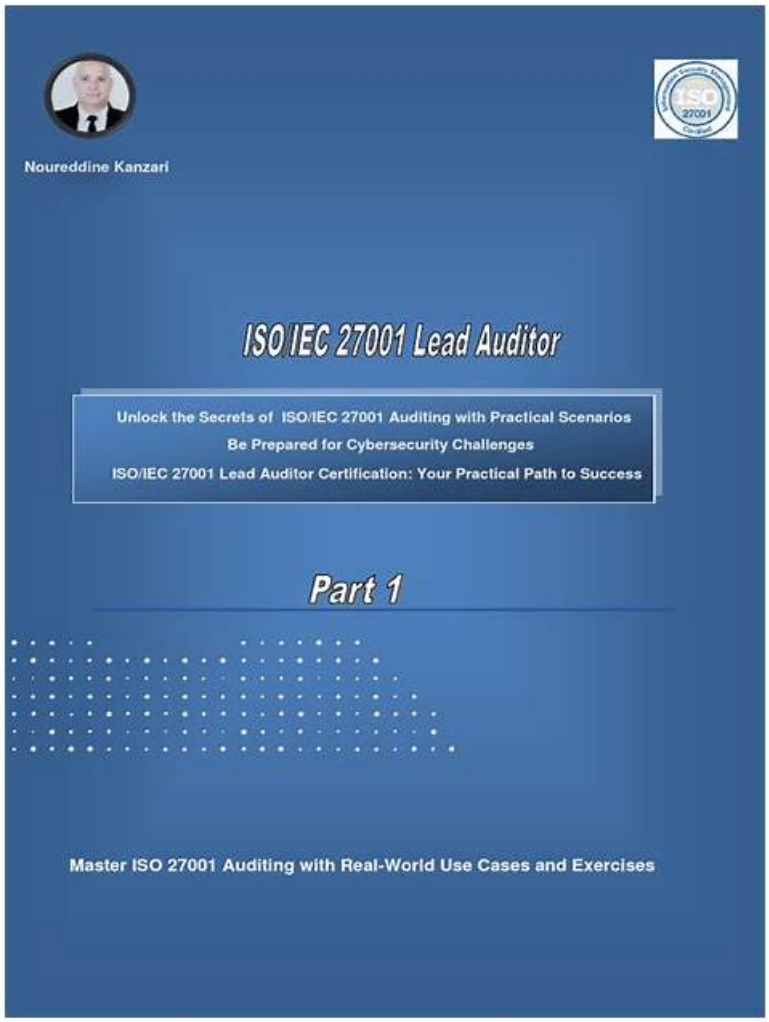
ISO-IEC-27001-Lead-Auditorトレーニング資料、ISO-IEC-27001-Lead-Auditor試験ガイド、ISO-IEC-27001-Lead-Auditor試験リソース



2026年GoShikenの最新ISO-IEC-27001-Lead-Auditor PDFダンプおよびISO-IEC-27001-Lead-Auditor試験エンジンの無料共有：https://drive.google.com/open?id=1NfH0Eu9kY9-zr-rkPJJeRgu_g7hUNjQA

常々、時間とお金ばかり効果がないです。正しい方法は大切です。我々GoShikenは一番効果的な方法を探してあなたにPECBのISO-IEC-27001-Lead-Auditor試験に合格させます。弊社のPECBのISO-IEC-27001-Lead-Auditorソフトを購入するのを決めるとき、我々は各方面であなたに保障を提供します。購入した前の無料の試み、購入するときのお支払いへの保障、購入した一年間の無料更新PECBのISO-IEC-27001-Lead-Auditor試験に失敗した全額での返金…これらは我々のお客様への承諾です。

PECB ISO-IEC-27001-Lead-Auditorの認定資格は、ISO/IEC 27001規格の認定リード監査員になることを目指すプロフェッショナル向けに設計されています。この認定試験は、情報セキュリティ、ITガバナンス、品質管理を含むさまざまな分野でのプロフェッショナルな認定資格やトレーニングコースを提供するグローバルなプロバイダーであるPECBによって提供されています。

>> ISO-IEC-27001-Lead-Auditor模擬試験問題集 <<

素敵なISO-IEC-27001-Lead-Auditor模擬試験問題集試験-試験の準備方法-正確的なISO-IEC-27001-Lead-Auditor日本語受験攻略

ISO-IEC-27001-Lead-Auditor学習教材は、すべての人々が学習効率を向上させるのに非常に役立ちます。すべてを効率的に行うと、プロモーションが簡単になります。 ISO-IEC-27001-Lead-Auditor試験の準備に費やす時間を短縮したい場合、ISO-IEC-27001-Lead-Auditor試験に合格して短時間で認定資格を取得したい場合は、ISO-IEC-27001-Lead-Auditor学習教材が最適な選択となります。あなたの夢。 ISO-IEC-27001-Lead-Auditor試験の質問を20〜30時間学習するだけで、自信を持ってISO-IEC-27001-Lead-Auditor試験に合格することができます。

PECB ISO-IEC-27001-Lead-Auditor資格試験は、世界的に認知され、産業界でも高く評価されています。この資格は、情報セキュリティ管理と監査における専門知識を証明することを望む個人にとって、貴重な資産です。この資格は、情報セキュリティに対する組織の取り組みや国際基準の遵守を示したい組織にも有益です。

PECB Certified ISO/IEC 27001 Lead Auditor exam 認定 ISO-IEC-27001-Lead-Auditor 試験問題 (Q286-Q291):

質問 # 286
Which two of the following statements are true?

- A. The audit programme describes the arrangements for a set of one or more audits planned for a specific time frame and directed towards a specific purpose.
- B. The audit plan describes the arrangements for a set of one or more audits planned for a specific time frame and directed towards a specific purpose.
- C. The audit plan describes the activities and arrangements for an audit.
- D. Once agreed, the audit plan is fixed and cannot be changed during the conducting of the audi.
- E. The audit programme describes the activities and arrangements for an audit.
- F. Responsibility for managing the audit programme rests with the audit team leader.

正解：B、C

解説：
The two true statements are B and E. According to ISO 19011:2022, the audit plan describes the arrangements for a set of one or more audits planned for a specific time frame and directed towards a specific purpose1, while the audit programme describes the activities and arrangements for an audit2. The other options are either false or irrelevant. The responsibility for managing the audit programme rests with the audit programme manager, not the audit team leader (A)3. The audit plan can be changed during the conducting of the audit if necessary, with the agreement of the audit client and the auditee4. The audit programme and the audit plan are not the same thing, so D and F are incorrect. References: 1: ISO 19011:2022, Guidelines for auditing management systems, Clause 3.8 \n2: ISO 19011:2022, Guidelines for auditing management systems, Clause 3.9 \n3: ISO 19011:2022, Guidelines for auditing management systems, Clause 5.3.1 \n4: ISO 19011:2022, Guidelines for auditing management systems, Clause 6.4.2

質問 # 287
During a third-party certification audit, you are presented with a list of issues by an auditee. Which four of the following constitute 'internal' issues in the context of a management system to ISO 27001:2022?

- A. Inability to source raw materials due to government sanctions
- B. A rise in interest rates in response to high inflation
- C. Poor levels of staff competence as a result of cuts in training expenditure
- D. Increased absenteeism as a result of poor management
- E. Poor morale as a result of staff holidays being reduced
- F. Higher labour costs as a result of an aging population
- G. A reduction in grants as a result of a change in government policy
- H. A fall in productivity linked to outdated production equipment

正解：C、D、E、H

解説：
According to ISO 27001:2022 clause 4.1, the organisation shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system (ISMS)12 External issues are factors outside the organisation that it cannot control, but can influence or adapt to. They include political, economic, social, technological, legal, and environmental factors that may affect the organisation's information security objectives, risks, and opportunities12 Internal issues are factors within the organisation that it can control or change. They include the organisation's structure, culture, values, policies, objectives, strategies, capabilities, resources, processes, activities, relationships, and performance that may affect the organisation's information security management system12 Therefore, the following issues are

considered 'internal' in the context of a management system to ISO 27001:2022:
Poor levels of staff competence as a result of cuts in training expenditure: This is an internal issue because it relates to the organisation's capability, resource, and process of developing and maintaining the competence of its personnel involved in the ISMS. The organisation can control or change its training expenditure and its impact on staff competence12 Poor morale as a result of staff holidays being reduced: This is an internal issue because it relates to the organisation's culture, value, and relationship with its employees. The organisation can control or change its staff holiday policy and its impact on staff morale12 Increased absenteeism as a result of poor management: This is an internal issue because it relates to the organisation's performance, structure, and accountability of its management. The organisation can control or change its management practices and its impact on staff absenteeism12 A fall in productivity linked to outdated production equipment: This is an internal issue because it relates to the organisation's capability, resource, and process of ensuring the availability and suitability of its production equipment. The organisation can control or change its equipment maintenance and upgrade and its impact on productivity12 The following issues are considered 'external' in the context of a management system to ISO 27001:2022:
Higher labour costs as a result of an aging population: This is an external issue because it relates to the social and demographic factor that affects the availability and cost of labour in the market. The organisation cannot control or change the aging population, but can influence or adapt to its impact on labour costs12 A rise in interest rates in response to high inflation: This is an external issue because it relates to the economic and monetary factor that affects the cost and availability of capital in the market. The organisation cannot control or change the interest rates or inflation, but can influence or adapt to its impact on capital costs12 A reduction in grants as a result of a change in government policy: This is an external issue because it relates to the political and legal factor that affects the availability and conditions of public funding for the organisation. The organisation cannot control or change the government policy, but can influence or adapt to its impact on grants12 Inability to source raw materials due to government sanctions: This is an external issue because it relates to the political and legal factor that affects the availability and cost of raw materials in the market. The organisation cannot control or change the government sanctions, but can influence or adapt to its impact on raw materials12 Reference:
1: ISO/IEC 27001:2022 Lead Auditor (Information Security Management Systems) Course by CQI and IRCA Certified Training 1
2: ISO/IEC 27001 Lead Auditor Training Course by PECB 2

質問 # 288
Which two of the following options do not participate in a first-party audit?

- A. An auditor from a consultancy organisation
- B. An auditor trained in the CQI and IRCA scheme
- C. An auditor trained in the organization
- D. A certification body auditor
- E. An auditor certified by CQI and IRCA
- F. An audit team from an accreditation body

正解：D、F

解説：
Explanation
A first-party audit is an internal audit in which the organization's own staff or contractors check the conformity and effectiveness of the ISMS. A certification body auditor and an audit team from an accreditation body are external auditors who conduct audits for the purpose of certification or accreditation.
They do not participate in a first-party audit, but rather in a third-party audit. References: First & Second Party Audits - operational services, The ISO 27001 Audit Process | Blog | OneTrust, The ISO 27001 Audit Process | A Beginner's Guide - IAS USA

質問 # 289
Scenario 7: Lawsy is a leading law firm with offices in New Jersey and New York City. It has over 50 attorneys offering sophisticated legal services to clients in business and commercial law, intellectual property, banking, and financial services. They believe they have a comfortable position in the market thanks to their commitment to implement information security best practices and remain up to date with technological developments.
Lawsy has implemented, evaluated, and conducted internal audits for an ISMS rigorously for two years now.
Now, they have applied for ISO/IEC 27001 certification to ISMA, a well-known and trusted certification body.
During stage 1 audit, the audit team reviewed all the ISMS documents created during the implementation.
They also reviewed and evaluated the records from management reviews and internal audits.
Lawsy submitted records of evidence that corrective actions on nonconformities were performed when necessary, so the audit team interviewed the internal auditor. The interview validated the adequacy and frequency of the internal audits by providing detailed insight into the internal audit plan and procedures.

The audit team continued with the verification of strategic documents, including the information security policy and risk evaluation criteria. During the information security policy review, the team noticed inconsistencies between the documented information describing governance framework (i.e., the information security policy) and the procedures.
Although the employees were allowed to take the laptops outside the workplace, Lawsy did not have procedures in place regarding the use of laptops in such cases. The policy only provided general information about the use of laptops. The company relied on employees' common knowledge to protect the confidentiality and integrity of information stored in the laptops. This issue was documented in the stage 1 audit report.
Upon completing stage 1 audit, the audit team leader prepared the audit plan, which addressed the audit objectives, scope, criteria, and procedures.
During stage 2 audit, the audit team interviewed the information security manager, who drafted the information security policy. He justified the Issue identified in stage 1 by stating that Lawsy conducts mandatory information security training and awareness sessions every three months.
Following the interview, the audit team examined 15 employee training records (out of 50) and concluded that Lawsy meets requirements of ISO/IEC 27001 related to training and awareness. To support this conclusion, they photocopied the examined employee training records.
Based on the scenario above, answer the following question:
Based on scenario 7, what should Lawsy do prior to the initiation of stage 2 audit?

- A. Define which audit test plans can be combined to verify compliance
- B. Perform a quality review of audit findings from stage 1 audit
- C. Review and confirm the audit plan with the certification body

正解：C

解説：
Prior to the initiation of stage 2 audit, Lawsy should review and confirm the audit plan with the certification body. This ensures that both parties agree on the objectives, scope, and procedures for the stage 2 audit, thus aligning expectations and facilitating a smoother audit process.
References: ISO 19011:2018, Guidelines for auditing management systems

質問 # 290
Scenario 9: Techmanic is a Belgian company founded in 1995 and currently operating in Brussels. It provides IT consultancy, software design, and hardware/software services, including deployment and maintenance. The company serves sectors like public services, finance, telecom, energy, healthcare, and education. As a customer-centered company, it prioritizes strong client relationships and leading security practices.
Techmanic has been ISO/IEC 27001 certified for a year and regards this certification with pride. During the certification audit, the auditor found some inconsistencies in its ISMS implementation. Since the observed situations did not affect the capability of its ISMS to achieve the intended results, Techmanic was certified after auditors followed up on the root cause analysis and corrective actions remotely During that year, the company added hosting to its list of services and requested to expand its certification scope to include that area The auditor in charge approved the request and notified Techmanic that the extension audit would be conducted during the surveillance audit Techmanic underwent a surveillance audit to verify its iSMS's continued effectiveness and compliance with ISO/IEC 27001. The surveillance audit aimed to ensure that Techmanic's security practices, including the recent addition of hosting services, aligned seamlessly with the rigorous requirements of the certification The auditor strategically utilized the findings from previous surveillance audit reports in the recertification activity with the purpose of replacing the need for additional recertification audits, specifically in the IT consultancy sector. Recognizing the value of continual improvement and learning from past assessments. