RC0-C02 Q&As

CompTIA Advanced Security Practitioner (CASP) Recertification Exam for Continuing Education

Pass CompTIA RC0-C02 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.lead4pass.com/rc0-c02.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A large corporation which is heavily reliant on IT platforms and systems is in financial difficulty and needs to drastically reduce costs in the short term to survive. The Chief Financial Officer (CFO) has mandated that all IT and architectural functions will be outsourced and a mixture of providers will be selected. One provider will manage the desktops for five years, another provider will manage the network for ten years, another provider will be responsible for security for four years, and an offshore provider will perform day to day business processing functions for two years. At the end of each contract the incumbent may be renewed or a new provider may be selected. Which of the following are the MOST likely risk implications of the CFO\\'s business decision?

A. Strategic architecture will be adversely impacted through the segregation of duties between the providers. Vendor management costs will remain unchanged. The risk position of the organization will decline as specialists now maintain the environment. The implementation of security controls and security updates will improve. Internal knowledge of IT systems will improve as providers maintain system documentation.

B. Strategic architecture will improve as more time can be dedicated to strategy. System stability will improve as providers use specialists and tested processes to maintain systems. Vendor management costs will increase and the organization\\'s flexibility to react to new market conditions will be reduced slightly. Internal knowledge of IT systems will improve as providers maintain system documentation. The risk position of the organization will remain unchanged.

C. Strategic architecture will not be impacted in the short term, but will be adversely impacted in the long term through the segregation of duties between the providers. Vendor management costs will stay the same and the organization\\'s flexibility to react to new market conditions will be improved through best of breed technology implementations. Internal knowledge of IT systems will decline over time. The implementation of security controls and security updates will not change.

D. Strategic architecture will be adversely impacted through the segregation of duties between the providers. Vendor management costs will increase and the organization\\'s flexibility to react to new market conditions will be reduced. Internal knowledge of IT systems will decline and decrease future platform development. The implementation of security controls and security updates will take longer as responsibility crosses multiple boundaries.

Correct Answer: D

QUESTION 2

Two universities are making their 802.11n wireless networks available to the other university\\'s students. The infrastructure will pass the student\\'s credentials back to the home school for authentication via the Internet.

The requirements are:

Mutual authentication of clients and authentication server

The design should not limit connection speeds

Authentication must be delegated to the home school No passwords should be sent unencrypted

The following design was implemented:

WPA2 Enterprise using EAP-PEAP-MSCHAPv2 will be used for wireless security

RADIUS proxy servers will be used to forward authentication requests to the home school

The RADIUS servers will have certificates from a common public certificate authority

A strong shared secret will be used for RADIUS server authentication

Which of the following security considerations should be added to the design?

A. The transport layer between the RADIUS servers should be secured

B. WPA Enterprise should be used to decrease the network overhead

C. The RADIUS servers should have local accounts for the visiting students

D. Students should be given certificates to use for authentication to the network

Correct Answer: A

One of the requirements in this question states, "No passwords should be sent unencrypted". The design that was implemented makes no provision for the encryption of passwords as they are sent between RADIUS servers. The local RADIUS servers will pass the student\\'s credentials back to the home school RADIUS servers for authentication via the Internet. When passing sensitive data such as usernames and passwords over the internet, the data should be sent over a secure connection. We can secure the transport layer between the RADIUS servers by implementing TLS (Transport Layer Security). Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL).

QUESTION 3

An information security assessor for an organization finished an assessment that identified critical issues with the human resource new employee management software application. The assessor submitted the report to senior management but nothing has happened. Which of the following would be a logical next step?

A. Meet the two key VPs and request a signature on the original assessment.

B. Include specific case studies from other organizations in an updated report.

C. Schedule a meeting with key human resource application stakeholders.

D. Craft an RFP to begin finding a new human resource application.

Correct Answer: C

You have submitted the report to senior management. It could be that the senior management are not that bothered about the HR application or they are just too busy to respond.

This question is asking for the logical next step. The next step should be to inform people that are interested in the HR application about your findings. To ensure that the key human resource application stakeholders fully understand the

implications of your findings, you should arrange a face-to-face meeting to discuss your report.

QUESTION 4

A security company is developing a new cloud-based log analytics platform. Its purpose is to allow:

Customers to upload their log files to the "big data" platform

Customers to perform remote log search

Customers to integrate into the platform using an API so that third party business intelligence tools can be used for the purpose of trending, insights, and/or discovery

Which of the following are the BEST security considerations to protect data from one customer being disclosed to other customers? (Select THREE).

