Question #1 *Topic 1*

Scenario: Northstorm is an online retail shop offering unique vintage and modern accessories. It initially entered a small market but gradually grew thanks to the development of the overall e-commerce landscape. Northstorm works exclusively on line and ensures efficient payment processing, inventory management, marketing tools, and shipment orders. It uses prioritized ordering to receive, restock, and ship its most popular products.

Northstorm has traditionally managed its IT operations by hosting its website and maintaining full control over its infrastructure, including hardware, software, and data administration. However, this approach hindered its growth due to the lack of responsive infrastructure. Seeking to enhance its e-commerce and payment systems, Northstorm opted to expand its in-house data centers, completing the expansion in two phases over three months. Initially, the company upgraded its core servers, point-of-sale, ordering, billing, database, and backup systems. The second phase involved improving mail, payment, and network functionalities. Additionally, during this phase, Northstorm adopted an international standard for personal identifiable information (PII) controllers and PII processors regarding PII processing to ensure its data handling practices were secure and compliant with global regulations.

Despite the expansion, Northstorm's upgraded data centers failed to meet its evolving business demands. This inadequacy led to several new challenges, including issues with order prioritization. Customers reported not receiving priority orders, and the company struggled with responsiveness. This was largely due to the main server's inability to process orders from YouDecide, an application designed to prioritize orders and simulate customer interactions. The application, reliant on advanced algorithms, was incompatible with the new operating system (OS) installed during the upgrade.

Faced with urgent compatibility issues, Northstorm quickly patched the application without proper validation, leading to the installation of a compromised version. This security lapse resulted in the main server being affected and the company's website going offline for a week.

Recognizing the need for a more reliable solution, the company decided to outsource its website hosting to an e-commerce provider. The company signed a confidentiality agreement concerning product ownership and conducted a thorough review of user access rights to enhance security before transitioning.

Based on the scenario above, answer the following question:

Which of the following situations represents a vulnerability in Northstorm's systems?

A. The new version of the application directly affected the main server

B. The need for a replacement version of the application

C. The new version of the application was not legitimate

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

Scenario: Northstorm is an online retail shop offering unique vintage and modern accessories. It initially entered a small market but gradually grew thanks to the development of the overall e-commerce landscape. Northstorm works exclusively on line and ensures efficient payment processing, inventory management, marketing tools, and shipment orders. It uses prioritized ordering to receive, restock, and ship its most popular products.

Northstorm has traditionally managed its IT operations by hosting its website and maintaining full control over its infrastructure, including hardware, software, and data administration. However, this approach hindered its growth due to the lack of responsive infrastructure. Seeking to enhance its e-commerce and payment systems, Northstorm opted to expand its in-house data centers, completing the expansion in two phases over three months. Initially, the company upgraded its core servers, point-of-sale, ordering, billing, database, and backup systems. The second phase involved improving mail, payment, and network functionalities. Additionally, during this phase, Northstorm adopted an international standard for personal identifiable information (PII) controllers and PII processors regarding PII processing to ensure its data handling practices were secure and compliant with global regulations.

Despite the expansion, Northstorm's upgraded data centers failed to meet its evolving business demands. This inadequacy led to several new challenges, including issues with order prioritization. Customers reported not receiving priority orders, and the company struggled with responsiveness. This was largely due to the main server's inability to process orders from YouDecide, an application designed to prioritize orders and simulate customer interactions. The application, reliant on advanced algorithms, was incompatible with the new operating system (OS) installed during the upgrade.

Faced with urgent compatibility issues, Northstorm quickly patched the application without proper validation, leading to the installation of a compromised version. This security lapse resulted in the main server being affected and the company's website going offline for a week.

Recognizing the need for a more reliable solution, the company decided to outsource its website hosting to an e-commerce provider. The company signed a confidentiality agreement concerning product ownership and conducted a thorough review of user access rights to enhance security before transitioning.

Which principle of information security has been affected regarding the website issue in scenario?

A. Availability, because Northstorm's website was unavailable

B. Integrity, because the new operating system did not support the application

C. Confidentiality, because Northstorm's website was hosted on the provider's servers

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

Scenario: Northstorm is an online retail shop offering unique vintage and modern accessories. It initially entered a small market but gradually grew thanks to the development of the overall e-commerce landscape. Northstorm works exclusively on line and ensures efficient payment processing, inventory management, marketing tools, and shipment orders. It uses prioritized ordering to receive, restock, and ship its most popular products.

Northstorm has traditionally managed its IT operations by hosting its website and maintaining full control over its infrastructure, including hardware, software, and data administration. However, this approach hindered its growth due to the lack of responsive infrastructure. Seeking to enhance its e-commerce and payment systems, Northstorm opted to expand its in-house data centers, completing the expansion in two phases over three months. Initially, the company upgraded its core servers, point-of-sale, ordering, billing, database, and backup systems. The second phase involved improving mail, payment, and network functionalities. Additionally, during this phase, Northstorm adopted an international standard for personal identifiable information (PII) controllers and PII processors regarding PII processing to ensure its data handling practices were secure and compliant with global regulations.

Despite the expansion, Northstorm's upgraded data centers failed to meet its evolving business demands. This inadequacy led to several new challenges, including issues with order prioritization. Customers reported not receiving priority orders, and the company struggled with responsiveness. This was largely due to the main server's inability to process orders from YouDecide, an application designed to prioritize orders and simulate customer interactions. The application, reliant on advanced algorithms, was incompatible with the new operating system (OS) installed during the upgrade.

Faced with urgent compatibility issues, Northstorm quickly patched the application without proper validation, leading to the installation of a compromised version. This security lapse resulted in the main server being affected and the company's website going offline for a week.

Recognizing the need for a more reliable solution, the company decided to outsource its website hosting to an e-commerce provider. The company signed a confidentiality agreement concerning product ownership and conducted a thorough review of user access rights to enhance security before transitioning.

Which of the following is a preventive control based on scenario?

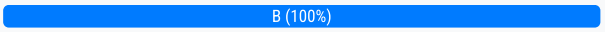
A. Using an application that prioritized orders based on its prior knowledge

B. Signing a confidentiality agreement

C. Expanding the capacity of the in-house data center

Suggested Answer: *C*

Community vote distribution



igizet 3 months ago

Selected Answer: B

Signing a confidentiality agreement concerning product ownership is a clear preventive control, as it helps prevent misuse or leakage of sensitive intellectual property.

upvoted 1 times

BB4 7 months, 2 weeks ago

Selected Answer: B

Expansion was in response to on prem being not responsive enough for the expansion. it was corrective not preventive

upvoted 2 times

Question #4 *Topic 1*

Scenario: Northstorm is an online retail shop offering unique vintage and modern accessories. It initially entered a small market but gradually grew thanks to the development of the overall e-commerce landscape. Northstorm works exclusively on line and ensures efficient payment processing, inventory management, marketing tools, and shipment orders. It uses prioritized ordering to receive, restock, and ship its most popular products.

Northstorm has traditionally managed its IT operations by hosting its website and maintaining full control over its infrastructure, including hardware, software, and data administration. However, this approach hindered its growth due to the lack of responsive infrastructure. Seeking to enhance its e-commerce and payment systems, Northstorm opted to expand its in-house data centers, completing the expansion in two phases over three months. Initially, the company upgraded its core servers, point-of-sale, ordering, billing, database, and backup systems. The second phase involved improving mail, payment, and network functionalities. Additionally, during this phase, Northstorm adopted an international standard for personal identifiable information (PII) controllers and PII processors regarding PII processing to ensure its data handling practices were secure and compliant with global regulations.

Despite the expansion, Northstorm's upgraded data centers failed to meet its evolving business demands. This inadequacy led to several new challenges, including issues with order prioritization. Customers reported not receiving priority orders, and the company struggled with responsiveness. This was largely due to the main server's inability to process orders from YouDecide, an application designed to prioritize orders and simulate customer interactions. The application, reliant on advanced algorithms, was incompatible with the new operating system (OS) installed during the upgrade.

Faced with urgent compatibility issues, Northstorm quickly patched the application without proper validation, leading to the installation of a compromised version. This security lapse resulted in the main server being affected and the company's website going offline for a week.

Recognizing the need for a more reliable solution, the company decided to outsource its website hosting to an e-commerce provider. The company signed a confidentiality agreement concerning product ownership and conducted a thorough review of user access rights to enhance security before transitioning.

According to scenario, Northstorm reviewed users' access rights. What is the type and function of this security control?

A. Detective and administrative

B. Corrective and managerial

C. Legal and technical

Suggested Answer: *A*

Community vote distribution

B (100%)

bd95cd5 1 week, 1 day ago

Selected Answer: B

Why not corrective? It was a post-incident governance measure to strengthen access control and prevent recurrence, not a monitoring or detection activity.

upvoted 1 times

Question #5 *Topic 1*

Scenario: Northstorm is an online retail shop offering unique vintage and modern accessories. It initially entered a small market but gradually grew thanks to the development of the overall e-commerce landscape. Northstorm works exclusively on line and ensures efficient payment processing, inventory management, marketing tools, and shipment orders. It uses prioritized ordering to receive, restock, and ship its most popular products.

Northstorm has traditionally managed its IT operations by hosting its website and maintaining full control over its infrastructure, including hardware, software, and data administration. However, this approach hindered its growth due to the lack of responsive infrastructure. Seeking to enhance its e-commerce and payment systems, Northstorm opted to expand its in-house data centers, completing the expansion in two phases over three months. Initially, the company upgraded its core servers, point-of-sale, ordering, billing, database, and backup systems. The second phase involved improving mail, payment, and network functionalities. Additionally, during this phase, Northstorm adopted an international standard for personal identifiable information (PII) controllers and PII processors regarding PII processing to ensure its data handling practices were secure and compliant with global regulations.

Despite the expansion, Northstorm's upgraded data centers failed to meet its evolving business demands. This inadequacy led to several new challenges, including issues with order prioritization. Customers reported not receiving priority orders, and the company struggled with responsiveness. This was largely due to the main server's inability to process orders from YouDecide, an application designed to prioritize orders and simulate customer interactions. The application, reliant on advanced algorithms, was incompatible with the new operating system (OS) installed during the upgrade.

Faced with urgent compatibility issues, Northstorm quickly patched the application without proper validation, leading to the installation of a compromised version. This security lapse resulted in the main server being affected and the company's website going offline for a week.

Recognizing the need for a more reliable solution, the company decided to outsource its website hosting to an e-commerce provider. The company signed a confidentiality agreement concerning product ownership and conducted a thorough review of user access rights to enhance security before transitioning.

Based on scenario, which international standard did Northstorm adopt during the second phase of expansion?

A. ISO/IEC 27701

B. ISO/IEC 27009

C. ISO/IEC 27003

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

After an information security incident, an organization created a comprehensive backup procedure involving regular, automated backups of all critical data to offsite storage locations. By doing so, which principle of information security is the organization applying in this case?

A. Integrity

B. Confidentiality

C. Availability

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

A data processing tool crashed when a user added more data to the buffer than its storage capacity allows. The incident was caused by the tool's inability to bound check arrays. What kind of vulnerability is this?

A. Intrinsic vulnerability, i.e., inability to bound check arrays, is a characteristic of the data processing tool

B. Extrinsic vulnerability, i.e., the exploit of the buffer overflow vulnerability, is caused by an external factor

C. None; buffer overflow is not a vulnerability; it is a threat

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

Which of the following best defines managerial controls?

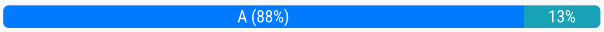
A. Controls related to the management of personnel, including training of employees, management reviews, and internal audits

B. Controls related to organizational structure, such as segregation of duties, job rotations, job descriptions, and approval processes

C. Controls related to the use of technical measures or technologies, such as firewalls, alarm systems, surveillance cameras, and IDSs

Suggested Answer: *A*

Community vote distribution



Cyza 4 months, 1 week ago

Selected Answer: A

According to the literature available, that is what a managerial control is and B is an administrative control while C is a technical control.

upvoted 1 times

rynzo 6 months, 1 week ago

Selected Answer: A

The answer is A. B is administrative control, and C is technical control.

upvoted 2 times

Szichen 7 months ago

Selected Answer: A

The best answer is A because that's what the notes state.

upvoted 2 times

BB4 7 months, 2 weeks ago

Selected Answer: A

Training, coaching and management review are managerial controls

upvoted 2 times

adili 8 months, 2 weeks ago

Selected Answer: B

The best answer is:

B. Controls related to the organizational structure, such as segregation of duties, job rotation, job descriptions, and approval processes.

Management controls are mechanisms put in place to ensure that an organization's strategic and operational objectives are achieved effectively. They include practices such as segregation of duties, approval processes, and organizational governance, which align with option B.

Option A refers more to administrative controls and oversight mechanisms.
Option C pertains to technical and physical security controls, such as firewalls, alarm systems, surveillance cameras, and IDS (Intrusion Detection Systems).

upvoted 1 times

Question #9 *Topic 1*

What is the objective of penetration testing in the risk assessment process?

A. To conduct thorough code reviews

B. To identify potential failures in the ICT protection schemes

C. To physically inspect hardware components

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Which controls are related to the Annex A controls of ISO/IEC 27001 and are often selected from other guides and standards or defined by the organization to meet its specific needs?

A. General controls

B. Strategic controls

C. Specific controls

Suggested Answer: *A*

Community vote distribution

Cyza 4 months, 1 week ago

Selected Answer: A

According to literature, A is the answer.

upvoted 1 times

ROCTW 5 months ago

Selected Answer: C

ISO/IEC 27001 Annex A provides a comprehensive list of information security controls. However, it's not a prescriptive "must-do" list. Organizations are required to conduct a risk assessment and then select the controls from Annex A (and potentially other sources) that are relevant to their specific risks and operational environment.

"Specific controls" refers to these chosen controls that are tailored to the organization's unique needs, often drawing from various sources beyond just Annex A, or even defining new controls as necessary.

upvoted 3 times

hussain_rj2 9 months, 1 week ago

Selected Answer: A

Annex A, is a general controls.

upvoted 2 times

Question #11 *Topic 1*

Which of the following statements regarding threats and vulnerabilities in information security is NOT correct?

A. Vulnerabilities can be intrinsic or extrinsic, related to the characteristics of the asset or to external factors

B. Threats must exploit a vulnerability to have a negative impact on the confidentiality, integrity, and/or availability of information

C. All vulnerabilities require immediate implementation of controls regardless of corresponding threats

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

Which situation presented below represents a threat?

A. An employee accesses unauthorized files using their legitimate credentials

B. An organization fails to implement multi-factor authentication (MFA) for its cloud services

C. Cyber attackers infiltrated the network by exploiting a zero-day vulnerability in the organization's firewall software

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

A cybersecurity company implemented an access control software that allows only authorized personnel to access sensitive files. Which type of control has the company implemented in this case?

