational in nature can be transformed into a meaningful business metric by using business terms and language and describing business outcomes. For example, a statistic related to the time required to install security patches can be described in terms of IT equipment that supports key business functions together with their compliance to a security process designed to reduce the probability or impact of a breach that could disrupt business operations.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because the removal of technical jargon alone may not be enough to provide business context. **C** is incorrect because an attractive visual display may simply provide little-understood information in visual form. **D** is incorrect because the statistic should first be portrayed in some kind of a quantitative format that can reveal trends over time. Still, a narrative may be helpful at times.

[**50**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q50)**.**   Which of the following is the best method for testing the following control: “Only authorized persons may approve user access requests”?

**A.**   Make some dummy access requests and see who approves them.

**B.**   Interview at least two process SMEs and review business records.

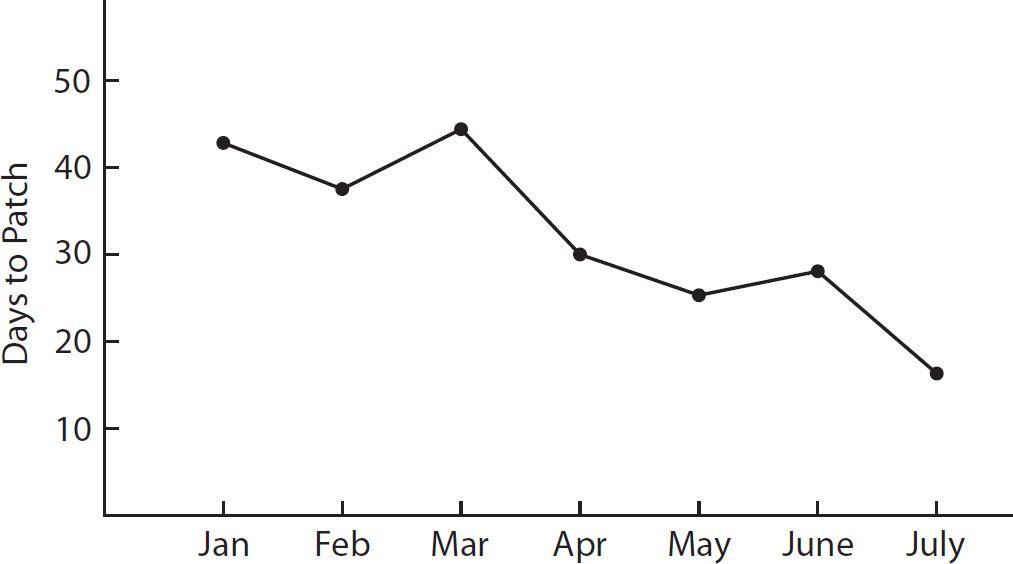
**C.**   Interview process owners and ask who the approvers are.

**D.**   Review business records and see who approved access requests.

Images  **B**. The best way to test this control is to interview two or more subject matter experts on the access request process and examine business records to see who has reviewed access requests.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because process owners and operators may be aware that “the auditors are watching” and may behave differently during audit tests than they normally would. **C** is incorrect because this option lacks the examination of business records (which would hopefully show the names of individual process approvers). **D** is incorrect because this option lacks interviews with two or more business process owners.

[**51**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q51)**.**   What does the following vulnerability management dashboard indicate to management?



**A.**   It takes more days to patch systems.

**B.**   It takes fewer days to patch systems.

**C.**   Risk is increasing over time.

**D.**   Risk is decreasing over time.

Images  **D**. Patches are being applied more quickly. Thus, risk is decreasing over time because patches are being applied more quickly.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because it is taking fewer days to patch systems, according to the chart. **B** is incorrect because the story here is that risk is decreasing as a result of patches being applied more quickly. **C** is incorrect because patches are being applied more quickly, which means risk is decreasing.

[**52**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q52)**.**   In an organization’s information security program, one of the strategy statements reads, “Improve security awareness outreach to company workers.” Which activities would best support this objective?

**A.**   Scan end-user workstations more frequently.

**B.**   Raise the minimum score required to complete security awareness training successfully.

**C.**   Publish a quarterly newsletter with security tips and articles.

**D.**   All of these are correct.

Images  **C**. Publishing a quarterly newsletter (in a medium often used in the organization) is the best activity. Security tips and articles will help company workers better understand the nature of cybersecurity risks and actions they can take to reduce risk.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because scanning end-user workstations will not improve users’ awareness of cybersecurity issues. **B** is incorrect because this does not improve outreach, but the level of competency required. **D** is incorrect because not all answers help to meet this objective.