A. Secure storage and transmission of API keys

B. Secure protocols for transmission of log files and search results

C. At least two years retention of log files in case of e-discovery requests

D. Multi-tenancy with RBAC support

E. Sanitizing filters to prevent upload of sensitive log file contents

F. Encryption of logical volumes on which the customers\\' log files reside

Correct Answer: ABD

The cloud-based log analytics platform will be used by multiple customers. We should therefore use a multi-tenancy solution. Multi-tenancy isolates each tenant\\'s (customer\\'s) services, jobs, and virtual machines from other tenants. RBAC (Role-Based Access Control) is used to assign permissions to each user. Roles are defined which have specific sets of permissions. Users are then assigned one or more roles according to what permissions they need (what roles they need to perform). Secure protocols for transmission of log files and search results: this is obvious. A secure protocol such as SSL/TLS should be used for the transmission of any sensitive data to prevent the data being captured by packet sniffing attacks. Encryptions keys used to access the API should be kept securely and transmitted securely. If a user is able to access another customer\\'s key, the users could access the other customer\\'s data.

QUESTION 5

A security consultant is conducting a network assessment and wishes to discover any legacy backup Internet connections the network may have. Where would the consultant find this information and why would it be valuable?

A. This information can be found in global routing tables, and is valuable because backup connections typically do not have perimeter protection as strong as the primary connection.

B. This information can be found by calling the regional Internet registry, and is valuable because backup connections typically do not require VPN access to the network.

C. This information can be found by accessing telecom billing records, and is valuable because backup connections typically have much lower latency than primary connections.

D. This information can be found by querying the network\\'s DNS servers, and is valuable because backup DNS servers typically allow recursive queries from Internet hosts.

Correct Answer: A

A routing table is a set of rules, often viewed in table format that is used to determine where data packets traveling over an Internet Protocol (IP) network will be directed. All IP- enabled devices, including routers and switches, use routing tables. Each packet contains information about its origin and destination. When a packet is received, a network device examines the packet and matches it to the routing table entry providing the best match for its destination. The table then provides the device with instructions for sending the packet to the next hop on its route across the network. Thus the

security consultant can use the global routing table to get the appropriate information.

QUESTION 6

Company A is merging with Company B. Company B uses mostly hosted services from an outside vendor, while Company A uses mostly in-house products. The project manager of the merger states the merged systems should meet these goals:

-Ability to customize systems per department

-Quick implementation along with an immediate ROI

-The internal IT team having administrative level control over all products

The project manager states the in-house services are the best solution. Because of staff shortages, the senior security administrator argues that security will be best maintained by continuing to use outsourced services. Which of the following solutions BEST solves the disagreement?

A. Raise the issue to the Chief Executive Officer (CEO) to escalate the decision to senior management with the recommendation to continue the outsourcing of all IT services.

B. Calculate the time to deploy and support the in-sourced systems accounting for the staff shortage and compare the costs to the ROI costs minus outsourcing costs. Present the document numbers to management for a final decision.

C. Perform a detailed cost benefit analysis of outsourcing vs. in-sourcing the IT systems and review the system documentation to assess the ROI of in-sourcing. Select COTS products to eliminate development time to meet the ROI goals.

D. Arrange a meeting between the project manager and the senior security administrator to review the requirements and determine how critical all the requirements are.

Correct Answer: B

QUESTION 7

A company has received the contract to begin developing a new suite of software tools to replace an aging collaboration solution. The original collaboration solution has been in place for nine years, contains over a million lines of code, and took over two years to develop originally. The SDLC has been broken up into eight primary stages, with each stage requiring an in-depth risk analysis before moving on to the next phase. Which of the following software development methods is MOST applicable?

A. Spiral model

B. Incremental model

C. Waterfall model

D. Agile model

Correct Answer: C

The waterfall model is a sequential software development processes, in which progress is seen as flowing steadily downwards through identified phases.

QUESTION 8

A security manager for a service provider has approved two vendors for connections to the service provider backbone. One vendor will be providing authentication services for its payment card service, and the other vendor will be providing maintenance to the service provider infrastructure sites. Which of the following business agreements is MOST relevant to the vendors and service provider\\'s relationship?

A. Memorandum of Agreement

B. Interconnection Security Agreement

C. Non-Disclosure Agreement

D. Operating Level Agreement

Correct Answer: B

The Interconnection Security Agreement (ISA) is a document that identifies the requirements for connecting systems and networks and details what security controls are to be used to protect the systems and sensitive data.

QUESTION 9

During a recent audit of servers, a company discovered that a network administrator, who required remote access, had deployed an unauthorized remote access application that communicated over common ports already allowed through the firewall. A network scan showed that this remote access application had already been installed on one third of the servers in the company. Which of the following is the MOST appropriate action that the company should take to provide a more appropriate solution?

A. Implement an IPS to block the application on the network

B. Implement the remote application out to the rest of the servers

C. Implement SSL VPN with SAML standards for federation

D. Implement an ACL on the firewall with NAT for remote access

Correct Answer: C

A Secure Sockets Layer (SSL) virtual private network (VPN) would provide the network administrator who requires remote access a secure and reliable method of accessing the system over the Internet. Security Assertion Markup Language (SAML) standards for federation will provide cross-web service authentication and authorization.

QUESTION 10

An extensible commercial software system was upgraded to the next minor release version to patch a security vulnerability. After the upgrade, an unauthorized intrusion into the system was detected. The software vendor is called in to troubleshoot the issue and reports that all core components were updated properly. Which of the following has been overlooked in securing the system? (Select TWO).

A. The company\\'s IDS signatures were not updated.

B. The company\\'s custom code was not patched.

C. The patch caused the system to revert to http.

D. The software patch was not cryptographically signed.

E. The wrong version of the patch was used.

F. Third-party plug-ins were not patched.

Correct Answer: BF

In this question, we have an extensible commercial software system. Extensibility is a software design principle defined as a system\\'s ability to have new functionality extended, in which the system\\'s internal structure and data flow are

minimally or not affected, particularly that recompiling or changing the original source code is unnecessary when changing a system\\'s behavior, either by the creator or other programmers.

Extensible systems are typically modified either by custom code or third party plugins. In this question, the core application was updated/patched. However, the custom code and third-party plugins were not patched. Therefore, a security

vulnerability remained with was exploited.

QUESTION 11

A manufacturer is planning to build a segregated network. There are requirements to segregate development and test infrastructure from production and the need to support multiple entry points into the network depending on the service being accessed. There are also strict rules in place to only permit user access from within the same zone. Currently, the following access requirements have been identified:

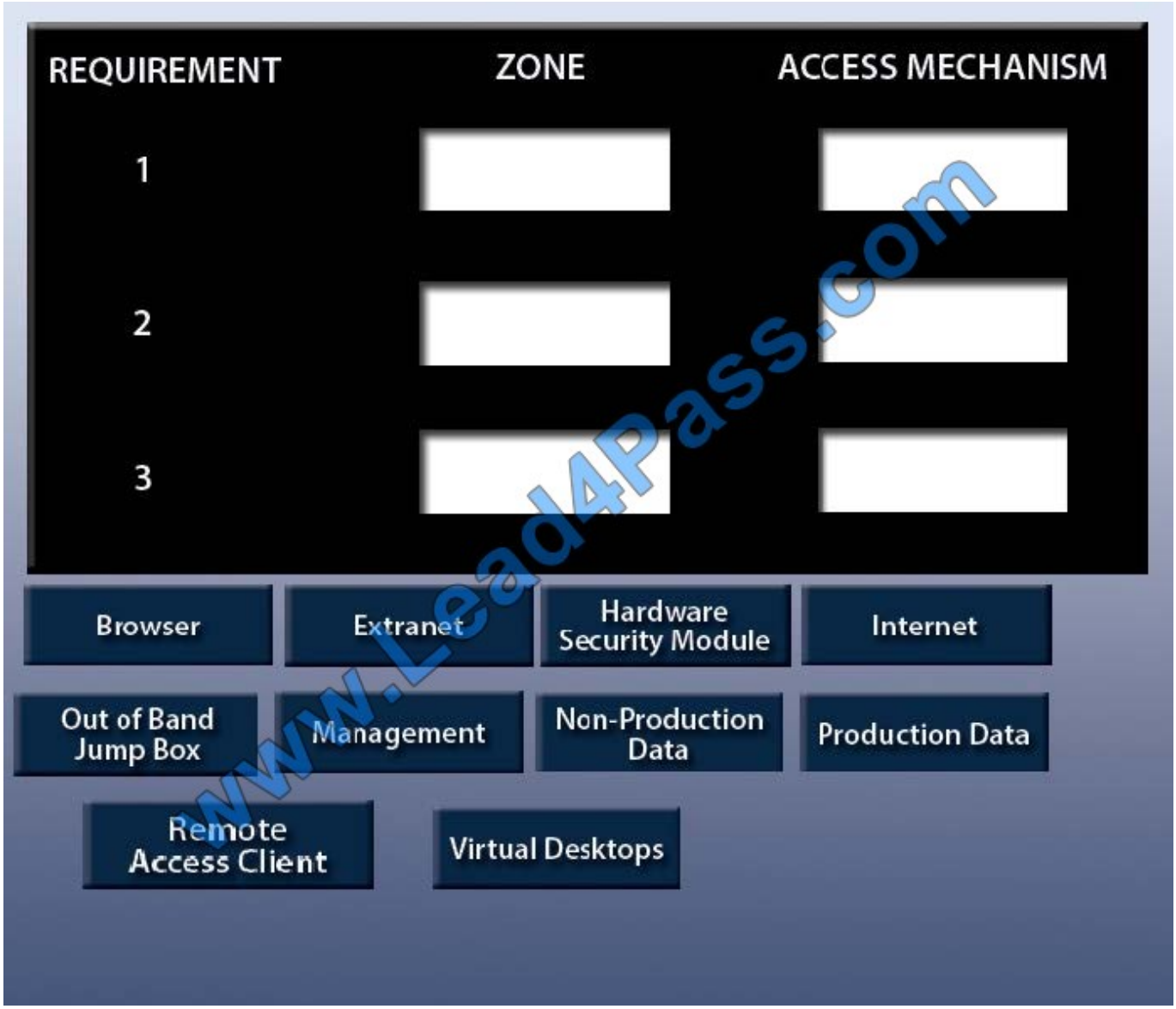
Developers have the ability to perform technical validation of development applications.

End users have the ability to access internal web applications.

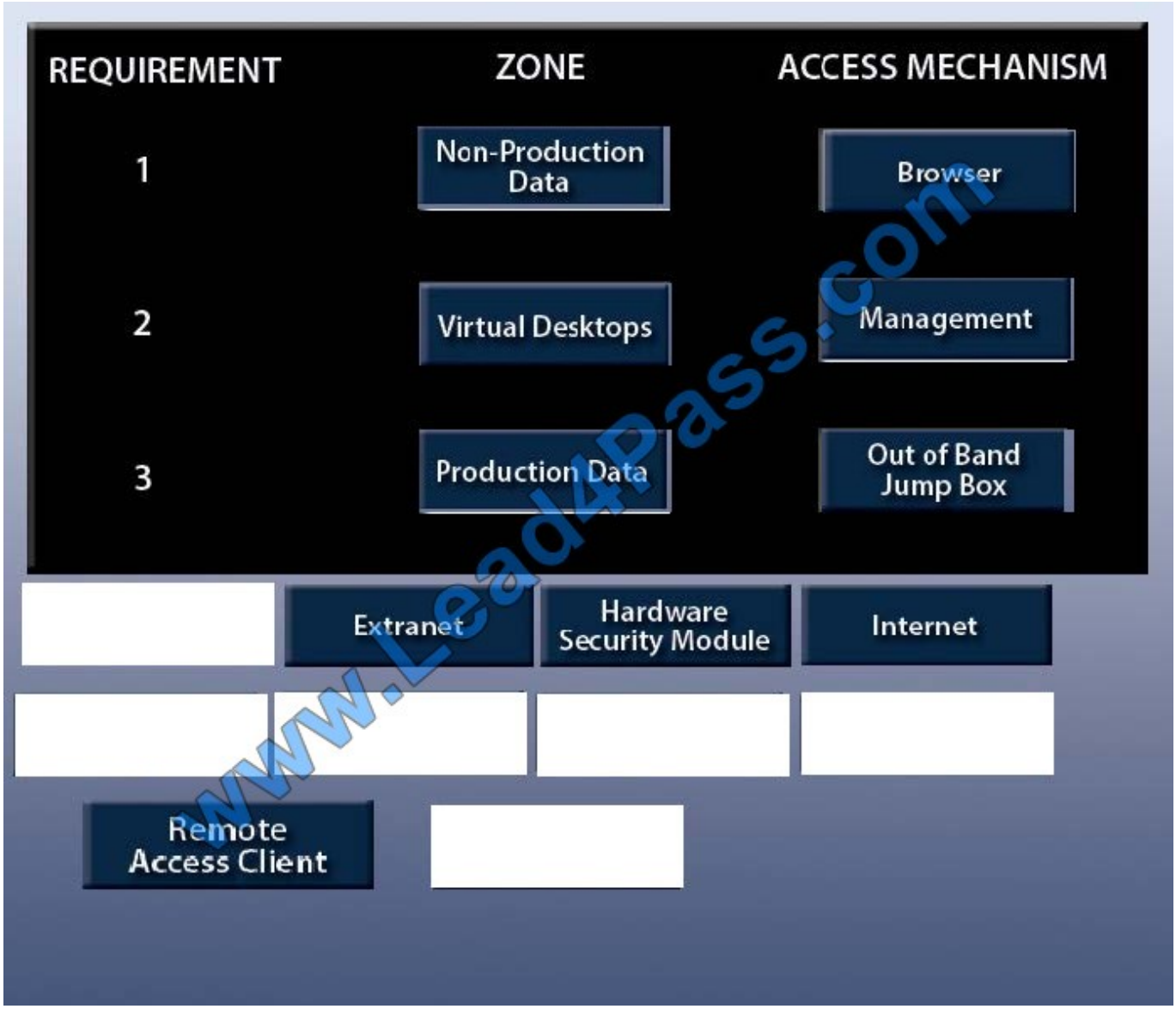
Third-party vendors have the ability to support applications.

In order to meet segregation and access requirements, drag and drop the appropriate network zone that the user would be accessing and the access mechanism to meet the above criteria. Options may be used once or not at all. All placeholders must be filled.

Select and Place:



Correct Answer:



QUESTION 12

The latest independent research shows that cyber attacks involving SCADA systems grew an average of 15% per year in each of the last four years, but that this year\\'s growth has slowed to around 7%. Over the same time period, the number of attacks against applications has decreased or stayed flat each year. At the start of the measure period, the incidence of PC boot loader or BIOS based attacks was negligible. Starting two years ago, the growth in the number of PC boot loader attacks has grown exponentially. Analysis of these trends would seem to suggest which of the following strategies should be employed?

A. Spending on SCADA protections should stay steady; application control spending should increase substantially and spending on PC boot loader controls should increase substantially.

B. Spending on SCADA security controls should stay steady; application control spending should decrease slightly and spending on PC boot loader protections should increase substantially.

C. Spending all controls should increase by 15% to start; spending on application controls should be suspended, and PC boot loader protection research should increase by 100%.

D. Spending on SCADA security controls should increase by 15%; application control spending should increase slightly, and spending on PC boot loader protections should remain steady.

Correct Answer: B

Spending on the security controls should stay steady because the attacks are still ongoing albeit reduced in occurrence Due to the incidence of BIOS-based attacks growing exponentially as the application attacks being decreased or staying flat spending should increase in this field.

QUESTION 13

A security architect has been engaged during the implementation stage of the SDLC to review a new HR software installation for security gaps. With the project under a tight schedule to meet market commitments on project delivery, which of the following security activities should be prioritized by the security architect? (Select TWO).

A. Perform penetration testing over the HR solution to identify technical vulnerabilities

B. Perform a security risk assessment with recommended solutions to close off high-rated risks

C. Secure code review of the HR solution to identify security gaps that could be exploited

D. Perform access control testing to ensure that privileges have been configured correctly

E. Determine if the information security standards have been complied with by the project

Correct Answer: BE

In this question, we are pushed for time to get the project completed. Therefore, we have to prioritize our security testing as we do not have time to fully test everything. One of the priorities from a security perspective should be to perform a security risk assessment with recommended solutions to close off high-rated risks. This is to test for the most potentially damaging risks and to remediate them. The other priority is to determine if the information security standards have been complied with by the project. Security of information/data is the most important aspect of security. Loss of data can be very damaging for a company in terms of liability and litigation.

QUESTION 14

A trust relationship has been established between two organizations with web based services. One organization is acting as the Requesting Authority (RA) and the other acts as the Provisioning Service Provider (PSP). Which of the following is correct about the trust relationship?

A. The trust relationship uses SAML in the SOAP header. The SOAP body transports the SPML requests / responses.

B. The trust relationship uses XACML in the SAML header. The SAML body transports the SOAP requests / responses.

C. The trust relationship uses SPML in the SOAP header. The SOAP body transports the SAML requests / responses.

D. The trust relationship uses SPML in the SAML header. The SAML body transports the SPML requests / responses.

Correct Answer: A

QUESTION 15

A company has noticed recently that its corporate information has ended up on an online forum. An investigation has identified that internal employees are sharing confidential corporate information on a daily basis. Which of the following are the MOST effective security controls that can be implemented to stop the above problem? (Select TWO).

A. Implement a URL filter to block the online forum

B. Implement NIDS on the desktop and DMZ networks

C. Security awareness compliance training for all employees

D. Implement DLP on the desktop, email gateway, and web proxies

E. Review of security policies and procedures

Correct Answer: CD

Security awareness compliance training for all employees should be implemented to educate employees about corporate policies and procedures for working with information technology (IT). Data loss prevention (DLP) should be implemented to make sure that users do not send sensitive or critical information outside the corporate network.