A. Preventive control

B. Detective control

C. Corrective control

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

Scenario: Clinic, founded in the 1990s, is a medical device company that specializes in treatments for heart-related conditions and complex surgical interventions. Based in Europe, it serves both patients and healthcare professionals. Clinic collects patient data to tailor treatments, monitor outcomes, and improve device functionality. To enhance data security and build trust, Clinic is implementing an information security management system (ISMS) based on ISO/IEC 27001. This initiative demonstrates Clinic's commitment to securely managing sensitive patient information and its proprietary technologies.

Clinic established the scope of its ISMS by solely considering internal issues, interfaces and dependencies between activities conducted internally and those outsourced to other organizations, and the expectations of interested parties. This scope was carefully documented and made accessible. In defining its ISMS, Clinic chose to focus specifically on key processes within critical departments such as Research and Development, Patient Data Management, and Customer Support.

Despite initial challenges. Clinic remained committed to its ISMS implementation, tailoring security controls to its unique needs. The project team excluded certain Annex A controls from ISO/IEC 27001, incorporating additional sector-specific controls to enhance security. The project team meticulously evaluated the applicability of these controls against internal and external factors, culminating in developing a comprehensive Statement of Applicability (SoA) detailing the rationale behind control selection and implementation.

As preparations for certification progressed, Brian, appointed as the team leader for the project team, adopted a self-directed risk assessment methodology to identify and evaluate the company, strategic issues, and security practices. This proactive approach ensured that Clinic's risk assessment aligned with its objectives and missions.

Based on the scenario above, answer the following question:

Does the Clinic's SoA document meet the ISO/IEC 27001 requirements for the SoA?

A. Yes, because it comprises an exhaustive list of controls considered applicable from Annex A of ISO/IEC 27001 and the other sources

B. No, because security controls selected from sources other than Annex A of ISO/IEC 27001 are included

C. No. because it does not contain the justification for the exclusion of controls from Annex A of ISO/IEC 27001

Suggested Answer: *C*

Community vote distribution

C (100%)

SuperMax 9 months, 2 weeks ago

Selected Answer: C

According to ISO/IEC 27001, the Statement of Applicability (SoA) must meet specific requirements, including:

Listing the applicable controls from Annex A: The SoA must include controls selected from Annex A of ISO/IEC 27001.

Justifying exclusions: If any controls from Annex A are excluded, the SoA must provide a clear justification for their exclusion.

Incorporating additional controls (if applicable): Organizations can include controls from other sources if necessary, but this does not negate the requirement to justify any exclusions from Annex A.

In the scenario, while the project team evaluates the applicability of Annex A controls and includes sector-specific controls, the question does not mention that the exclusions from Annex A are justified. This omission means the SoA does not fully meet ISO/IEC 27001 requirements.

upvoted 4 times

Question #15 *Topic 1*

Scenario: Clinic, founded in the 1990s, is a medical device company that specializes in treatments for heart-related conditions and complex surgical interventions. Based in Europe, it serves both patients and healthcare professionals. Clinic collects patient data to tailor treatments, monitor outcomes, and improve device functionality. To enhance data security and build trust, Clinic is implementing an information security management system (ISMS) based on ISO/IEC 27001. This initiative demonstrates Clinic's commitment to securely managing sensitive patient information and its proprietary technologies.

Clinic established the scope of its ISMS by solely considering internal issues, interfaces and dependencies between activities conducted internally and those outsourced to other organizations, and the expectations of interested parties. This scope was carefully documented and made accessible. In defining its ISMS, Clinic chose to focus specifically on key processes within critical departments such as Research and Development, Patient Data Management, and Customer Support.

Despite initial challenges. Clinic remained committed to its ISMS implementation, tailoring security controls to its unique needs. The project team excluded certain Annex A controls from ISO/IEC 27001, incorporating additional sector-specific controls to enhance security. The project team meticulously evaluated the applicability of these controls against internal and external factors, culminating in developing a comprehensive Statement of Applicability (SoA) detailing the rationale behind control selection and implementation.

As preparations for certification progressed, Brian, appointed as the team leader for the project team, adopted a self-directed risk assessment methodology to identify and evaluate the company, strategic issues, and security practices. This proactive approach ensured that Clinic's risk assessment aligned with its objectives and missions.

According to scenario, was the scope of Clinic's ISMS determined correctly?

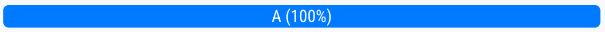
A. No, Clinic should have also considered external issues

B. Yes, the scope of Clinic's ISMS was determined correctly

C. No, Clinic should have also included exclusions along with justifications for them as part of its ISMS scope

Suggested Answer: *A*

Community vote distribution



CloudMasterGuru 8 months, 1 week ago

Selected Answer: A

As per clause 4.1 of determine scope, the organization should consider internal and external issues and also the potential impact of the climate change

upvoted 1 times

Question #16 *Topic 1*

Scenario: Clinic, founded in the 1990s, is a medical device company that specializes in treatments for heart-related conditions and complex surgical interventions. Based in Europe, it serves both patients and healthcare professionals. Clinic collects patient data to tailor treatments, monitor outcomes, and improve device functionality. To enhance data security and build trust, Clinic is implementing an information security management system (ISMS) based on ISO/IEC 27001. This initiative demonstrates Clinic's commitment to securely managing sensitive patient information and its proprietary technologies.

Clinic established the scope of its ISMS by solely considering internal issues, interfaces and dependencies between activities conducted internally and those outsourced to other organizations, and the expectations of interested parties. This scope was carefully documented and made accessible. In defining its ISMS, Clinic chose to focus specifically on key processes within critical departments such as Research and Development, Patient Data Management, and Customer Support.

Despite initial challenges. Clinic remained committed to its ISMS implementation, tailoring security controls to its unique needs. The project team excluded certain Annex A controls from ISO/IEC 27001, incorporating additional sector-specific controls to enhance security. The project team meticulously evaluated the applicability of these controls against internal and external factors, culminating in developing a comprehensive Statement of Applicability (SoA) detailing the rationale behind control selection and implementation.

As preparations for certification progressed, Brian, appointed as the team leader for the project team, adopted a self-directed risk assessment methodology to identify and evaluate the company, strategic issues, and security practices. This proactive approach ensured that Clinic's risk assessment aligned with its objectives and missions.

Based on scenario, Clinic initially defined its information security objectives and then conducted a risk assessment. Is this acceptable?

A. Yes, because objectives can be adjusted later to fit the risk assessment results

B. No, because the risk assessment should be conducted only once objectives are fully implemented

C. No, information security objectives must be established, taking into account risk assessment results, as per ISO/IEC 27001 requirements

Suggested Answer: *C*

Community vote distribution

11b404b 5 months, 3 weeks ago

Selected Answer: C

Answer is C. According to ISO/IEC 27001, you must first conduct a risk assessment to understand the threats, vulnerabilities, and impacts affecting your information security.

upvoted 1 times

Question #17 *Topic 1*

Scenario: Clinic, founded in the 1990s, is a medical device company that specializes in treatments for heart-related conditions and complex surgical interventions. Based in Europe, it serves both patients and healthcare professionals. Clinic collects patient data to tailor treatments, monitor outcomes, and improve device functionality. To enhance data security and build trust, Clinic is implementing an information security management system (ISMS) based on ISO/IEC 27001. This initiative demonstrates Clinic's commitment to securely managing sensitive patient information and its proprietary technologies.

Clinic established the scope of its ISMS by solely considering internal issues, interfaces and dependencies between activities conducted internally and those outsourced to other organizations, and the expectations of interested parties. This scope was carefully documented and made accessible. In defining its ISMS, Clinic chose to focus specifically on key processes within critical departments such as Research and Development, Patient Data Management, and Customer Support.

Despite initial challenges. Clinic remained committed to its ISMS implementation, tailoring security controls to its unique needs. The project team excluded certain Annex A controls from ISO/IEC 27001, incorporating additional sector-specific controls to enhance security. The project team meticulously evaluated the applicability of these controls against internal and external factors, culminating in developing a comprehensive Statement of Applicability (SoA) detailing the rationale behind control selection and implementation.

As preparations for certification progressed, Brian, appointed as the team leader for the project team, adopted a self-directed risk assessment methodology to identify and evaluate the company, strategic issues, and security practices. This proactive approach ensured that Clinic's risk assessment aligned with its objectives and missions.

Based on scenario, the Clinic decided that the ISMS would cover only key processes and departments. Is this acceptable?

A. Yes, but the decision to exclude other processes and departments must be justified

B. Yes, organizations may limit the scope of the ISMS, but they cannot request a certification audit if the ISMS scope does not include all processes and departments

C. No, Clinic must include all processes and departments in the scope, regardless of their importance or relevance to the ISMS

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

Scenario: Clinic, founded in the 1990s, is a medical device company that specializes in treatments for heart-related conditions and complex surgical interventions. Based in Europe, it serves both patients and healthcare professionals. Clinic collects patient data to tailor treatments, monitor outcomes, and improve device functionality. To enhance data security and build trust, Clinic is implementing an information security management system (ISMS) based on ISO/IEC 27001. This initiative demonstrates Clinic's commitment to securely managing sensitive patient information and its proprietary technologies.

Clinic established the scope of its ISMS by solely considering internal issues, interfaces and dependencies between activities conducted internally and those outsourced to other organizations, and the expectations of interested parties. This scope was carefully documented and made accessible. In defining its ISMS, Clinic chose to focus specifically on key processes within critical departments such as Research and Development, Patient Data Management, and Customer Support.

Despite initial challenges. Clinic remained committed to its ISMS implementation, tailoring security controls to its unique needs. The project team excluded certain Annex A controls from ISO/IEC 27001, incorporating additional sector-specific controls to enhance security. The project team meticulously evaluated the applicability of these controls against internal and external factors, culminating in developing a comprehensive Statement of Applicability (SoA) detailing the rationale behind control selection and implementation.

As preparations for certification progressed, Brian, appointed as the team leader for the project team, adopted a self-directed risk assessment methodology to identify and evaluate the company, strategic issues, and security practices. This proactive approach ensured that Clinic's risk assessment aligned with its objectives and missions.

Based on scenario, which methodology did Brian choose to conduct risk assessment?

A. OCTAVE

B. MEHARI

C. EBIOS

Suggested Answer: *A*

Community vote distribution

A (100%)

SuperMax 9 months, 2 weeks ago

Selected Answer: A

The scenario describes Brian adopting a self-directed risk assessment methodology tailored to the company's needs. While the scenario does not explicitly name a specific methodology, the characteristics of the approach align with certain methodologies commonly used for risk assessment.

upvoted 3 times

Question #19 *Topic 1*

According to ISO/IEC 27001, clause 5.1, Leadership and commitment, which of the following is NOT a responsibility of top management?

A. Ensuring the availability of resources for the ISMS and promoting continual improvement

B. Conducting regular internal audits to assess the effectiveness of the ISMS

C. Directing and supporting persons to contribute to the effectiveness of the ISMS

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

A marketing agency has developed its risk assessment approach as part of the ISMS implementation. Is this acceptable?

A. Yes, any risk assessment methodology that complies with the ISO/IEC 27001 requirements can be used

B. Yes, only if the risk assessment methodology is aligned with recognized risk assessment methodologies

C. No, the risk assessment methodology provided by ISO/IEC 27001 should be used when implementing an ISMS

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

Which of the following statements regarding documented information in an organization's ISMS is incorrect?

A. The purpose of documented information is to guide the ISMS operation and provide evidence of process effectiveness

B. The collection of documented information should be a target in itself

C. Documented information should not be detailed and complex to ensure thoroughness

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Scenario: Cobt, an insurance company in London, offers various commercial, industrial, and life insurance solutions. In recent years, the number of Cobt's clients has increased enormously. Having a huge amount of data to process, the company decided that certifying against ISO/IEC 27001 would bring many benefits to securing information and show its commitment to continual improvement. While the company was well-versed in conducting regular risk assessments, implementing an ISMS brought major changes to its daily operations. During the risk assessment process, a risk was identified where significant defects occurred without being detected or prevented by the organization's internal control mechanisms.
The company followed a methodology to implement the ISMS and had an operational ISMS in place after only a few months. After successfully implementing the ISMS, Cobt applied for ISO/IEC 27001 certification. Sarah, an experienced auditor, was assigned to the audit. Upon thoroughly analyzing the audit offer, Sarah accepted her responsibilities as an audit team leader and immediately started to obtain general information about Cobt. She established the audit criteria and objective, planned the audit, and assigned the audit team members' responsibilities.
Sarah acknowledged that although Cobt has expanded significantly by offering diverse commercial and insurance solutions, it still relies on some manual processes. Therefore, her initial focus was to gather information on how the company manages its information security risks. Sarah contacted Gobt's representatives to request access to information related to risk management for the off-site review, as initially agreed upon for part of the audit. However, Cobt later refused, claiming that such information is too sensitive to be accessed outside of the company. This refusal raised concerns about the audit's feasibility, particularly regarding the availability and cooperation of the auditee and access to evidence.
Moreover, Cobt raised concerns about the audit schedule, stating that it does not property reflect the recent changes the company made. It pointed out that the actions to be performed during the audit apply only to the initial scope and do not encompass the latest changes made in the audit scope.
Sarah also evaluated the materiality of the situation, considering the significance of the information denied for the audit objectives. In this case, the refusal by Cobt raised questions about the completeness of the audit and its ability to provide reasonable assurance. Following these situations, Sarah decided to withdraw from the audit before a certification agreement was signed and communicated her decision to Cobt and the certification body. This decision was made to ensure adherence to audit principles and maintain transparency, highlighting her commitment to consistently upholding these principles.
Based on the scenario above, answer the following question:
What type of risk did Cobt identify during the last risk assessment?

A. Inherent risk

B. Control risk

C. Detection risk

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

Scenario: Cobt, an insurance company in London, offers various commercial, industrial, and life insurance solutions. In recent years, the number of Cobt's clients has increased enormously. Having a huge amount of data to process, the company decided that certifying against ISO/IEC 27001 would bring many benefits to securing information and show its commitment to continual improvement. While the company was well-versed in conducting regular risk assessments, implementing an ISMS brought major changes to its daily operations. During the risk assessment process, a risk was identified where significant defects occurred without being detected or prevented by the organization's internal control mechanisms.
The company followed a methodology to implement the ISMS and had an operational ISMS in place after only a few months. After successfully implementing the ISMS, Cobt applied for ISO/IEC 27001 certification. Sarah, an experienced auditor, was assigned to the audit. Upon thoroughly analyzing the audit offer, Sarah accepted her responsibilities as an audit team leader and immediately started to obtain general information about Cobt. She established the audit criteria and objective, planned the audit, and assigned the audit team members' responsibilities.
Sarah acknowledged that although Cobt has expanded significantly by offering diverse commercial and insurance solutions, it still relies on some manual processes. Therefore, her initial focus was to gather information on how the company manages its information security risks. Sarah contacted Gobt's representatives to request access to information related to risk management for the off-site review, as initially agreed upon for part of the audit. However, Cobt later refused, claiming that such information is too sensitive to be accessed outside of the company. This refusal raised concerns about the audit's feasibility, particularly regarding the availability and cooperation of the auditee and access to evidence.
Moreover, Cobt raised concerns about the audit schedule, stating that it does not property reflect the recent changes the company made. It pointed out that the actions to be performed during the audit apply only to the initial scope and do not encompass the latest changes made in the audit scope.
Sarah also evaluated the materiality of the situation, considering the significance of the information denied for the audit objectives. In this case, the refusal by Cobt raised questions about the completeness of the audit and its ability to provide reasonable assurance. Following these situations, Sarah decided to withdraw from the audit before a certification agreement was signed and communicated her decision to Cobt and the certification body. This decision was made to ensure adherence to audit principles and maintain transparency, highlighting her commitment to consistently upholding these principles.
Based on the role of Sarah described in scenario, which of the following should NOT be part of her responsibilities?

A. Assigning responsibilities to the audit team members

B. Defining the audit criteria and objectives

C. Planning the audit

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

Scenario: Cobt, an insurance company in London, offers various commercial, industrial, and life insurance solutions. In recent years, the number of Cobt's clients has increased enormously. Having a huge amount of data to process, the company decided that certifying against ISO/IEC 27001 would bring many benefits to securing information and show its commitment to continual improvement. While the company was well-versed in conducting regular risk assessments, implementing an ISMS brought major changes to its daily operations. During the risk assessment process, a risk was identified where significant defects occurred without being detected or prevented by the organization's internal control mechanisms.
The company followed a methodology to implement the ISMS and had an operational ISMS in place after only a few months. After successfully implementing the ISMS, Cobt applied for ISO/IEC 27001 certification. Sarah, an experienced auditor, was assigned to the audit. Upon thoroughly analyzing the audit offer, Sarah accepted her responsibilities as an audit team leader and immediately started to obtain general information about Cobt. She established the audit criteria and objective, planned the audit, and assigned the audit team members' responsibilities.
Sarah acknowledged that although Cobt has expanded significantly by offering diverse commercial and insurance solutions, it still relies on some manual processes. Therefore, her initial focus was to gather information on how the company manages its information security risks. Sarah contacted Gobt's representatives to request access to information related to risk management for the off-site review, as initially agreed upon for part of the audit. However, Cobt later refused, claiming that such information is too sensitive to be accessed outside of the company. This refusal raised concerns about the audit's feasibility, particularly regarding the availability and cooperation of the auditee and access to evidence.
Moreover, Cobt raised concerns about the audit schedule, stating that it does not property reflect the recent changes the company made. It pointed out that the actions to be performed during the audit apply only to the initial scope and do not encompass the latest changes made in the audit scope.
Sarah also evaluated the materiality of the situation, considering the significance of the information denied for the audit objectives. In this case, the refusal by Cobt raised questions about the completeness of the audit and its ability to provide reasonable assurance. Following these situations, Sarah decided to withdraw from the audit before a certification agreement was signed and communicated her decision to Cobt and the certification body. This decision was made to ensure adherence to audit principles and maintain transparency, highlighting her commitment to consistently upholding these principles.
Based on the information provided in scenario, Cobt refused to provide the auditors with information on risk management. How would you, as an auditor, resolve such a situation?

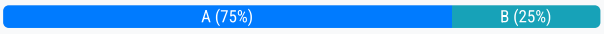
A. By only accessing such information on-site or when Cobt's representatives are present

B. By refusing the audit mandate since it is within an auditor's right to do so when the confidentiality agreement is not followed

C. By reminding Cobt's representatives that the audit team leader decides the access that the audit team should have to information during the audit process

Suggested Answer: *A*

Community vote distribution



ROCTW 5 months ago

Selected Answer: B

ISO 27006 – 9.4.5: If the auditee refuses to cooperate or provide evidence, the certification body should consider withdrawing, refusing, or terminating the audit.

upvoted 1 times

8e1c45b 8 months, 3 weeks ago

Selected Answer: A

This approach balances the need for thorough auditing with the company's confidentiality requirements, fostering trust and cooperation without jeopardizing the integrity of the audit process.

upvoted 1 times

SuperMax 9 months, 2 weeks ago

Selected Answer: A

This is a balanced approach that respects Cobt's concerns about sensitive information while ensuring the audit can proceed effectively.
ISO/IEC 27001 audits require access to critical information, but auditors can adapt by reviewing sensitive information on-site under supervision to address confidentiality concerns.
B. By refusing the audit mandate since it is within an auditor's right to do so when the confidentiality agreement is not followed:

Refusing the mandate should be the last resort if no other resolution is possible. In this scenario, a refusal would prematurely escalate the situation,

which could be avoided by accommodating Cobt's concerns through on-site access.
C. By reminding Cobt's representatives that the audit team leader decides the access that the audit team should have to information during the audit process:

While technically accurate, this response may be perceived as confrontational and could harm the auditor-auditee relationship. It does not address Cobt's specific concerns about information sensitivity.
upvoted 2 times

Question #25 *Topic 1*

Scenario: Cobt, an insurance company in London, offers various commercial, industrial, and life insurance solutions. In recent years, the number of Cobt's clients has increased enormously. Having a huge amount of data to process, the company decided that certifying against ISO/IEC 27001 would bring many benefits to securing information and show its commitment to continual improvement. While the company was well-versed in conducting regular risk assessments, implementing an ISMS brought major changes to its daily operations. During the risk assessment process, a risk was identified where significant defects occurred without being detected or prevented by the organization's internal control mechanisms.
The company followed a methodology to implement the ISMS and had an operational ISMS in place after only a few months. After successfully implementing the ISMS, Cobt applied for ISO/IEC 27001 certification. Sarah, an experienced auditor, was assigned to the audit. Upon thoroughly analyzing the audit offer, Sarah accepted her responsibilities as an audit team leader and immediately started to obtain general information about Cobt. She established the audit criteria and objective, planned the audit, and assigned the audit team members' responsibilities.
Sarah acknowledged that although Cobt has expanded significantly by offering diverse commercial and insurance solutions, it still relies on some manual processes. Therefore, her initial focus was to gather information on how the company manages its information security risks. Sarah contacted Gobt's representatives to request access to information related to risk management for the off-site review, as initially agreed upon for part of the audit. However, Cobt later refused, claiming that such information is too sensitive to be accessed outside of the company. This refusal raised concerns about the audit's feasibility, particularly regarding the availability and cooperation of the auditee and access to evidence.
Moreover, Cobt raised concerns about the audit schedule, stating that it does not property reflect the recent changes the company made. It pointed out that the actions to be performed during the audit apply only to the initial scope and do not encompass the latest changes made in the audit scope.
Sarah also evaluated the materiality of the situation, considering the significance of the information denied for the audit objectives. In this case, the refusal by Cobt raised questions about the completeness of the audit and its ability to provide reasonable assurance. Following these situations, Sarah decided to withdraw from the audit before a certification agreement was signed and communicated her decision to Cobt and the certification body. This decision was made to ensure adherence to audit principles and maintain transparency, highlighting her commitment to consistently upholding these principles.
Based on scenario, Cobt stated that the audit schedule did not properly reflect the recent changes they made in the audit scope. What should Sarah do in this case?

A. Change the audit schedule as requested by Cobt, as the scope should reflect the status and importance of the activities to be audited

B. Continue the audit with the initial scope since Cobt can request a change in the audit scope only if there are recent changes in technologies in place

C. Change the audit schedule only if Cobt, Sarah, and the certification body agree on the changes in the audit scope

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

Scenario: Cobt, an insurance company in London, offers various commercial, industrial, and life insurance solutions. In recent years, the number of Cobt's clients has increased enormously. Having a huge amount of data to process, the company decided that certifying against ISO/IEC 27001 would bring many benefits to securing information and show its commitment to continual improvement. While the company was well-versed in conducting regular risk assessments, implementing an ISMS brought major changes to its daily operations. During the risk assessment process, a risk was identified where significant defects occurred without being detected or prevented by the organization's internal control mechanisms.
The company followed a methodology to implement the ISMS and had an operational ISMS in place after only a few months. After successfully implementing the ISMS, Cobt applied for ISO/IEC 27001 certification. Sarah, an experienced auditor, was assigned to the audit. Upon thoroughly analyzing the audit offer, Sarah accepted her responsibilities as an audit team leader and immediately started to obtain general information about Cobt. She established the audit criteria and objective, planned the audit, and assigned the audit team members' responsibilities.
Sarah acknowledged that although Cobt has expanded significantly by offering diverse commercial and insurance solutions, it still relies on some manual processes. Therefore, her initial focus was to gather information on how the company manages its information security risks. Sarah contacted Gobt's representatives to request access to information related to risk management for the off-site review, as initially agreed upon for part of the audit. However, Cobt later refused, claiming that such information is too sensitive to be accessed outside of the company. This refusal raised concerns about the audit's feasibility, particularly regarding the availability and cooperation of the auditee and access to evidence.
Moreover, Cobt raised concerns about the audit schedule, stating that it does not property reflect the recent changes the company made. It pointed out that the actions to be performed during the audit apply only to the initial scope and do not encompass the latest changes made in the audit scope.
Sarah also evaluated the materiality of the situation, considering the significance of the information denied for the audit objectives. In this case, the refusal by Cobt raised questions about the completeness of the audit and its ability to provide reasonable assurance. Following these situations, Sarah decided to withdraw from the audit before a certification agreement was signed and communicated her decision to Cobt and the certification body. This decision was made to ensure adherence to audit principles and maintain transparency, highlighting her commitment to consistently upholding these principles.
Based on scenario, Sarah decided to withdraw from the audit before a certification agreement was signed. Is this acceptable?

A. Yes, Sarah can withdraw from the audit, but only if the certification body approves her withdrawal

B. Yes, there is no relation between Sarah's withdrawal from the audit and the certification agreement

C. No, the certification agreement is directly tied to the auditor's presence

Suggested Answer: *B*

Community vote distribution

B (100%)

rckxrun 5 months, 2 weeks ago

Selected Answer: B

The correct answer is: B

upvoted 1 times

8e1c45b 8 months, 3 weeks ago

Selected Answer: B

Sarah's decision to withdraw from the audit is acceptable because her role as the audit team leader is independent of the certification agreement.

upvoted 2 times

Question #27 *Topic 1*

Three auditors were assigned to conduct a certification audit in Company X. Before the audit commenced, the certification body provided the auditors' names and background information to Company X. Company X requested the replacement of one of the auditors because they are a former employee. Is this acceptable?

A. Yes, a situation of conflict of interest is a valid reason to request the replacement of the auditor

B. No, the auditee can request the replacement of the auditor only if a valid reason is presented such as unprofessional conduct or situations with real conflict of interest

C. No, the auditee cannot request the replacement of auditors

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

What is the main reason for sending an engagement letter before the initial contact with the auditee?

A. To confirm the authority to conduct the audit

B. To provide initial audit details and schedule the initial contact

C. To establish the audit objectives

Suggested Answer: *A*

Community vote distribution

B (100%)

ROCTW 5 months ago

Selected Answer: B

The engagement letter serves as the initial communication and a foundational document for the audit process. It sets the stage for the upcoming audit by:

Establishing the Basic Framework: It acts as an "opening statement" for the audit, conveying essential information to the auditee before any direct, face-to-face communication begins.
Setting Expectations: The letter typically outlines the audit's purpose, scope, anticipated timeline, the audit team members (at least the lead auditor), and initial requests for assistance and resources from the auditee. This helps the auditee prepare and understand what to expect.
Scheduling the Next Steps: Most directly, it proposes or confirms the time and method for the initial meeting with the auditee (e.g., the opening meeting or preliminary interviews).

upvoted 1 times

Question #29 *Topic 1*

In a joint audit involving multiple audit teams, how many audit team leaders are typically designated per audit?

A. One audit team leader per audit, regardless of the number of audit teams involved

B. Each audit team appoints its own audit team leader

C. There are no designated audit team leaders in joint audits

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

Why should materiality be considered during the initial contact?

A. To determine the audit duration

B. To define the audit team roles

C. To set the audit objectives

Suggested Answer: *A*

Community vote distribution

A (100%)

8e1c45b 8 months, 1 week ago

Selected Answer: A

Materiality during Initial contact is Determine the duration of the audit , Stage 1 - identify key process, Materiality during stage 2 audit is Adjust the plan based on the materiality of each process or asset.

upvoted 2 times

CloudMasterGuru 8 months, 1 week ago

Selected Answer: A

During the initial contact, materiality is taken into account to determine the duration of the audit based on the inherent risks to the organization.

upvoted 2 times

Question #31 *Topic 1*

During which stage of the audit do auditors identify key processes to be audited and prioritized on the basis of materiality?

A. Initial contact

B. Stage 1 audit

C. Stage 2 audit

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

When multiple offices of a certification body are involved, what must be ensured?

A. Each office has a separate legally enforceable agreement with the client

B. A legally enforceable agreement that covers all sites within the certification scope

C. Only the main office has a legally agreement with the client

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

An organization is evaluating the materiality of different processes within its ISMS. It is assessing the direct expenses involved with personnel, third party services, and general fees. Which factor of materiality is the company primarily considering?

A. Cost of operations

B. Cost of the process

C. Potential cost of errors or nonconformities

Suggested Answer: *A*

Community vote distribution

haaki 1 week, 3 days ago

Selected Answer: B

For an ISMS, the following should be taken into account when determining materiality:
1.Cost of the process (material, software, licensing fees, or a combination of these)
2.Cost of operations (personnel, third party services, general fees, or a combination of these)
upvoted 1 times

Cyza 4 months, 1 week ago

Selected Answer: A

According to literature those costs are directly linked to cost of operations and not process
upvoted 1 times

rckxrun 5 months, 2 weeks ago

Selected Answer: B

The correct answer is: B
These represent the costs directly attributable to the process itself, making B. Cost of the process the correct answer.

A. Cost of operations
Refers to overall operational costs across the organization, not individual processes.
C. Potential cost of errors or nonconformities
Involves estimating future losses due to errors, breaches, or nonconformities—more related to risk impact, not current expenses.
upvoted 1 times

8e1c45b 8 months, 1 week ago

Selected Answer: A

A- Cost of operations
upvoted 1 times

BB4 8 months, 3 weeks ago

Selected Answer: A

Cost of the process (material, software, licensing fees)
Cost of Operations (personnel, third-party services, general fees)
upvoted 1 times

Question #34 *Topic 1*

Scenario: Rebuildy is a construction company located in Bangkok, Thailand, that specializes in designing, building, and maintaining residential buildings. To ensure the security of sensitive project data and client information, Rebuildy decided to implement an ISMS based on ISO/IEC 27001. This included a comprehensive understanding of information security risks, a defined continual improvement approach, and robust business solutions.

The ISMS implementation outcomes are presented below:

Information security is achieved by applying a set of security controls and establishing policies, processes, and procedures.

Security controls are implemented based on risk assessment and aim to eliminate or reduce risks to an acceptable level.

All processes ensure the continual improvement of the ISMS based on the plan-do-check-act (PDCA) model.

The information security policy is part of a security manual drafted based on best security practices. Therefore, it is not a stand-alone document.

Information security roles and responsibilities have been clearly stated in every employee's job description.

Management reviews of the ISMS are conducted at planned intervals.

Rebuildy applied for certification after two midterm management reviews and one annual internal audit. Before the certification audit, one of Rebuildy's former employees approached one of the audit team members to tell them that Rebuildy has several security problems that the company is trying to conceal. The former employee presented the documented evidence to the audit team member. Electra, a key client of Rebuildy, also submitted evidence on the same issues, and the auditor determined to retain this evidence instead of the former employee's. The audit team member remained in contact with Electra until the audit was completed, discussing the nonconformities found during the audit. Electra provided additional evidence to support these findings.

At the beginning of the audit, the audit team interviewed the company's top management. They discussed, among other things, the top management's commitment to the ISMS implementation. The evidence obtained from these discussions was documented in written confirmation, which was used to determine Rebuildy's conformity to several clauses of ISO/IEC 27001.

The documented evidence obtained from Electra was attached to the audit report, along with the nonconformities report. Among others, the following nonconformities were detected:

An instance of improper user access control settings was detected within the company's financial reporting system.

A stand-alone information security policy has not been established. Instead, the company uses a security manual drafted based on best security practices.

After receiving these documents from the audit team, the team leader met Rebuildy's top management to present the audit findings. The audit team reported the findings related to the financial reporting system and the lack of a stand-alone information security policy. The top management expressed dissatisfaction with the findings and suggested that the audit team leader's conduct was unprofessional, implying they might request a replacement. Under pressure, the audit team leader decided to cooperate with top management to downplay the significance of the detected nonconformities. Consequently, the audit team leader adjusted the report to present a more favorable view, thus misrepresenting the true extent of Rebuildy's compliance issues.

Based on the scenario above, answer the following question:

Is it acceptable for the auditor to prioritize keeping the evidence provided by Electra over the evidence provided by the former employee?

A. No, because evidence from a former employee is always more reliable than that from a client

B. No, both sources of evidence should be retained and evaluated equally

C. Yes, because evidence from a client is considered more reliable due to their independent status

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

Scenario: Rebuildy is a construction company located in Bangkok, Thailand, that specializes in designing, building, and maintaining residential buildings. To ensure the security of sensitive project data and client information, Rebuildy decided to implement an ISMS based on ISO/IEC 27001. This included a comprehensive understanding of information security risks, a defined continual improvement approach, and robust business solutions.

The ISMS implementation outcomes are presented below:

Information security is achieved by applying a set of security controls and establishing policies, processes, and procedures.

Security controls are implemented based on risk assessment and aim to eliminate or reduce risks to an acceptable level.

All processes ensure the continual improvement of the ISMS based on the plan-do-check-act (PDCA) model.

The information security policy is part of a security manual drafted based on best security practices. Therefore, it is not a stand-alone document.

Information security roles and responsibilities have been clearly stated in every employee's job description.

Management reviews of the ISMS are conducted at planned intervals.

Rebuildy applied for certification after two midterm management reviews and one annual internal audit. Before the certification audit, one of Rebuildy's former employees approached one of the audit team members to tell them that Rebuildy has several security problems that the company is trying to conceal. The former employee presented the documented evidence to the audit team member. Electra, a key client of Rebuildy, also submitted evidence on the same issues, and the auditor determined to retain this evidence instead of the former employee's. The audit team member remained in contact with Electra until the audit was completed, discussing the nonconformities found during the audit. Electra provided additional evidence to support these findings.

At the beginning of the audit, the audit team interviewed the company's top management. They discussed, among other things, the top management's commitment to the ISMS implementation. The evidence obtained from these discussions was documented in written confirmation, which was used to determine Rebuildy's conformity to several clauses of ISO/IEC 27001.

The documented evidence obtained from Electra was attached to the audit report, along with the nonconformities report. Among others, the following nonconformities were detected:

An instance of improper user access control settings was detected within the company's financial reporting system.

A stand-alone information security policy has not been established. Instead, the company uses a security manual drafted based on best security practices.

After receiving these documents from the audit team, the team leader met Rebuildy's top management to present the audit findings. The audit team reported the findings related to the financial reporting system and the lack of a stand-alone information security policy. The top management expressed dissatisfaction with the findings and suggested that the audit team leader's conduct was unprofessional, implying they might request a replacement. Under pressure, the audit team leader decided to cooperate with top management to downplay the significance of the detected nonconformities. Consequently, the audit team leader adjusted the report to present a more favorable view, thus misrepresenting the true extent of Rebuildy's compliance issues.

Based on the last paragraph of scenario, what did the audit team leader commit?

A. Ordinary negligence

B. Gross negligence

C. Fraud

Suggested Answer: *C*

Community vote distribution

C (100%)

11b404b 5 months, 3 weeks ago

Selected Answer: C

The audit team leader intentionally misrepresented the audit findings to make Rebuildy appear more compliant than they actually were.

upvoted 2 times

BB4 7 months, 3 weeks ago

Selected Answer: C

Fraud as it involved intentional deception or misrepresentation

upvoted 2 times

Question #36 *Topic 1*

Scenario: Rebuildy is a construction company located in Bangkok, Thailand, that specializes in designing, building, and maintaining residential buildings. To ensure the security of sensitive project data and client information, Rebuildy decided to implement an ISMS based on ISO/IEC 27001. This included a comprehensive understanding of information security risks, a defined continual improvement approach, and robust business solutions.

The ISMS implementation outcomes are presented below:

Information security is achieved by applying a set of security controls and establishing policies, processes, and procedures.

Security controls are implemented based on risk assessment and aim to eliminate or reduce risks to an acceptable level.

All processes ensure the continual improvement of the ISMS based on the plan-do-check-act (PDCA) model.

The information security policy is part of a security manual drafted based on best security practices. Therefore, it is not a stand-alone document.

Information security roles and responsibilities have been clearly stated in every employee's job description.

Management reviews of the ISMS are conducted at planned intervals.

Rebuildy applied for certification after two midterm management reviews and one annual internal audit. Before the certification audit, one of Rebuildy's former employees approached one of the audit team members to tell them that Rebuildy has several security problems that the company is trying to conceal. The former employee presented the documented evidence to the audit team member. Electra, a key client of Rebuildy, also submitted evidence on the same issues, and the auditor determined to retain this evidence instead of the former employee's. The audit team member remained in contact with Electra until the audit was completed, discussing the nonconformities found during the audit. Electra provided additional evidence to support these findings.

At the beginning of the audit, the audit team interviewed the company's top management. They discussed, among other things, the top management's commitment to the ISMS implementation. The evidence obtained from these discussions was documented in written confirmation, which was used to determine Rebuildy's conformity to several clauses of ISO/IEC 27001.

The documented evidence obtained from Electra was attached to the audit report, along with the nonconformities report. Among others, the following nonconformities were detected:

An instance of improper user access control settings was detected within the company's financial reporting system.

A stand-alone information security policy has not been established. Instead, the company uses a security manual drafted based on best security practices.

After receiving these documents from the audit team, the team leader met Rebuildy's top management to present the audit findings. The audit team reported the findings related to the financial reporting system and the lack of a stand-alone information security policy. The top management expressed dissatisfaction with the findings and suggested that the audit team leader's conduct was unprofessional, implying they might request a replacement. Under pressure, the audit team leader decided to cooperate with top management to downplay the significance of the detected nonconformities. Consequently, the audit team leader adjusted the report to present a more favorable view, thus misrepresenting the true extent of Rebuildy's compliance issues.

Did the audit team adhere to audit best practices regarding the situation with the financial reporting system? Refer to scenario.

A. Yes, as it is beyond the scope of the audit

B. No. the audit team should have contacted the certification body and reported the situation

C. No, the audit team should have withdrawn from the audit due to the illegal nature of the act

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

Scenario: Rebuildy is a construction company located in Bangkok, Thailand, that specializes in designing, building, and maintaining residential buildings. To ensure the security of sensitive project data and client information, Rebuildy decided to implement an ISMS based on ISO/IEC 27001. This included a comprehensive understanding of information security risks, a defined continual improvement approach, and robust business solutions.

The ISMS implementation outcomes are presented below:

Information security is achieved by applying a set of security controls and establishing policies, processes, and procedures.

Security controls are implemented based on risk assessment and aim to eliminate or reduce risks to an acceptable level.

All processes ensure the continual improvement of the ISMS based on the plan-do-check-act (PDCA) model.

The information security policy is part of a security manual drafted based on best security practices. Therefore, it is not a stand-alone document.

Information security roles and responsibilities have been clearly stated in every employee's job description.

Management reviews of the ISMS are conducted at planned intervals.

Rebuildy applied for certification after two midterm management reviews and one annual internal audit. Before the certification audit, one of Rebuildy's former employees approached one of the audit team members to tell them that Rebuildy has several security problems that the company is trying to conceal. The former employee presented the documented evidence to the audit team member. Electra, a key client of Rebuildy, also submitted evidence on the same issues, and the auditor determined to retain this evidence instead of the former employee's. The audit team member remained in contact with Electra until the audit was completed, discussing the nonconformities found during the audit. Electra provided additional evidence to support these findings.

At the beginning of the audit, the audit team interviewed the company's top management. They discussed, among other things, the top management's commitment to the ISMS implementation. The evidence obtained from these discussions was documented in written confirmation, which was used to determine Rebuildy's conformity to several clauses of ISO/IEC 27001.

The documented evidence obtained from Electra was attached to the audit report, along with the nonconformities report. Among others, the following nonconformities were detected:

An instance of improper user access control settings was detected within the company's financial reporting system.

A stand-alone information security policy has not been established. Instead, the company uses a security manual drafted based on best security practices.

After receiving these documents from the audit team, the team leader met Rebuildy's top management to present the audit findings. The audit team reported the findings related to the financial reporting system and the lack of a stand-alone information security policy. The top management expressed dissatisfaction with the findings and suggested that the audit team leader's conduct was unprofessional, implying they might request a replacement. Under pressure, the audit team leader decided to cooperate with top management to downplay the significance of the detected nonconformities. Consequently, the audit team leader adjusted the report to present a more favorable view, thus misrepresenting the true extent of Rebuildy's compliance issues.

Based on scenario, the audit team used the information obtained from interviews with top management to determine Rebuildy's conformity to several ISO/IEC 27001 clauses. Is this acceptable?

A. No, the audit team should have used only documentary evidence, such as policies and procedures, to determine conformity

B. Yes, the audit team obtained verbal evidence by written confirmations from the top management, which can be used to determine conformity to the standard

C. Yes, interviews with top management are the most reliable form of audit evidence and can be used to determine conformity to the standard without further verification

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

Scenario: Rebuildy is a construction company located in Bangkok, Thailand, that specializes in designing, building, and maintaining residential buildings. To ensure the security of sensitive project data and client information, Rebuildy decided to implement an ISMS based on ISO/IEC 27001. This included a comprehensive understanding of information security risks, a defined continual improvement approach, and robust business solutions.

The ISMS implementation outcomes are presented below:

Information security is achieved by applying a set of security controls and establishing policies, processes, and procedures.

Security controls are implemented based on risk assessment and aim to eliminate or reduce risks to an acceptable level.

All processes ensure the continual improvement of the ISMS based on the plan-do-check-act (PDCA) model.

The information security policy is part of a security manual drafted based on best security practices. Therefore, it is not a stand-alone document.

Information security roles and responsibilities have been clearly stated in every employee's job description.

Management reviews of the ISMS are conducted at planned intervals.

Rebuildy applied for certification after two midterm management reviews and one annual internal audit. Before the certification audit, one of Rebuildy's former employees approached one of the audit team members to tell them that Rebuildy has several security problems that the company is trying to conceal. The former employee presented the documented evidence to the audit team member. Electra, a key client of Rebuildy, also submitted evidence on the same issues, and the auditor determined to retain this evidence instead of the former employee's. The audit team member remained in contact with Electra until the audit was completed, discussing the nonconformities found during the audit. Electra provided additional evidence to support these findings.

At the beginning of the audit, the audit team interviewed the company's top management. They discussed, among other things, the top management's commitment to the ISMS implementation. The evidence obtained from these discussions was documented in written confirmation, which was used to determine Rebuildy's conformity to several clauses of ISO/IEC 27001.

The documented evidence obtained from Electra was attached to the audit report, along with the nonconformities report. Among others, the following nonconformities were detected:

An instance of improper user access control settings was detected within the company's financial reporting system.

A stand-alone information security policy has not been established. Instead, the company uses a security manual drafted based on best security practices.

After receiving these documents from the audit team, the team leader met Rebuildy's top management to present the audit findings. The audit team reported the findings related to the financial reporting system and the lack of a stand-alone information security policy. The top management expressed dissatisfaction with the findings and suggested that the audit team leader's conduct was unprofessional, implying they might request a replacement. Under pressure, the audit team leader decided to cooperate with top management to downplay the significance of the detected nonconformities. Consequently, the audit team leader adjusted the report to present a more favorable view, thus misrepresenting the true extent of Rebuildy's compliance issues.

Which action described in scenario indicates that the audit team leader violated the independence principle?

A. The audit team leader sent a favorable report after discussing the audit conclusions with the top management

B. The audit team included the former employee's evidence in the audit report without revealing the source

C. The audit team leader revealed confidential information about Rebuildy to the former employee

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

Scenario: Branding is a marketing company that works with some of the most famous companies in the US. To reduce internal costs, Branding has outsourced the software development and IT helpdesk operations to Techvology for over two years. Techvology, equipped with the necessary expertise, manages Branding's software, network, and hardware needs. Branding has implemented an information security management system (ISMS) and is certified against ISO/IEC 27001, demonstrating its commitment to maintaining high standards of information security. It actively conducts audits on Techvology to ensure that the security of its outsourced operations complies with ISO/IEC 27001 certification requirements.
During the last audit, Branding's audit team defined the processes to be audited and the audit schedule. They adopted an evidence-based approach, particularly in light of two information security incidents reported by Techvology in the past year. The focus was on evaluating how these incidents were addressed and ensuring compliance with the terms of the outsourcing agreement.
The audit began with a comprehensive review of Techvology's methods for monitoring the quality of outsourced operations, assessing whether the services provided met Branding's expectations and agreed-upon standards. The auditors also verified whether Techvology complied with the contractual requirements established between the two entities. This involved thoroughly examining the terms and conditions in the outsourcing agreement to guarantee that all aspects, including information security measures, are being adhered to.
Furthermore, the audit included a critical evaluation of the governance processes Techvology uses to manage its outsourced operations and other organizations. This step is crucial for Branding to verify that proper controls and oversight mechanisms are in place to mitigate potential risks associated with the outsourcing arrangement.
The auditors conducted interviews with various levels of Techvology's personnel and analyzed the incident resolution records. In addition, Techvology provided the records that served as evidence that they conducted awareness sessions for the staff regarding incident management. Based on the information gathered, they predicted that both information security incidents were caused by incompetent personnel. Therefore, auditors requested to see the personnel files of the employees involved in the incidents to review evidence of their competence, such as relevant experience, certificates, and records of attended trainings.
Branding's auditors performed a critical evaluation of the validity of the evidence obtained and remained alert for evidence that could contradict or question the reliability of the documented information received. During the audit at Techvology, the auditors upheld this approach by critically assessing the incident resolution records and conducting thorough interviews with employees at different levels and functions. They did not merely take the word of Techvology's representatives for facts; instead, they sought concrete evidence to support the representatives' claims about the incident management processes.
Based on the scenario above, answer the following question:
Were the auditors diligent in adhering to the auditing process for outsourced operations?

A. Yes, they demonstrated diligence and judgment in their auditing practices

B. No, the auditors did not request a sample of employment contracts until the end of the audit

C. No, the auditors did not interview any of Techvology's top management during the audit

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

Scenario: Branding is a marketing company that works with some of the most famous companies in the US. To reduce internal costs, Branding has outsourced the software development and IT helpdesk operations to Techvology for over two years. Techvology, equipped with the necessary expertise, manages Branding's software, network, and hardware needs. Branding has implemented an information security management system (ISMS) and is certified against ISO/IEC 27001, demonstrating its commitment to maintaining high standards of information security. It actively conducts audits on Techvology to ensure that the security of its outsourced operations complies with ISO/IEC 27001 certification requirements.
During the last audit, Branding's audit team defined the processes to be audited and the audit schedule. They adopted an evidence-based approach, particularly in light of two information security incidents reported by Techvology in the past year. The focus was on evaluating how these incidents were addressed and ensuring compliance with the terms of the outsourcing agreement.
The audit began with a comprehensive review of Techvology's methods for monitoring the quality of outsourced operations, assessing whether the services provided met Branding's expectations and agreed-upon standards. The auditors also verified whether Techvology complied with the contractual requirements established between the two entities. This involved thoroughly examining the terms and conditions in the outsourcing agreement to guarantee that all aspects, including information security measures, are being adhered to.
Furthermore, the audit included a critical evaluation of the governance processes Techvology uses to manage its outsourced operations and other organizations. This step is crucial for Branding to verify that proper controls and oversight mechanisms are in place to mitigate potential risks associated with the outsourcing arrangement.
The auditors conducted interviews with various levels of Techvology's personnel and analyzed the incident resolution records. In addition, Techvology provided the records that served as evidence that they conducted awareness sessions for the staff regarding incident management. Based on the information gathered, they predicted that both information security incidents were caused by incompetent personnel. Therefore, auditors requested to see the personnel files of the employees involved in the incidents to review evidence of their competence, such as relevant experience, certificates, and records of attended trainings.
Branding's auditors performed a critical evaluation of the validity of the evidence obtained and remained alert for evidence that could contradict or question the reliability of the documented information received. During the audit at Techvology, the auditors upheld this approach by critically assessing the incident resolution records and conducting thorough interviews with employees at different levels and functions. They did not merely take the word of Techvology's representatives for facts; instead, they sought concrete evidence to support the representatives' claims about the incident management processes.
According to scenario, what type of audit evidence did the auditors collect to determine the source of the information security incidents?

A. Verbal and documentary evidence

B. Confirmative and technical evidence

C. Analytical and mathematical evidence

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

Scenario: Branding is a marketing company that works with some of the most famous companies in the US. To reduce internal costs, Branding has outsourced the software development and IT helpdesk operations to Techvology for over two years. Techvology, equipped with the necessary expertise, manages Branding's software, network, and hardware needs. Branding has implemented an information security management system (ISMS) and is certified against ISO/IEC 27001, demonstrating its commitment to maintaining high standards of information security. It actively conducts audits on Techvology to ensure that the security of its outsourced operations complies with ISO/IEC 27001 certification requirements.
During the last audit, Branding's audit team defined the processes to be audited and the audit schedule. They adopted an evidence-based approach, particularly in light of two information security incidents reported by Techvology in the past year. The focus was on evaluating how these incidents were addressed and ensuring compliance with the terms of the outsourcing agreement.
The audit began with a comprehensive review of Techvology's methods for monitoring the quality of outsourced operations, assessing whether the services provided met Branding's expectations and agreed-upon standards. The auditors also verified whether Techvology complied with the contractual requirements established between the two entities. This involved thoroughly examining the terms and conditions in the outsourcing agreement to guarantee that all aspects, including information security measures, are being adhered to.
Furthermore, the audit included a critical evaluation of the governance processes Techvology uses to manage its outsourced operations and other organizations. This step is crucial for Branding to verify that proper controls and oversight mechanisms are in place to mitigate potential risks associated with the outsourcing arrangement.
The auditors conducted interviews with various levels of Techvology's personnel and analyzed the incident resolution records. In addition, Techvology provided the records that served as evidence that they conducted awareness sessions for the staff regarding incident management. Based on the information gathered, they predicted that both information security incidents were caused by incompetent personnel. Therefore, auditors requested to see the personnel files of the employees involved in the incidents to review evidence of their competence, such as relevant experience, certificates, and records of attended trainings.
Branding's auditors performed a critical evaluation of the validity of the evidence obtained and remained alert for evidence that could contradict or question the reliability of the documented information received. During the audit at Techvology, the auditors upheld this approach by critically assessing the incident resolution records and conducting thorough interviews with employees at different levels and functions. They did not merely take the word of Techvology's representatives for facts; instead, they sought concrete evidence to support the representatives' claims about the incident management processes.
Based on scenario, what type of audit did Branding conduct?

A. First party audit

B. Second party audit

C. Third party audit

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 1*

Scenario: Branding is a marketing company that works with some of the most famous companies in the US. To reduce internal costs, Branding has outsourced the software development and IT helpdesk operations to Techvology for over two years. Techvology, equipped with the necessary expertise, manages Branding's software, network, and hardware needs. Branding has implemented an information security management system (ISMS) and is certified against ISO/IEC 27001, demonstrating its commitment to maintaining high standards of information security. It actively conducts audits on Techvology to ensure that the security of its outsourced operations complies with ISO/IEC 27001 certification requirements.
During the last audit, Branding's audit team defined the processes to be audited and the audit schedule. They adopted an evidence-based approach, particularly in light of two information security incidents reported by Techvology in the past year. The focus was on evaluating how these incidents were addressed and ensuring compliance with the terms of the outsourcing agreement.
The audit began with a comprehensive review of Techvology's methods for monitoring the quality of outsourced operations, assessing whether the services provided met Branding's expectations and agreed-upon standards. The auditors also verified whether Techvology complied with the contractual requirements established between the two entities. This involved thoroughly examining the terms and conditions in the outsourcing agreement to guarantee that all aspects, including information security measures, are being adhered to.
Furthermore, the audit included a critical evaluation of the governance processes Techvology uses to manage its outsourced operations and other organizations. This step is crucial for Branding to verify that proper controls and oversight mechanisms are in place to mitigate potential risks associated with the outsourcing arrangement.
The auditors conducted interviews with various levels of Techvology's personnel and analyzed the incident resolution records. In addition, Techvology provided the records that served as evidence that they conducted awareness sessions for the staff regarding incident management. Based on the information gathered, they predicted that both information security incidents were caused by incompetent personnel. Therefore, auditors requested to see the personnel files of the employees involved in the incidents to review evidence of their competence, such as relevant experience, certificates, and records of attended trainings.
Branding's auditors performed a critical evaluation of the validity of the evidence obtained and remained alert for evidence that could contradict or question the reliability of the documented information received. During the audit at Techvology, the auditors upheld this approach by critically assessing the incident resolution records and conducting thorough interviews with employees at different levels and functions. They did not merely take the word of Techvology's representatives for facts; instead, they sought concrete evidence to support the representatives' claims about the incident management processes.
Which auditing principle is explained in the last paragraph of scenario?

A. Risk-based approach

B. Fair presentation

C. Professional skepticism

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #43 *Topic 1*

Scenario: Branding is a marketing company that works with some of the most famous companies in the US. To reduce internal costs, Branding has outsourced the software development and IT helpdesk operations to Techvology for over two years. Techvology, equipped with the necessary expertise, manages Branding's software, network, and hardware needs. Branding has implemented an information security management system (ISMS) and is certified against ISO/IEC 27001, demonstrating its commitment to maintaining high standards of information security. It actively conducts audits on Techvology to ensure that the security of its outsourced operations complies with ISO/IEC 27001 certification requirements.
During the last audit, Branding's audit team defined the processes to be audited and the audit schedule. They adopted an evidence-based approach, particularly in light of two information security incidents reported by Techvology in the past year. The focus was on evaluating how these incidents were addressed and ensuring compliance with the terms of the outsourcing agreement.
The audit began with a comprehensive review of Techvology's methods for monitoring the quality of outsourced operations, assessing whether the services provided met Branding's expectations and agreed-upon standards. The auditors also verified whether Techvology complied with the contractual requirements established between the two entities. This involved thoroughly examining the terms and conditions in the outsourcing agreement to guarantee that all aspects, including information security measures, are being adhered to.
Furthermore, the audit included a critical evaluation of the governance processes Techvology uses to manage its outsourced operations and other organizations. This step is crucial for Branding to verify that proper controls and oversight mechanisms are in place to mitigate potential risks associated with the outsourcing arrangement.
The auditors conducted interviews with various levels of Techvology's personnel and analyzed the incident resolution records. In addition, Techvology provided the records that served as evidence that they conducted awareness sessions for the staff regarding incident management. Based on the information gathered, they predicted that both information security incidents were caused by incompetent personnel. Therefore, auditors requested to see the personnel files of the employees involved in the incidents to review evidence of their competence, such as relevant experience, certificates, and records of attended trainings.
Branding's auditors performed a critical evaluation of the validity of the evidence obtained and remained alert for evidence that could contradict or question the reliability of the documented information received. During the audit at Techvology, the auditors upheld this approach by critically assessing the incident resolution records and conducting thorough interviews with employees at different levels and functions. They did not merely take the word of Techvology's representatives for facts; instead, they sought concrete evidence to support the representatives' claims about the incident management processes.
According to ISO/IEC 27001 requirements, is Branding required to control the services offered by Techvology continually? Refer to scenario.

A. Yes, Branding is responsible for controlling and monitoring the quality of Techvology's services

B. Yes, only if this is a requirement specified in the contractual agreement between the two companies

C. No, Branding is not responsible for controlling the services offered by Techvology, but is responsible for monitoring them

Suggested Answer: *C*

Community vote distribution

ROCTW 5 months ago

Selected Answer: A

A.5.19 ~ A.5.22

upvoted 2 times

Question #44 *Topic 1*

Prior to initiating the audit activities, the auditors considered the auditee's context, critical processes, and expectations. Which auditing principle has been applied?

A. Due professional care

B. Professional skepticism

C. Integrity

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

What is the main difference between qualitative and quantitative evidence?

A. Qualitative evidence originates from the analysis of a sample related to determining the audit criteria, while quantitative evidence originates from the analysis of unquantifiable information

B. Qualitative evidence focuses on evaluating if a process or control complies with the audit criteria, while quantitative evidence aims to determine if a process in operation is functional and effective

C. Qualitative evidence is used to make estimations about the whole population, while quantitative evidence focuses on evaluating if a process complies with standard requirements

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

Finnco, a subsidiary of a certification body, provided ISMS consultancy services to an organization. Considering this scenario, when can the certification body certify the organization?

A. There is no time constraint in such a situation

B. The certification body can certify the organization immediately after consulting services end

C. If a minimum period of two years has passed since the last consulting activities

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #47 *Topic 1*

How does predictive analytics help auditors in identifying potential risks?

A. By providing real-lime analysis of financial data

B. By predicting future outcomes based on trends

C. By organizing data from various sources

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

Scenario: Cyber ACrypt is a cybersecurity company that provides endpoint protection by offering anti-malware and device security, asset life cycle management, and device encryption. To validate its ISMS against ISO/IEC 27001 and demonstrate its commitment to cybersecurity excellence, the company underwent a meticulous audit process led by John, the appointed audit team leader.

Upon accepting the audit mandate, John promptly organized a meeting to outline the audit plan and team roles. This phase was crucial for aligning the team with the audit's objectives and scope. However, the initial presentation to Cyber ACrypt's staff revealed a significant gap in understanding the audit's scope and objectives, indicating potential readiness challenges within the company.

As the stage 1 audit commenced, the team prepared for on-site activities. They reviewed Cyber ACrypt's documented information, including the information security policy and operational procedures ensuring each piece conformed to and was standardized in format with author identification, production date, version number, and approval date. Additionally, the audit team ensured that each document contained the information required by the respective clause of the standard. This phase revealed that a detailed audit of the documentation describing task execution was unnecessary, streamlining the process and focusing the team's efforts on critical areas. During the phase of conducting on-site activities, the team evaluated management responsibility for the Cyber ACrypt's policies. This thorough examination aimed to ascertain continual improvement and adherence to ISMS requirements. Subsequently, in the document, the stage 1 audit outputs phase, the audit team meticulously documented their findings, underscoring their conclusions regarding the fulfillment of the stage 1 objectives. This documentation was vital for the audit team and Cyber ACrypt to understand the preliminary audit outcomes and areas requiring attention.

The audit team also decided to conduct interviews with key interested parties. This decision was motivated by the objective of collecting robust audit evidence to validate the management system's compliance with ISO/IEC 27001 requirements. Engaging with interested parties across various levels of Cyber ACrypt provided the audit team with invaluable perspectives and an understanding of the ISMS's implementation and effectiveness.

The stage 1 audit report unveiled critical areas of concern. The Statement of Applicability (SoA) and the ISMS policy were found to be lacking in several respects, including insufficient risk assessment, inadequate access controls, and lack of regular policy reviews. This prompted Cyber ACrypt to take immediate action to address these shortcomings. Their prompt response and modifications to the strategic documents reflected a strong commitment to achieving compliance.

The technical expertise introduced to bridge the audit team's cybersecurity knowledge gap played a pivotal role in identifying shortcomings in the risk assessment methodology and reviewing network architecture. This included evaluating firewalls, intrusion detection and prevention systems, and other network security measures, as well as assessing how Cyber ACrypt detects, responds to, and recovers from external and internal threats. Under John's supervision, the technical expert communicated the audit findings to the representatives of Cyber ACrypt. However, the audit team observed that the expert's objectivity might have been compromised due to receiving consultancy fees from the auditee. Considering the behavior of the technical expert during the audit, the audit team leader decided to discuss this concern with the certification body.

Based on the scenario above, answer the following question:

Which activity was NOT conducted correctly by the audit team during stage 1 audit?

A. Preparing for on-site activities by including the information security policy and operational procedures for review

B. Conducting on-site activities by evaluating management responsibility for the Cyber ACrypt's policies

C. Documenting the stage 1 audit outputs by failing to include the relevant evidence or supporting documentation

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

Scenario: Cyber ACrypt is a cybersecurity company that provides endpoint protection by offering anti-malware and device security, asset life cycle management, and device encryption. To validate its ISMS against ISO/IEC 27001 and demonstrate its commitment to cybersecurity excellence, the company underwent a meticulous audit process led by John, the appointed audit team leader.

Upon accepting the audit mandate, John promptly organized a meeting to outline the audit plan and team roles. This phase was crucial for aligning the team with the audit's objectives and scope. However, the initial presentation to Cyber ACrypt's staff revealed a significant gap in understanding the audit's scope and objectives, indicating potential readiness challenges within the company.

As the stage 1 audit commenced, the team prepared for on-site activities. They reviewed Cyber ACrypt's documented information, including the information security policy and operational procedures ensuring each piece conformed to and was standardized in format with author identification, production date, version number, and approval date. Additionally, the audit team ensured that each document contained the information required by the respective clause of the standard. This phase revealed that a detailed audit of the documentation describing task execution was unnecessary, streamlining the process and focusing the team's efforts on critical areas. During the phase of conducting on-site activities, the team evaluated management responsibility for the Cyber ACrypt's policies. This thorough examination aimed to ascertain continual improvement and adherence to ISMS requirements. Subsequently, in the document, the stage 1 audit outputs phase, the audit team meticulously documented their findings, underscoring their conclusions regarding the fulfillment of the stage 1 objectives. This documentation was vital for the audit team and Cyber ACrypt to understand the preliminary audit outcomes and areas requiring attention.

The audit team also decided to conduct interviews with key interested parties. This decision was motivated by the objective of collecting robust audit evidence to validate the management system's compliance with ISO/IEC 27001 requirements. Engaging with interested parties across various levels of Cyber ACrypt provided the audit team with invaluable perspectives and an understanding of the ISMS's implementation and effectiveness.

The stage 1 audit report unveiled critical areas of concern. The Statement of Applicability (SoA) and the ISMS policy were found to be lacking in several respects, including insufficient risk assessment, inadequate access controls, and lack of regular policy reviews. This prompted Cyber ACrypt to take immediate action to address these shortcomings. Their prompt response and modifications to the strategic documents reflected a strong commitment to achieving compliance.

The technical expertise introduced to bridge the audit team's cybersecurity knowledge gap played a pivotal role in identifying shortcomings in the risk assessment methodology and reviewing network architecture. This included evaluating firewalls, intrusion detection and prevention systems, and other network security measures, as well as assessing how Cyber ACrypt detects, responds to, and recovers from external and internal threats. Under John's supervision, the technical expert communicated the audit findings to the representatives of Cyber ACrypt. However, the audit team observed that the expert's objectivity might have been compromised due to receiving consultancy fees from the auditee. Considering the behavior of the technical expert during the audit, the audit team leader decided to discuss this concern with the certification body.

According to scenario, Cyber ACrypt modified the SoA and the ISMS policy after the stage 1 audit report. How do you define this situation?

A. Unacceptable, once the external audit passes stage 1, the SoA and the ISMS policy cannot be modified

B. Acceptable, situations that lead to major nonconformities during the stage 2 audit should be corrected

C. Acceptable, minor modifications to the SoA and ISMS policy can be made until the submission of the final audit report

Suggested Answer: *C*

Community vote distribution

ROCTW 5 months ago

Selected Answer: B

The primary purpose of a Stage 1 audit is to assess an organization's readiness for the full certification audit (Stage 2). This includes evaluating the maturity of its Information Security Management System (ISMS) documentation, its understanding of the ISO/IEC 27001 standard's requirements, and identifying any significant gaps or deficiencies that could impede the Stage 2 audit.

The scenario clearly states: "The stage 1 audit report unveiled critical areas of concern. The Statement of Applicability (SoA) and the ISMS policy were found to be lacking in several respects, including insufficient risk assessment, inadequate access controls, and lack of regular policy reviews." These were identified as critical deficiencies that, if left unaddressed, would likely result in major nonconformities during the Stage 2 audit.

upvoted 1 times

Question #50 *Topic 1*

Scenario: Cyber ACrypt is a cybersecurity company that provides endpoint protection by offering anti-malware and device security, asset life cycle management, and device encryption. To validate its ISMS against ISO/IEC 27001 and demonstrate its commitment to cybersecurity excellence, the company underwent a meticulous audit process led by John, the appointed audit team leader.

Upon accepting the audit mandate, John promptly organized a meeting to outline the audit plan and team roles. This phase was crucial for aligning the team with the audit's objectives and scope. However, the initial presentation to Cyber ACrypt's staff revealed a significant gap in understanding the audit's scope and objectives, indicating potential readiness challenges within the company.

As the stage 1 audit commenced, the team prepared for on-site activities. They reviewed Cyber ACrypt's documented information, including the information security policy and operational procedures ensuring each piece conformed to and was standardized in format with author identification, production date, version number, and approval date. Additionally, the audit team ensured that each document contained the information required by the respective clause of the standard. This phase revealed that a detailed audit of the documentation describing task execution was unnecessary, streamlining the process and focusing the team's efforts on critical areas. During the phase of conducting on-site activities, the team evaluated management responsibility for the Cyber ACrypt's policies. This thorough examination aimed to ascertain continual improvement and adherence to ISMS requirements. Subsequently, in the document, the stage 1 audit outputs phase, the audit team meticulously documented their findings, underscoring their conclusions regarding the fulfillment of the stage 1 objectives. This documentation was vital for the audit team and Cyber ACrypt to understand the preliminary audit outcomes and areas requiring attention.

The audit team also decided to conduct interviews with key interested parties. This decision was motivated by the objective of collecting robust audit evidence to validate the management system's compliance with ISO/IEC 27001 requirements. Engaging with interested parties across various levels of Cyber ACrypt provided the audit team with invaluable perspectives and an understanding of the ISMS's implementation and effectiveness.

The stage 1 audit report unveiled critical areas of concern. The Statement of Applicability (SoA) and the ISMS policy were found to be lacking in several respects, including insufficient risk assessment, inadequate access controls, and lack of regular policy reviews. This prompted Cyber ACrypt to take immediate action to address these shortcomings. Their prompt response and modifications to the strategic documents reflected a strong commitment to achieving compliance.

The technical expertise introduced to bridge the audit team's cybersecurity knowledge gap played a pivotal role in identifying shortcomings in the risk assessment methodology and reviewing network architecture. This included evaluating firewalls, intrusion detection and prevention systems, and other network security measures, as well as assessing how Cyber ACrypt detects, responds to, and recovers from external and internal threats. Under John's supervision, the technical expert communicated the audit findings to the representatives of Cyber ACrypt. However, the audit team observed that the expert's objectivity might have been compromised due to receiving consultancy fees from the auditee. Considering the behavior of the technical expert during the audit, the audit team leader decided to discuss this concern with the certification body.

Based on scenario, is the audit team leader's decision regarding the technical expert's behavior acceptable?

A. No, the audit team leader should have reported the issue directly to the top management instead

B. No, questioning the expert's objectivity is not a valid reason for the audit team leader to discuss the matter with the certification body

C. Yes, if the auditor is skeptical about the technical expert's objectivity, he must discuss his concerns with the certification body

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #51 *Topic 1*

Scenario: Cyber ACrypt is a cybersecurity company that provides endpoint protection by offering anti-malware and device security, asset life cycle management, and device encryption. To validate its ISMS against ISO/IEC 27001 and demonstrate its commitment to cybersecurity excellence, the company underwent a meticulous audit process led by John, the appointed audit team leader.

Upon accepting the audit mandate, John promptly organized a meeting to outline the audit plan and team roles. This phase was crucial for aligning the team with the audit's objectives and scope. However, the initial presentation to Cyber ACrypt's staff revealed a significant gap in understanding the audit's scope and objectives, indicating potential readiness challenges within the company.

As the stage 1 audit commenced, the team prepared for on-site activities. They reviewed Cyber ACrypt's documented information, including the information security policy and operational procedures ensuring each piece conformed to and was standardized in format with author identification, production date, version number, and approval date. Additionally, the audit team ensured that each document contained the information required by the respective clause of the standard. This phase revealed that a detailed audit of the documentation describing task execution was unnecessary, streamlining the process and focusing the team's efforts on critical areas. During the phase of conducting on-site activities, the team evaluated management responsibility for the Cyber ACrypt's policies. This thorough examination aimed to ascertain continual improvement and adherence to ISMS requirements. Subsequently, in the document, the stage 1 audit outputs phase, the audit team meticulously documented their findings, underscoring their conclusions regarding the fulfillment of the stage 1 objectives. This documentation was vital for the audit team and Cyber ACrypt to understand the preliminary audit outcomes and areas requiring attention.

The audit team also decided to conduct interviews with key interested parties. This decision was motivated by the objective of collecting robust audit evidence to validate the management system's compliance with ISO/IEC 27001 requirements. Engaging with interested parties across various levels of Cyber ACrypt provided the audit team with invaluable perspectives and an understanding of the ISMS's implementation and effectiveness.

The stage 1 audit report unveiled critical areas of concern. The Statement of Applicability (SoA) and the ISMS policy were found to be lacking in several respects, including insufficient risk assessment, inadequate access controls, and lack of regular policy reviews. This prompted Cyber ACrypt to take immediate action to address these shortcomings. Their prompt response and modifications to the strategic documents reflected a strong commitment to achieving compliance.

The technical expertise introduced to bridge the audit team's cybersecurity knowledge gap played a pivotal role in identifying shortcomings in the risk assessment methodology and reviewing network architecture. This included evaluating firewalls, intrusion detection and prevention systems, and other network security measures, as well as assessing how Cyber ACrypt detects, responds to, and recovers from external and internal threats. Under John's supervision, the technical expert communicated the audit findings to the representatives of Cyber ACrypt. However, the audit team observed that the expert's objectivity might have been compromised due to receiving consultancy fees from the auditee. Considering the behavior of the technical expert during the audit, the audit team leader decided to discuss this concern with the certification body.

Based on scenario, was the objective of the interviews during the stage 1 audit accordingly set by the audit team?

A. Yes, the objective of the interviews is to collect oud1t evidence to validate the management systems compliance with ISO/IEC 27001 requirements

B. No, the objective of the interviews was not aligned with the management system's key performance indicators (KPIs), reducing the audit's effectiveness

C. No, the objective of the interviews is to ensure an adequate understanding of the challenges the auditee faces

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #52 *Topic 1*

Scenario: Cyber ACrypt is a cybersecurity company that provides endpoint protection by offering anti-malware and device security, asset life cycle management, and device encryption. To validate its ISMS against ISO/IEC 27001 and demonstrate its commitment to cybersecurity excellence, the company underwent a meticulous audit process led by John, the appointed audit team leader.

Upon accepting the audit mandate, John promptly organized a meeting to outline the audit plan and team roles. This phase was crucial for aligning the team with the audit's objectives and scope. However, the initial presentation to Cyber ACrypt's staff revealed a significant gap in understanding the audit's scope and objectives, indicating potential readiness challenges within the company.

As the stage 1 audit commenced, the team prepared for on-site activities. They reviewed Cyber ACrypt's documented information, including the information security policy and operational procedures ensuring each piece conformed to and was standardized in format with author identification, production date, version number, and approval date. Additionally, the audit team ensured that each document contained the information required by the respective clause of the standard. This phase revealed that a detailed audit of the documentation describing task execution was unnecessary, streamlining the process and focusing the team's efforts on critical areas. During the phase of conducting on-site activities, the team evaluated management responsibility for the Cyber ACrypt's policies. This thorough examination aimed to ascertain continual improvement and adherence to ISMS requirements. Subsequently, in the document, the stage 1 audit outputs phase, the audit team meticulously documented their findings, underscoring their conclusions regarding the fulfillment of the stage 1 objectives. This documentation was vital for the audit team and Cyber ACrypt to understand the preliminary audit outcomes and areas requiring attention.

The audit team also decided to conduct interviews with key interested parties. This decision was motivated by the objective of collecting robust audit evidence to validate the management system's compliance with ISO/IEC 27001 requirements. Engaging with interested parties across various levels of Cyber ACrypt provided the audit team with invaluable perspectives and an understanding of the ISMS's implementation and effectiveness.

The stage 1 audit report unveiled critical areas of concern. The Statement of Applicability (SoA) and the ISMS policy were found to be lacking in several respects, including insufficient risk assessment, inadequate access controls, and lack of regular policy reviews. This prompted Cyber ACrypt to take immediate action to address these shortcomings. Their prompt response and modifications to the strategic documents reflected a strong commitment to achieving compliance.

The technical expertise introduced to bridge the audit team's cybersecurity knowledge gap played a pivotal role in identifying shortcomings in the risk assessment methodology and reviewing network architecture. This included evaluating firewalls, intrusion detection and prevention systems, and other network security measures, as well as assessing how Cyber ACrypt detects, responds to, and recovers from external and internal threats. Under John's supervision, the technical expert communicated the audit findings to the representatives of Cyber ACrypt. However, the audit team observed that the expert's objectivity might have been compromised due to receiving consultancy fees from the auditee. Considering the behavior of the technical expert during the audit, the audit team leader decided to discuss this concern with the certification body.

Which of the following criteria for evaluating documented information was NOT validated by the audit team? Refer to scenario.

A. Content of the documented information

B. Format of the documented information

C. Procedure for managing the documented information

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #53 *Topic 1*

Scenario: Webvue, headquartered in Japan, is a technology company specializing in the development, support, and maintenance of computer software Webvue provides solutions across various technology fields and business sectors. Its flagship service is CloudWebvue, a comprehensive cloud computing platform offering storage, networking, and virtual computing services. Designed for both businesses and individual users, CloudWebvue is known for its flexibility, scalability, and reliability.

Webvue has decided to only include CloudWebvue in its ISO/IEC 27001 certification scope. Thus, the stage 1 and 2 audits were performed simultaneously. Webvue takes pride in its strictness regarding asset confidentiality. They protect the information stored in CloudWebvue by using appropriate cryptographic controls. Every piece of information of any classification level, whether for internal use, restricted, or confidential, is first encrypted with a unique corresponding hash and then stored in the cloud.

The audit team comprised five persons Keith, Sean, Layla, Sam, and Tina. Keith, the most experienced auditor on the IT and information security auditing team, was the audit team leader. His responsibilities included planning the audit and managing the audit team. Sean and Layla were experienced in project planning, business analysis, and IT systems (hardware and application). Their tasks included audit planning according to Webvue's internal systems and processes. Sam and Tina, on the other hand, who had recently completed their education, were responsible for completing the day-to-day tasks while developing their audit skills.

While verifying conformity to control 8.24 Use of cryptography of ISO/IEC 27001 Annex A through interviews with the relevant staff, the audit team found out that the cryptographic keys have been initially generated based on random bit generator (RBG) and other best practices for the generation of the cryptographic keys. After checking Webvue's cryptography policy, they concluded that the information obtained by the interviews was true. However, the cryptographic keys are still in use because the policy does not address the use and lifetime of cryptographic keys.

As later agreed upon between Webvue and the certification body, the audit team opted to conduct a virtual audit specifically focused on verifying conformity to control 8.11 Data Masking of ISO/IEC 27001 within Webvue, aligning with the certification scope and audit objectives. They examined the processes involved in protecting data within CloudWebvue, focusing on how the company adhered to its policies and regulatory standards. As part of this process, Keith, the audit team leader, took screenshot copies of relevant documents and cryptographic key management procedures to document and analyze the effectiveness of Webvue's practices.

Webvue uses generated test data for testing purposes. However, as determined by both the interview with the manager of the QA Department and the procedures used by this department, sometimes live system data are used. In such scenarios, large amounts of data are generated while producing more accurate results. The test data is protected and controlled, as verified by the simulation of the encryption process performed by Webvue's personnel during the audit.

While interviewing the manager of the QA Department, Keith observed that employees in the Security Training Department were not following proper procedures, even though this department fell outside the audit scope. Despite the exclusion in the audit scope, the nonconformity in the Security Training Department has potential implications for the processes within the audit scope, specifically impacting data security and cryptographic practices in CloudWebvue. Therefore, Keith incorporated this finding into the audit report and accordingly informed the auditee.

Based on the scenario above, answer the following question:

To verify conformity to the protection of test data control, Webvue's personnel simulated the encryption process. Is this acceptable?

A. No, the encryption process must not be simulated since it affects the auditee's operations

B. Yes, if the auditor is not competent to perform the operations linked to a test, a representative of the auditee may have the role of a technical expert

C. Yes, simulation of a process to verify conformity to a control can be done with the assistance of the auditee's personnel

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #54 *Topic 1*

Scenario: Webvue, headquartered in Japan, is a technology company specializing in the development, support, and maintenance of computer software Webvue provides solutions across various technology fields and business sectors. Its flagship service is CloudWebvue, a comprehensive cloud computing platform offering storage, networking, and virtual computing services. Designed for both businesses and individual users, CloudWebvue is known for its flexibility, scalability, and reliability.

Webvue has decided to only include CloudWebvue in its ISO/IEC 27001 certification scope. Thus, the stage 1 and 2 audits were performed simultaneously. Webvue takes pride in its strictness regarding asset confidentiality. They protect the information stored in CloudWebvue by using appropriate cryptographic controls. Every piece of information of any classification level, whether for internal use, restricted, or confidential, is first encrypted with a unique corresponding hash and then stored in the cloud.

The audit team comprised five persons Keith, Sean, Layla, Sam, and Tina. Keith, the most experienced auditor on the IT and information security auditing team, was the audit team leader. His responsibilities included planning the audit and managing the audit team. Sean and Layla were experienced in project planning, business analysis, and IT systems (hardware and application). Their tasks included audit planning according to Webvue's internal systems and processes. Sam and Tina, on the other hand, who had recently completed their education, were responsible for completing the day-to-day tasks while developing their audit skills.

While verifying conformity to control 8.24 Use of cryptography of ISO/IEC 27001 Annex A through interviews with the relevant staff, the audit team found out that the cryptographic keys have been initially generated based on random bit generator (RBG) and other best practices for the generation of the cryptographic keys. After checking Webvue's cryptography policy, they concluded that the information obtained by the interviews was true. However, the cryptographic keys are still in use because the policy does not address the use and lifetime of cryptographic keys.

As later agreed upon between Webvue and the certification body, the audit team opted to conduct a virtual audit specifically focused on verifying conformity to control 8.11 Data Masking of ISO/IEC 27001 within Webvue, aligning with the certification scope and audit objectives. They examined the processes involved in protecting data within CloudWebvue, focusing on how the company adhered to its policies and regulatory standards. As part of this process, Keith, the audit team leader, took screenshot copies of relevant documents and cryptographic key management procedures to document and analyze the effectiveness of Webvue's practices.

Webvue uses generated test data for testing purposes. However, as determined by both the interview with the manager of the QA Department and the procedures used by this department, sometimes live system data are used. In such scenarios, large amounts of data are generated while producing more accurate results. The test data is protected and controlled, as verified by the simulation of the encryption process performed by Webvue's personnel during the audit.

While interviewing the manager of the QA Department, Keith observed that employees in the Security Training Department were not following proper procedures, even though this department fell outside the audit scope. Despite the exclusion in the audit scope, the nonconformity in the Security Training Department has potential implications for the processes within the audit scope, specifically impacting data security and cryptographic practices in CloudWebvue. Therefore, Keith incorporated this finding into the audit report and accordingly informed the auditee.

Based on scenario, the audit team checked Webvue's cryptography policy to obtain reasonable assurance of the information obtained during the interviews. Which type of audit procedure has been used?

A. Observation

B. Corroboration

C. Evaluation

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #55 *Topic 1*

Scenario: Webvue, headquartered in Japan, is a technology company specializing in the development, support, and maintenance of computer software Webvue provides solutions across various technology fields and business sectors. Its flagship service is CloudWebvue, a comprehensive cloud computing platform offering storage, networking, and virtual computing services. Designed for both businesses and individual users, CloudWebvue is known for its flexibility, scalability, and reliability.

Webvue has decided to only include CloudWebvue in its ISO/IEC 27001 certification scope. Thus, the stage 1 and 2 audits were performed simultaneously. Webvue takes pride in its strictness regarding asset confidentiality. They protect the information stored in CloudWebvue by using appropriate cryptographic controls. Every piece of information of any classification level, whether for internal use, restricted, or confidential, is first encrypted with a unique corresponding hash and then stored in the cloud.

The audit team comprised five persons Keith, Sean, Layla, Sam, and Tina. Keith, the most experienced auditor on the IT and information security auditing team, was the audit team leader. His responsibilities included planning the audit and managing the audit team. Sean and Layla were experienced in project planning, business analysis, and IT systems (hardware and application). Their tasks included audit planning according to Webvue's internal systems and processes. Sam and Tina, on the other hand, who had recently completed their education, were responsible for completing the day-to-day tasks while developing their audit skills.

While verifying conformity to control 8.24 Use of cryptography of ISO/IEC 27001 Annex A through interviews with the relevant staff, the audit team found out that the cryptographic keys have been initially generated based on random bit generator (RBG) and other best practices for the generation of the cryptographic keys. After checking Webvue's cryptography policy, they concluded that the information obtained by the interviews was true. However, the cryptographic keys are still in use because the policy does not address the use and lifetime of cryptographic keys.

As later agreed upon between Webvue and the certification body, the audit team opted to conduct a virtual audit specifically focused on verifying conformity to control 8.11 Data Masking of ISO/IEC 27001 within Webvue, aligning with the certification scope and audit objectives. They examined the processes involved in protecting data within CloudWebvue, focusing on how the company adhered to its policies and regulatory standards. As part of this process, Keith, the audit team leader, took screenshot copies of relevant documents and cryptographic key management procedures to document and analyze the effectiveness of Webvue's practices.

Webvue uses generated test data for testing purposes. However, as determined by both the interview with the manager of the QA Department and the procedures used by this department, sometimes live system data are used. In such scenarios, large amounts of data are generated while producing more accurate results. The test data is protected and controlled, as verified by the simulation of the encryption process performed by Webvue's personnel during the audit.

While interviewing the manager of the QA Department, Keith observed that employees in the Security Training Department were not following proper procedures, even though this department fell outside the audit scope. Despite the exclusion in the audit scope, the nonconformity in the Security Training Department has potential implications for the processes within the audit scope, specifically impacting data security and cryptographic practices in CloudWebvue. Therefore, Keith incorporated this finding into the audit report and accordingly informed the auditee.

Based on scenario, which audit procedure was used to verify conformity to the use of test data?

A. Documented information review

B. Corroboration

C. Technical verification

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #56 *Topic 1*

Scenario: Webvue, headquartered in Japan, is a technology company specializing in the development, support, and maintenance of computer software Webvue provides solutions across various technology fields and business sectors. Its flagship service is CloudWebvue, a comprehensive cloud computing platform offering storage, networking, and virtual computing services. Designed for both businesses and individual users, CloudWebvue is known for its flexibility, scalability, and reliability.

Webvue has decided to only include CloudWebvue in its ISO/IEC 27001 certification scope. Thus, the stage 1 and 2 audits were performed simultaneously. Webvue takes pride in its strictness regarding asset confidentiality. They protect the information stored in CloudWebvue by using appropriate cryptographic controls. Every piece of information of any classification level, whether for internal use, restricted, or confidential, is first encrypted with a unique corresponding hash and then stored in the cloud.

The audit team comprised five persons Keith, Sean, Layla, Sam, and Tina. Keith, the most experienced auditor on the IT and information security auditing team, was the audit team leader. His responsibilities included planning the audit and managing the audit team. Sean and Layla were experienced in project planning, business analysis, and IT systems (hardware and application). Their tasks included audit planning according to Webvue's internal systems and processes. Sam and Tina, on the other hand, who had recently completed their education, were responsible for completing the day-to-day tasks while developing their audit skills.

While verifying conformity to control 8.24 Use of cryptography of ISO/IEC 27001 Annex A through interviews with the relevant staff, the audit team found out that the cryptographic keys have been initially generated based on random bit generator (RBG) and other best practices for the generation of the cryptographic keys. After checking Webvue's cryptography policy, they concluded that the information obtained by the interviews was true. However, the cryptographic keys are still in use because the policy does not address the use and lifetime of cryptographic keys.

As later agreed upon between Webvue and the certification body, the audit team opted to conduct a virtual audit specifically focused on verifying conformity to control 8.11 Data Masking of ISO/IEC 27001 within Webvue, aligning with the certification scope and audit objectives. They examined the processes involved in protecting data within CloudWebvue, focusing on how the company adhered to its policies and regulatory standards. As part of this process, Keith, the audit team leader, took screenshot copies of relevant documents and cryptographic key management procedures to document and analyze the effectiveness of Webvue's practices.

Webvue uses generated test data for testing purposes. However, as determined by both the interview with the manager of the QA Department and the procedures used by this department, sometimes live system data are used. In such scenarios, large amounts of data are generated while producing more accurate results. The test data is protected and controlled, as verified by the simulation of the encryption process performed by Webvue's personnel during the audit.

While interviewing the manager of the QA Department, Keith observed that employees in the Security Training Department were not following proper procedures, even though this department fell outside the audit scope. Despite the exclusion in the audit scope, the nonconformity in the Security Training Department has potential implications for the processes within the audit scope, specifically impacting data security and cryptographic practices in CloudWebvue. Therefore, Keith incorporated this finding into the audit report and accordingly informed the auditee.

Did Keith make the appropriate decision regarding Webvue's documents during the virtual audit? Refer to scenario.

A. Yes, taking screenshots of document copies is allowed without prior permission, provided the audit is not being recorded

B. No, because he should have obtained permission before taking screenshot copies of documents

C. No, as screenshot copies are not permitted at all during virtual audits

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #57 *Topic 1*

Scenario: Webvue, headquartered in Japan, is a technology company specializing in the development, support, and maintenance of computer software Webvue provides solutions across various technology fields and business sectors. Its flagship service is CloudWebvue, a comprehensive cloud computing platform offering storage, networking, and virtual computing services. Designed for both businesses and individual users, CloudWebvue is known for its flexibility, scalability, and reliability.

Webvue has decided to only include CloudWebvue in its ISO/IEC 27001 certification scope. Thus, the stage 1 and 2 audits were performed simultaneously. Webvue takes pride in its strictness regarding asset confidentiality. They protect the information stored in CloudWebvue by using appropriate cryptographic controls. Every piece of information of any classification level, whether for internal use, restricted, or confidential, is first encrypted with a unique corresponding hash and then stored in the cloud.

The audit team comprised five persons Keith, Sean, Layla, Sam, and Tina. Keith, the most experienced auditor on the IT and information security auditing team, was the audit team leader. His responsibilities included planning the audit and managing the audit team. Sean and Layla were experienced in project planning, business analysis, and IT systems (hardware and application). Their tasks included audit planning according to Webvue's internal systems and processes. Sam and Tina, on the other hand, who had recently completed their education, were responsible for completing the day-to-day tasks while developing their audit skills.

While verifying conformity to control 8.24 Use of cryptography of ISO/IEC 27001 Annex A through interviews with the relevant staff, the audit team found out that the cryptographic keys have been initially generated based on random bit generator (RBG) and other best practices for the generation of the cryptographic keys. After checking Webvue's cryptography policy, they concluded that the information obtained by the interviews was true. However, the cryptographic keys are still in use because the policy does not address the use and lifetime of cryptographic keys.

As later agreed upon between Webvue and the certification body, the audit team opted to conduct a virtual audit specifically focused on verifying conformity to control 8.11 Data Masking of ISO/IEC 27001 within Webvue, aligning with the certification scope and audit objectives. They examined the processes involved in protecting data within CloudWebvue, focusing on how the company adhered to its policies and regulatory standards. As part of this process, Keith, the audit team leader, took screenshot copies of relevant documents and cryptographic key management procedures to document and analyze the effectiveness of Webvue's practices.

Webvue uses generated test data for testing purposes. However, as determined by both the interview with the manager of the QA Department and the procedures used by this department, sometimes live system data are used. In such scenarios, large amounts of data are generated while producing more accurate results. The test data is protected and controlled, as verified by the simulation of the encryption process performed by Webvue's personnel during the audit.

While interviewing the manager of the QA Department, Keith observed that employees in the Security Training Department were not following proper procedures, even though this department fell outside the audit scope. Despite the exclusion in the audit scope, the nonconformity in the Security Training Department has potential implications for the processes within the audit scope, specifically impacting data security and cryptographic practices in CloudWebvue. Therefore, Keith incorporated this finding into the audit report and accordingly informed the auditee.

Based on scenario, was Keith's choice regarding the incorporation of the Security Training Department in the audit report appropriate?

A. Yes, he should have incorporated the Security Training Department in the audit report

B. No, he should have included it without informing the auditee about the observed situation

C. No, he should not have included it and only informed the auditee about the observed situation

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #58 *Topic 1*

As an auditor, you have noticed that ABC Inc. has established a procedure to manage the removable storage media. The procedure is based on the classification scheme adopted by ABC Inc. Thus, if the information stored is classified as "confidential," the procedure applies. On the other hand, information classified as "public" does not have confidentiality requirements; thus, only a procedure for ensuring its integrity and availability applies. What type of audit finding is this?

A. Nonconformity

B. Anomaly

C. Conformity

Suggested Answer: *A*

Community vote distribution

C (100%)

8e1c45b 8 months, 1 week ago

Selected Answer: C

C is right

upvoted 2 times

SuperMax 9 months, 2 weeks ago

Selected Answer: C

ABC Inc. has established a procedure for managing removable storage media based on a classification scheme. This approach ensures that "confidential" information is handled in a manner that preserves confidentiality, while "public" information is managed with a focus on integrity and availability. By aligning its procedures with the adopted classification scheme, ABC Inc. is demonstrating adherence to its established controls, processes, and standards.

In the context of an audit, this would be considered conformity because the organization is operating in compliance with its own documented policies and procedures. There is no evidence in the scenario to suggest a failure to meet requirements (nonconformity) or an irregularity that would constitute an anomaly.

upvoted 2 times

Question #59 *Topic 1*

EquiBank is undergoing an external audit of its financial management system. The auditors are evaluating the logic of transactions processed by EquiBank's financial software. To ensure accuracy, they use simulations to validate operations, calculations, and controls programmed in the software applications. What type of computer assisted audit technique (CAAT) is used by the auditors?

A. Plotting and cartography software applications

B. Utility software

C. Data test

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #60 *Topic 1*

What is the purpose of using a combination of audit test plans?

A. To verify compliance with standards and criteria through multiple methods

B. To ensure that all areas of the organization are audited equally

C. To reduce the need for frequent audits

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #61 *Topic 1*

Which of the following types of audit requires that the auditee and audit team agree on remote access protocols prior to conducting the audit?

A. Virtual

B. Internal

C. External

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #62 *Topic 1*

What is the purpose of audit test plans in the audit process?

A. To develop detailed audit reports

B. To conduct audit procedures such as observation and interviews

C. To select all elements of the management system for validation

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #63 *Topic 1*

The auditor used sampling to ensure that event logs recording information security events are maintained and regularly reviewed. Sampling was based on the audit objectives, whereas the sample selection process was based on the probability theory. What type of sampling was used?

A. Statistical sampling

B. Judgment-based sampling

C. Multi-site sampling

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #64 *Topic 1*

Which option below is correct about the audit plan?

A. The audit plan involves the use of several audit procedures

B. The audit plan should be flexible to allow for modifications

C. The auditee's top management prepares the audit plan

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #65 *Topic 1*

Which of the following can be considered as a minor nonconformity?

A. The organization has established access control measures limiting access to sensitive data; however, employees are not regularly trained to recognize phishing attempts, increasing the risk of malware infiltration and data breaches

B. The organization has implemented a password policy requiring complex passwords, but the system lacks multi-factor authentication, leaving accounts vulnerable to unauthorized access in case of password compromise

C. The organization has communicated its information security policy, including a framework for objectives and action principles. The policy considers business characteristics, and legal, regulatory, and contractual requirements, but lacks reference to continual ISMS improvement

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #66 *Topic 1*

Scenario: Tessa, Malik, and Michael are an audit team of independent and qualified experts in the field of security, compliance, and business planning and strategies. They are assigned to conduct a certification audit in Clastus, a large web design company. They have previously shown excellent work ethics, including impartiality and objectiveness, while conducting audits. This time, Clastus is positive that they will be one step ahead if they get certified against ISO/IEC 27001.

Tessa, the audit team leader, has expertise in auditing and a very successful background in IT-related issues, compliance, and governance. Malik has an organizational planning and risk management background. His expertise relies on the level of synthesis and analysis of an organizations security controls and its risk tolerance in accurately characterizing the risk level within an organization. On the other hand, Michael is an expert in the practical security of controls assessment by following rigorous standardized programs.

After performing the required auditing activities, Tessa initiated an audit team meeting. They analyzed one of Michael's findings to decide on the issue objectively and accurately. The issue Michael had encountered was a minor nonconformity in the organizations daily operations, which he believed was caused by one of the organization's IT technicians. As such, Tessa met with the top management and told them who was responsible for the nonconformity after they inquired about the names of the persons responsible.

To facilitate clarity and understanding, Tessa conducted the closing meeting on the last day of the audit. During this meeting, she presented the identified nonconformities to the Clastus management. However, Tessa received advice to avoid providing unnecessary evidence in the audit report for the Clastus certification audit, ensuring that the report remains concise and focused on the critical findings.

Based on the evidence examined, the audit team drafted the audit conclusions and decided that two areas of the organization must be audited before the certification can be granted. These decisions were later presented to the auditee, who did not accept the findings and proposed to provide additional information. Despite the auditee's comments, the auditors, having already decided on the certification recommendation, did not accept the additional information. The auditee's top management insisted that the audit conclusions did not represent reality, but the audit team remained firm in their decision.

Based on the scenario above, answer the following question:

Based on the decision of the audit team, what is the next step that Clastus should take?

A. Submit action plans

B. Evaluate corrective actions

C. Perform a follow-up of action plans

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #67 *Topic 1*

Scenario: Tessa, Malik, and Michael are an audit team of independent and qualified experts in the field of security, compliance, and business planning and strategies. They are assigned to conduct a certification audit in Clastus, a large web design company. They have previously shown excellent work ethics, including impartiality and objectiveness, while conducting audits. This time, Clastus is positive that they will be one step ahead if they get certified against ISO/IEC 27001.

Tessa, the audit team leader, has expertise in auditing and a very successful background in IT-related issues, compliance, and governance. Malik has an organizational planning and risk management background. His expertise relies on the level of synthesis and analysis of an organizations security controls and its risk tolerance in accurately characterizing the risk level within an organization. On the other hand, Michael is an expert in the practical security of controls assessment by following rigorous standardized programs.

After performing the required auditing activities, Tessa initiated an audit team meeting. They analyzed one of Michael's findings to decide on the issue objectively and accurately. The issue Michael had encountered was a minor nonconformity in the organizations daily operations, which he believed was caused by one of the organization's IT technicians. As such, Tessa met with the top management and told them who was responsible for the nonconformity after they inquired about the names of the persons responsible.

To facilitate clarity and understanding, Tessa conducted the closing meeting on the last day of the audit. During this meeting, she presented the identified nonconformities to the Clastus management. However, Tessa received advice to avoid providing unnecessary evidence in the audit report for the Clastus certification audit, ensuring that the report remains concise and focused on the critical findings.

Based on the evidence examined, the audit team drafted the audit conclusions and decided that two areas of the organization must be audited before the certification can be granted. These decisions were later presented to the auditee, who did not accept the findings and proposed to provide additional information. Despite the auditee's comments, the auditors, having already decided on the certification recommendation, did not accept the additional information. The auditee's top management insisted that the audit conclusions did not represent reality, but the audit team remained firm in their decision.

According to scenario, the audit team did not accept the auditee's comments because they had already taken the certification recommendation decision. Is this acceptable?

A. Yes, when the audit team decides on a certification recommendation, they cannot accept any additional information

B. No, the auditee can provide additional information if they disagree with the certification recommendation

C. No, the auditor should not consider the revisions that resulted from discussions with the auditee in the certification recommendation decision

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #68 *Topic 1*

Scenario: Tessa, Malik, and Michael are an audit team of independent and qualified experts in the field of security, compliance, and business planning and strategies. They are assigned to conduct a certification audit in Clastus, a large web design company. They have previously shown excellent work ethics, including impartiality and objectiveness, while conducting audits. This time, Clastus is positive that they will be one step ahead if they get certified against ISO/IEC 27001.

Tessa, the audit team leader, has expertise in auditing and a very successful background in IT-related issues, compliance, and governance. Malik has an organizational planning and risk management background. His expertise relies on the level of synthesis and analysis of an organizations security controls and its risk tolerance in accurately characterizing the risk level within an organization. On the other hand, Michael is an expert in the practical security of controls assessment by following rigorous standardized programs.

After performing the required auditing activities, Tessa initiated an audit team meeting. They analyzed one of Michael's findings to decide on the issue objectively and accurately. The issue Michael had encountered was a minor nonconformity in the organizations daily operations, which he believed was caused by one of the organization's IT technicians. As such, Tessa met with the top management and told them who was responsible for the nonconformity after they inquired about the names of the persons responsible.

To facilitate clarity and understanding, Tessa conducted the closing meeting on the last day of the audit. During this meeting, she presented the identified nonconformities to the Clastus management. However, Tessa received advice to avoid providing unnecessary evidence in the audit report for the Clastus certification audit, ensuring that the report remains concise and focused on the critical findings.

Based on the evidence examined, the audit team drafted the audit conclusions and decided that two areas of the organization must be audited before the certification can be granted. These decisions were later presented to the auditee, who did not accept the findings and proposed to provide additional information. Despite the auditee's comments, the auditors, having already decided on the certification recommendation, did not accept the additional information. The auditee's top management insisted that the audit conclusions did not represent reality, but the audit team remained firm in their decision.

According to scenario, what must the audit team leader, Tessa, do regarding the presentation of nonconformities during the closing meeting?

A. Provide detailed analysis of each nonconformity, including potential impacts on the organization

B. Only present major nonconformities

C. Consistently align discussions with the relevant standard clauses

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #69 *Topic 1*

Scenario: Tessa, Malik, and Michael are an audit team of independent and qualified experts in the field of security, compliance, and business planning and strategies. They are assigned to conduct a certification audit in Clastus, a large web design company. They have previously shown excellent work ethics, including impartiality and objectiveness, while conducting audits. This time, Clastus is positive that they will be one step ahead if they get certified against ISO/IEC 27001.

Tessa, the audit team leader, has expertise in auditing and a very successful background in IT-related issues, compliance, and governance. Malik has an organizational planning and risk management background. His expertise relies on the level of synthesis and analysis of an organizations security controls and its risk tolerance in accurately characterizing the risk level within an organization. On the other hand, Michael is an expert in the practical security of controls assessment by following rigorous standardized programs.

After performing the required auditing activities, Tessa initiated an audit team meeting. They analyzed one of Michael's findings to decide on the issue objectively and accurately. The issue Michael had encountered was a minor nonconformity in the organizations daily operations, which he believed was caused by one of the organization's IT technicians. As such, Tessa met with the top management and told them who was responsible for the nonconformity after they inquired about the names of the persons responsible.

To facilitate clarity and understanding, Tessa conducted the closing meeting on the last day of the audit. During this meeting, she presented the identified nonconformities to the Clastus management. However, Tessa received advice to avoid providing unnecessary evidence in the audit report for the Clastus certification audit, ensuring that the report remains concise and focused on the critical findings.

Based on the evidence examined, the audit team drafted the audit conclusions and decided that two areas of the organization must be audited before the certification can be granted. These decisions were later presented to the auditee, who did not accept the findings and proposed to provide additional information. Despite the auditee's comments, the auditors, having already decided on the certification recommendation, did not accept the additional information. The auditee's top management insisted that the audit conclusions did not represent reality, but the audit team remained firm in their decision.

Based on scenario, Tessa is advised to avoid providing unnecessary evidence in the audit report for the Clastus certification audit. Is this recommended?

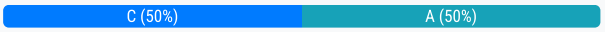
A. Yes, to avoid including information that may compromise the audits confidentiality

B. Yes, to simplify the report for a better understanding

C. Yes, to ensure that all relevant evidence is considered and addressed

Suggested Answer: *B*

Community vote distribution



ROCTW 5 months ago

Selected Answer: A

C has logical inconsistency.

Given these considerations, option A appears to be the more logically sound answer when interpreting "avoid providing unnecessary evidence" within the context of audit practice that balances information sufficiency with confidentiality. It reflects the need for audit reports to be concise while also managing information sensitivity.

Option C, on the other hand, is problematic due to its semantic contradiction.

Therefore, A is recommended based on the consideration of audit report content and confidentiality management, while C is problematic due to its logical inconsistency.

upvoted 1 times

ROCTW 5 months ago

Selected Answer: C

The core principle of an audit report, especially for certification, is that it must be accurate, complete, and provide sufficient evidence to support its findings and conclusions. While conciseness is desirable, it cannot come at the expense of completeness or accuracy.

upvoted 1 times

Question #70 *Topic 1*

Scenario: Tessa, Malik, and Michael are an audit team of independent and qualified experts in the field of security, compliance, and business planning and strategies. They are assigned to conduct a certification audit in Clastus, a large web design company. They have previously shown excellent work ethics, including impartiality and objectiveness, while conducting audits. This time, Clastus is positive that they will be one step ahead if they get certified against ISO/IEC 27001.

Tessa, the audit team leader, has expertise in auditing and a very successful background in IT-related issues, compliance, and governance. Malik has an organizational planning and risk management background. His expertise relies on the level of synthesis and analysis of an organizations security controls and its risk tolerance in accurately characterizing the risk level within an organization. On the other hand, Michael is an expert in the practical security of controls assessment by following rigorous standardized programs.

After performing the required auditing activities, Tessa initiated an audit team meeting. They analyzed one of Michael's findings to decide on the issue objectively and accurately. The issue Michael had encountered was a minor nonconformity in the organizations daily operations, which he believed was caused by one of the organization's IT technicians. As such, Tessa met with the top management and told them who was responsible for the nonconformity after they inquired about the names of the persons responsible.

To facilitate clarity and understanding, Tessa conducted the closing meeting on the last day of the audit. During this meeting, she presented the identified nonconformities to the Clastus management. However, Tessa received advice to avoid providing unnecessary evidence in the audit report for the Clastus certification audit, ensuring that the report remains concise and focused on the critical findings.

Based on the evidence examined, the audit team drafted the audit conclusions and decided that two areas of the organization must be audited before the certification can be granted. These decisions were later presented to the auditee, who did not accept the findings and proposed to provide additional information. Despite the auditee's comments, the auditors, having already decided on the certification recommendation, did not accept the additional information. The auditee's top management insisted that the audit conclusions did not represent reality, but the audit team remained firm in their decision.

According to scenario, was the closing meeting conducted accordingly?

A. Yes, the closing meeting is conducted on the last day of the audit

B. No, it should be conducted after the audit conclusions have been drafted

C. No, it should be conducted after several weeks of completing the on-site audit

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #71 *Topic 1*

Who is primarily responsible for the preparation and content of the audit report?

A. Audit team leader

B. Audit team member

C. Certification body

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #72 *Topic 1*

After analyzing the audit conclusions, Company X accepted the risk related to one of the detected nonconformities. They claimed no corrective action was necessary; however, their decision was not documented is this acceptable?

A. Yes, the auditee's management can decide to accept the risk instead of implementing corrective actions, and documenting such a decision is not necessary

B. No. the decision of the auditee to accept the risk instead of implementing corrective actions should be justified and documented

C. No, the auditee must implement corrective actions for all the observations documented during the audit

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!