[**53**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q53)**.**   A company’s IT organization has decided to implement a single sign-on (SSO) portal in the coming year. What are the most important security-related considerations that should be included in advance planning for the SSO portal?

**A.**   SAML integration with applications

**B.**   Password quality and password reset

**C.**   Multifactor authentication

**D.**   HMAC integration

Images  **A**. The point of single sign-on is to make authentication to a large number of applications a matter of clicking a button. Without SAML or equivalent integration capabilities, it will take considerable effort to integrate an SSO portal with an organization’s business applications.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because password quality and password reset, while vital capabilities, are not always controlled by an SSO portal. **C** is incorrect because multifactor authentication, while vital, is not always controlled by an SSO portal. **D** is incorrect because HMAC is a deprecated protocol for authentication.

[**54**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q54)**.**   All of the following are advantages to outsourcing an IS audit function, *except* which one?

**A.**   Avoidance of hiring and retaining talent

**B.**   Cost savings of contractors versus full-time employees

**C.**   No need to find onsite workspace

**D.**   Cost savings for training and professional development

Images  **B**. There is usually no cost savings for outsourcing IS audit, because these personnel generally perform their work onsite. Consulting and contracting costs are almost always significantly higher than salaries of equivalent full-time personnel.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because an organization that outsources IS auditors does not need to worry about hiring and retaining talent; instead, this is a problem for the consulting firm or contracting agency. **C** is incorrect because IS auditors still need workspace because much of their work is performed onsite. **D** is incorrect because organizations do not need to manage training and professional development for contractors and consultants.

[**55**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q55)**.**   What is the best approach to the development of an organization’s security incident response plan?

**A.**   Developing separate security incident recordkeeping

**B.**   Developing a general IR plan and leaving the details to subject matter experts

**C.**   Developing detailed playbooks and relying on the organization’s crisis management plan

**D.**   Leveraging the organization’s crisis management plan

Images  **D**. The best approach for developing any IR plan is to leverage existing processes wherever possible, including the corporate crisis management plan, an IT incident response plan, and emergency communications plans. Leveraging existing processes is more effective than building separate parallel processes.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because existing incident recordkeeping should be leveraged instead of building a separate record. **B** is incorrect because detailed IR playbooks should also be developed so that SMEs understand what steps to take for various incident scenarios. **C** is incorrect because an overall IR plan is needed, even when there are detailed IR playbooks and a crisis management plan.

[**56**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q56)**.**   Which of the following statements about guidelines is correct?

**A.**   Guidelines are mandatory.

**B.**   Guidelines are optional and not required.

**C.**   Security policies are derived from guidelines.

**D.**   Security controls are derived from guidelines.

Images  **B**. Guidelines describe various ways that security policies can be implemented. They are not required, but they provide guidance to personnel who are looking for ways of implementing policies.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because guidelines are not mandatory, but instead offer guidance on the implementation of policy. **C** is incorrect because policies are not derived from guidelines; instead, guidelines are derived from policies. **D** is incorrect because controls are not derived from guidelines.

[**57**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q57)**.**   What is the purpose of a security awareness program?

**A.**   Helps personnel understand proper computer usage

**B.**   Informs personnel about security policy

**C.**   Helps personnel develop better judgment when handling company information

**D.**   Meets compliance requirements for PCI-DSS and SOX

Images  **C**. The main purpose of security awareness is to help personnel be more aware of cybersecurity-related risks and to help them develop better judgment so that they will make better decisions in a wide variety of situations.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because security awareness training includes content on proper computer usage, but also on safe computer usage and other topics such as security while traveling and workplace safety. **B** is incorrect because security awareness training goes beyond security policy. **D** is incorrect because compliance is not the only driver for security awareness training.

[**58**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q58)**.**   What is meant by the term “move to the left” in the context of information security and systems development?

**A.**   Introduce security earlier in the development lifecycle.

**B.**   Introduce security later in the development lifecycle.

**C.**   Remediate security flaws more slowly.

**D.**   Remediate security flaws more quickly.

Images  **A**. The term “move to the left” signifies that security is introduced earlier in the systems development lifecycle. For instance, if an organization performs vulnerability scans after a new software version is released to production, then performing vulnerability scans on prerelease software before it is released to production would be a “move to the left.” In another example, if an organization performs static code scans during the nightly build run, then performing static code scans at code check-in would be a “move to the left.”

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because “move to the left” means that security is introduced earlier, not later, in the systems development lifecycle. **C** and **D** are incorrect because “move to the left” is not related to the timing of remediation.

[**59**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q59)**.**   An online retail organization accepts credit card payments and is therefore required to comply with PCI-DSS. Which of the following statements is correct regarding the organization’s service providers that have access to the organization’s credit card payment information?

**A.**   The organization is required to verify each service provider’s PCI-DSS compliance annually.

**B.**   The organization is required to verify each service provider’s PCI-DSS compliance status annually.

**C.**   The organization is required to assess each service provider’s PCI-DSS compliance annually.

**D.**   The organization is required to verify each service provider’s PCI-DSS compliance quarterly.

Images  **B**. According to PCI-DSS requirement 12.8.4 (PCI-DSS version 3.2), each organization is required to “maintain a program to monitor its service providers’ PCI-DSS compliance status at least annually.” This can be as simple as requesting each service provider to send a copy of its most recent Attestation of Compliance (AOC) to the organization.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because organizations are not required to verify each service provider’s compliance (implying some kind of an audit). **C** is incorrect because organizations are not required to assess its service providers for PCI-DSS compliance. **D** is incorrect because organizations are not required to verify its service providers’ PCI-DSS compliance quarterly, but rather annually.

[**60**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q60)**.**   An organization performs phishing testing on a monthly basis. Over the past year, the average of click-through rates has changed from 42 percent to 14 percent. What conclusion can be drawn from this trend?

**A.**   End users are more likely to click on actual phishing messages.

**B.**   Phishing messages are more likely to reach end users’ inboxes.

**C.**   End users are less likely to click on actual phishing messages.

**D.**   Phishing messages are less likely to reach end users’ inboxes.

Images  **C**. A reduction in click-through rates in phishing testing means that fewer end users are being tricked by test phishing messages that are sent to them via e-mail. Provided the quality of the test messages was good, this is an indication that end users are less likely to click on actual phishing messages that are sent to them.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because the trend indicates they are less likely to click on actual phishing messages, not more likely. **B** and **D** are incorrect because this metric provides no indication on the likelihood of actual phishing messages to arrive in end-user inboxes.

[**61**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q61)**.**   Which of the following is the best approach for a “state of the security program” for the board of directors?

**A.**   Executive summary and details from an enterprise risk assessment

**B.**   Executive summary portion of an enterprise risk assessment

**C.**   Detailed workbook containing statistics and metrics for the past 12 months

**D.**   Short slide deck showing key risk indicators, accomplishments, and incidents

Images  **D**. A typical board of directors is going to be most interested in summary information and trends. A list of security incidents is valuable information as well.

Images  **A**, **B**, and **C**are incorrect. **A** and **B** are incorrect because a risk assessment paints a picture of risk at a point in time, but it does not provide trends that tell the audience whether the security program is improving or whether it is reducing risk. **C** is incorrect because most boards are not going to want detailed information, but instead will want summary information that describes what the detailed information means. In some cases, some board members may want to reference detailed information as supporting evidence.

[**62**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q62)**.**   An organization has hired a new CISO to make strategic improvements to the information security program. As one of her first important tasks, the new CISO is going to write a program charter document that describes the organization’s security program, key roles and responsibilities, primary business processes, and relationships with key business stakeholders and external parties. What is the best approach to producing this charter document?

**A.**   Develop the charter document based upon ISO/IEC 27001.

**B.**   First identify and interview key business stakeholders to understand their cyber-risk needs and concerns.

**C.**   Develop the charter document based upon information security best practices.

**D.**   Develop the charter document based upon industry-sector best practices.

Images  **B**. To align a security program to the business, it is first necessary to become familiar with key attributes of the organization, which is best obtained through discussions with key business stakeholders, business unit leaders, and department heads. Only then can a security leader hope to develop an information security program that is aligned to the business.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because the alignment of an information security program charter is a secondary concern, once a security leader has determined how to align a program to the business. **C** and **D** are incorrect, because alignment to general and industry-sector best practices runs the risk of misalignment with the organization.

[**63**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q63)**.**   Approximately how many personnel would need to be identified to fully staff a 24/7/365 SOC, which can ensure shift coverage even during vacation and sick time?

**A.**   12

**B.**   3

**C.**   9

**D.**   24

Images  **A**. At least 12 persons are needed to cover all working shifts each week in a security operations center (SOC), assuming eight-hour shifts.

Images  **B**, **C**, and **D**are incorrect. **B** and **C** are incorrect because even nine workers cannot fully cover all of the shifts during a week, as well as cover staff absences due to vacation, sick leave, and training. **D** is incorrect because it indicates more workers than are necessary.

[**64**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q64)**.**   What is the best approach for implementation of a DLP system in an organization’s e-mail environment?

**A.**   Develop a data classification policy, and implement active controls.

**B.**   Develop a data classification policy, train users, and perform scans of unstructured data stores.

**C.**   Develop a data classification policy, train users, and implement active controls.

**D.**   Develop a data classification policy, train users, and implement passive controls.

Images  **D**. Success in a DLP implementation requires that the organization have a well-defined data classification policy, together with handling procedures. User training is a must, as organizations will need to rely at least partly on individual end-user judgment. Implementing DLP tools in passive (monitoring) mode enables the organization to learn more about data movement; once use cases become clear, active (intervention) controls can be slowly implemented.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because the implementation of active controls right away is highly likely to disrupt key business process and draw ire from end users and department heads whose business operations are being impacted. **B** is incorrect because static data discovery is not highly related to e-mail use. **C** is incorrect because it is first important to implement passive (monitoring) controls to learn about data flow before implementing active (blocking) controls, so that blocking controls do not disrupt business operations.

[**65**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q65)**.**   An organization has experienced numerous instances of unintended data exfiltration via its corporate e-mail system. All of the following approaches for solving this problem are valid *except* which one?

**A.**   Warn users who are sending e-mail to external recipients so they can double-check recipients.

**B.**   Automatically encrypt attachments in outgoing messages to external recipients.

**C.**   Disable e-mail recipient auto-complete.

**D.**   Warn users who are sending e-mail with attachments to external recipients so they can double-check recipients.

Images  **B**. Automatic encryption of attachments in outgoing messages is not likely to help in the situation described, where too much data exfiltration is occurring. Depending on the encryption approach used, the solution will either result in no one being able to read attachments or the wrong recipients being able to read attachments anyway.

Images  **A**, **C**, and **D**are incorrect. **A** and **D** are incorrect because warning users about e-mail going to external parties is a valid step to take, particularly if the problem has been about users selecting the wrong recipients. **C** is incorrect because disabling e-mail recipient auto-complete *can* be an effective remedy if there are numerous cases of data being sent to the wrong recipients.

[**66**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q66)**.**   During the organization’s annual goal-setting session, the CISO was asked first to describe the security program’s goals for the new year. Why would the CISO prefer to wait until later?

**A.**   The CISO is unprepared and needs more time to establish goals.

**B.**   The CISO needs to know what goals the CIO will set before describing security goals.

**C.**   The CISO wants to get ideas from others so that security goals will be more credible.

**D.**   The CISO first needs to understand the organization’s overall goals, as well as those of business leaders.

Images  **D**. In order for an organization’s security program to be aligned with the business, it is necessary for the CISO to first know and understand the organization’s goals and objectives. Only then can the security leader develop information security program goals that will support the organization’s objectives.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because this is not the best answer. **B** is incorrect because the CISO needs to know more than just the CIO’s goals. **C** is incorrect because this is not the best answer.

[**67**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q67)**.**   The statement, “Passwords can be constructed from words, phrases, numbers, and special characters in a variety of ways that are easily remembered but not easily guessed,” is an example of what?

**A.**   A guideline

**B.**   A standard

**C.**   A policy

**D.**   A procedure

Images  **A**. The phrase, “Passwords can be constructed from words, phrases, numbers, and special characters in a variety of ways that are easily remembered but not easily guessed,” is a guideline, as it is guidance to users to help them determine how to comply with a policy or standard. One hint that this is a guideline is the lack of minimum length of a password.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because a standard would specify minimum length, which is not included in the example. **C** is incorrect because this statement is not a policy statement. **D** is incorrect because the statement is not a procedure for setting a password, but rather offers guidance on its composition.

[**68**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q68)**.**   Which of the following statements is correct about PCI-DSS audits?

**A.**   An organization with a PCI-ISA (internal security assessor) does not have to undergo external PCI-DSS audits.

**B.**   An organization can be compliant with PCI-DSS if it completes the audit and has project plans for noncompliant controls.

**C.**   An organization must have all PCI-DSS controls in place to be compliant with PCI-DSS.

**D.**   An organization must complete a PCI-DSS audit to be compliant with PCI-DSS.

Images  **C**. For an organization to be compliant with PCI-DSS, all PCI-DSS controls must be in place. This includes any compensating controls that may be required.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because organizations that meet specific criteria (including but not limited to credit card transaction volume thresholds) are required to undergo PCI-DSS external audits, regardless of whether they have an ISA on staff or not. **B** is incorrect because the rules of PCI-DSS compliance state that all controls must be in place; plans for implementing controls later are not valid substitutes for ineffective controls. **D** is incorrect because completing an audit does not necessarily mean the audit was completed successfully.

[**69**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q69)**.**   Which of the following is the most effective means for making information security policies, standards, and guidelines available to an organization’s workforce?

**A.**   Policies, standards, and guidelines should be on a “need to know” basis and not published or sent to personnel.

**B.**   Publish policies, standards, and guidelines on an intranet site where they can be easily found.

**C.**   E-mail policies, standards, and guidelines to the workforce once per year.

**D.**   Publish policies, standards, and guidelines in hard copy and have copies available at the security office.

Images  **B**. For most organizations, the most effective way to make security-related content available, including policies, standards, guidelines, and other materials, is to publish them on an internal user website (an intranet) where they can be easily accessed.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because security-related content, including policies, standards, and guidelines, should be made available to all personnel. **C** is incorrect because e-mailing security policies, standards, and guidelines is not an effective way of communicating this kind of content in most organizations. Often, people will read and then discard such messages and then will not have that content at hand later on if needed. **D** is incorrect because it is impractical in most organizations to publish security-related content such as policies, standards, and guidelines in hard copy format, because workers at other locations would not have ready access to them.

[**70**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q70)**.**   What is the best approach in most organizations for ensuring that cybersecurity personnel remain current in their knowledge and skills?

**A.**   Security personnel can study on their own and do not require support from the organization.

**B.**   Build a library of books on various security topics that security personnel can check out and read.

**C.**   Provide at least one month of formal training per year.

**D.**   Provide at least one week of formal training per year.

Images  **D**. The best approach to help keep security personnel current on knowledge and skills is to make at least one week of training available to them once per year. Different personnel will opt for various approaches, including attending a conference with training sessions, taking a long web-based study course, studying for certifications, or a number of half-day or one-day training events. Organizations that fail to provide this type of training support to its cybersecurity personnel often experience excessive staff turnover: the threats, practices, and tools in cybersecurity are changing rapidly, and a week of training helps security personnel keep up, at best.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because it is unwise to require security personnel to fend for themselves, as they will be more likely to seek employment elsewhere. **B** is incorrect because a library is practical more for reference than for building new skills; further, in distributed organizations, a library would benefit only workers near the library (or there would be the trouble of shipping books to them). **C** is incorrect because a full month of training is impractical because of the costs involved.

[**71**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q71)**.**   In an organization with an established security culture, some personnel complain about the time required to undergo the annual eight-hour security awareness training, claiming that they are already proficient in the subject matter and that the organization would benefit more from their continuing their work duties. What is the best approach to address this matter?

**A.**   Permit personnel to skip security awareness training topics if they first pass tests on those topics.

**B.**   Permit those personnel to skip security awareness training.

**C.**   Permit personnel to skip security awareness training if they achieved good test scores in previous years.

**D.**   Require all personnel to undergo training because it is required by policy.

Images  **A**. Known as “testing out,” the technique of permitting students to take tests on various topics and permitting them to skip instruction if they pass those tests is a common practice.

Images  **B**, **C**, and **D**are incorrect. **B** and **C** are incorrect because some of the personnel who were proficient in prior years could fail to stay current and be unaware of new threats and practices. **D** is incorrect because this does not directly address their concern, which is reasonable.

[**72**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q72)**.**   An organization undergoes quarterly phishing testing to see how proficient its workforce is in detecting phishing messages. What is the best approach to take for individuals who fail to detect test phishing messages and click on their contents?

**A.**   Post their names on a “wall of shame” as a way of ensuring that personnel work harder to detect phishing messages properly.

**B.**   Require that they undergo reinforcement training.

**C.**   Remove their access privileges for a period of time.

**D.**   Require that they write a short essay on the risk of phishing messages.

Images  **B**. When workers click on a test phishing message, the best practice is to send them back to some reinforcement training in the hopes that their proficiency will improve.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because publicly shaming personnel for a mistake is not a productive tool. **C** is incorrect because this could have operational impact on the business. **D** is incorrect because writing an essay is not a typical sanction in a business, although it is more common in academic settings.

[**73**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q73)**.**   An organization is required, via a legal agreement, to perform account activity reviews. Which of the following best defines an account activity review?

**A.**   A review to see how many changes to users’ accounts are performed during a time period

**B.**   A review to see how frequently users log in to their accounts

**C.**   A review to see how busy users are when they log in to their accounts

**D.**   A review to see whether users have logged in to their accounts during a specific time period

Images  **D**. An account activity review determines whether each user account is active in a given time period, typically a month or a quarter. After such a review, any user accounts with no logins are candidates for being locked or removed. This helps to reduce risks of unauthorized access to a system by reducing the number of personnel who have access to the system.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because an account activity review is not related to the numbers of changes made to user accounts in a system. **B** is incorrect because a user account review is not so much concerned with the frequency of logins, but rather is concerned with whether an account has gone dormant—the user has not logged in for an extended period of time. **C** is incorrect because an account activity review is not concerned with how busy users are in a system.

[**74**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q74)**.**   A particular organization is a financial software as a service (SaaS) provider in the financial services industry. Many of the organization’s customers claim that they have a regulatory requirement to conduct audits of the SaaS provider. What remedy is available to the SaaS provider to minimize or eliminate these customer audits?

**A.**   Undertake an annual SOC2 Type 2 audit.

**B.**   Undertake an annual SOC2 Type 1 audit.

**C.**   Undertake an annual SOC1 Type 2 audit of relevant controls.

**D.**   Undertake an annual SOC1 Type 1 audit of relevant controls.

Images  **C**. An organization providing financial-related services to customers can undertake annual (or semiannual) SOC1 Type 2 audits. This audit is an effective and cost-saving substitute for customers performing their own audits.

Images  **A**, **B**, and **D**are incorrect. **A**and**B**are incorrect because a SOC2 audit will not effectively dissuade customers’ auditors from wanting to perform their own audits. **D** is incorrect because a Type 1 audit will not provide sufficient comfort to auditors in customer organizations

[**75**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q75)**.**   An organization provides training content to corporate customers via a SaaS platform. Because the organization’s SaaS platform includes some sensitive information about its customers, some of the customers want to perform audits of the SaaS organization. What can the SaaS organization do to reduce the number of such audit requests?

**A.**   Undergo an annual penetration test of its SaaS application.

**B.**   Undergo an annual penetration test of its infrastructure.

**C.**   Undergo an annual SOC2 Type 1 audit.

**D.**   Undergo an annual SOC2 Type 2 audit.

Images  **D**. The best approach for a nonfinancial SaaS organization to fend off audit requests from its customers is to undergo an annual SOC2 Type 2 audit. In a Type 2 audit, auditors (which are required to be public accounting firms) examine business processes as well as business records and develop detailed reports on every control’s effectiveness.

Images  **A**, **B**, and **C**are incorrect. **A** and **B** are incorrect because penetration tests reveal only a narrow facet of risk to customers. **C** is incorrect because a SOC2 Type 1 audit is an examination of the organization’s business process documents only and does not show whether those processes are being performed properly and effectively.

[**76**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q76)**.**   A CISO is turning her attention to the organization’s third-party risk management process, which has risk classification tiers into which each third party is classified. The CISO is concerned with “scope creep” among its third parties. In this context, what does this mean?

**A.**   Third parties that, over time, provide additional services that should elevate them into higher-risk tiers

**B.**   Third parties whose security programs degrade over time

**C.**   Third parties that outsource more and more of their operations to fourth parties

**D.**   Third parties that improve their security programs over time

Images  **A**. It is a good practice to establish a risk tier system for third parties and then to perform risk assessments at varying levels of rigor, based on their classification. “Scope creep” in this context means that a third party is initially classified at a low-risk tier. Then a change in the services that the third party provides to the organization changes, resulting in its being placed into a higher-risk tier. Unfortunately, often a CISO is not made aware of the changes in the business relationship with such a third party, and hence it remains in a lower-risk tier, where risk assessments are less rigorous.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect; although the degradation of a third party’s security program would be a matter of concern, this is not known as “scope creep.” **C** is incorrect because the phenomenon of third parties outsourcing services to fourth parties is not known as “scope creep.” **D** is incorrect because the improvement of a third party’s security program is not known as “scope creep.”

[**77**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q77)**.**   Of what value are metrics about dropped packets on firewalls?

**A.**   These metrics are a measure of security breaches that have been avoided.

**B.**   These metrics are of operational value only.

**C.**   These metrics are a measure of DDoS attacks that have been blocked.

**D.**   These metrics are of no value.

Images  **B**. Metrics about firewall-dropped packets generally are of operational value only, related to firewall workload and whether they are of sufficient capacity to protect networks properly from intrusion.

Images  **A**, **C**, and **D**are incorrect. **A** is incorrect because dropped packets are rarely about security breaches. **C** is incorrect because dropped packets are rarely about DDoS attacks. **D** is incorrect because the volume of dropped packets has some operational value related to firewall performance.

[**78**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q78)**.**   When in an audit is it acceptable to use a sample instead of an entire population?

**A.**   When the entire population is too large to test

**B.**   When automation is in place to ensure consistency

**C.**   When logging is in place to measure results

**D.**   When alerting is in place to notify personnel of exceptions

Images  **A**. Sampling is acceptable when the entire population of objects is too large to examine one-by-one. During an audit, if an excessive number of exceptions is found, additional samples can be taken to understand the problem better.

Images  **B**, **C**, and **D**are incorrect. **B** is incorrect because automation is not a requirement for sampling. **C** is incorrect because the presence of logging is generally not a factor on a sampling decision (even if the audit is about logging). **D** is incorrect because alerting is not related to sampling decisions.

[**79**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q79)**.**   An audit of a privileged user account has turned up a high number of exceptions from the sample. What is the appropriate next step?

**A.**   Notify management that there has been a breach.

**B.**   Stop the audit.

**C.**   Select additional samples.

**D.**   Complete the audit report.

Images  **C**. Generally speaking, during an audit in which a large number of exceptions has been identified in a given sampling, it is appropriate to select additional samples to determine the extent of the control’s ineffectiveness.

Images  **A**, **B**, and **D**are incorrect. **A** is incorrect because audit exceptions of privileged user accounts does not automatically signify a breach has occurred. **B** is incorrect because this is no reason to stop the audit. **D** is incorrect because the audit is not complete; more samples should be selected and analyzed.

[**80**](https://learning.oreilly.com/library/view/cism-certified-information/9781260456127/ch4.xhtml#ch4q80)**.**   James, a CISO in a software company, is preparing a report for the board of directors prior to an upcoming board meeting. What is the best method for James to deliver this report to board members?

**A.**   E-mail the report to board members.

**B.**   Orally deliver the report to the board members during the board meeting.

**C.**   Provide hard copies of the report to board members during the board meeting discussion.

**D.**   Securely send the report to board members in advance of the board meeting, and then review and discuss the report at the board meeting.

Images  **D**. The best approach is to provide a “preread” copy (a full copy) to board members a week or more before the board meeting and then to discuss the contents of the report at the board meeting. By providing the report in advance, board members can read the report at their leisure and prepare comments and questions for the CISO.

Images  **A**, **B**, and **C**are incorrect. **A** is incorrect because simply e-mailing the report to board members is insufficient; it is likely that they will want to engage in a live discussion about the contents of the report. **B** is incorrect because simply delivering the report orally deprives board members of the report itself, which probably contains considerably more detail. **C** is incorrect because it is better that hard copies be provided in advance of the meeting so that board members can read the report in advance and formulate questions for the CISO.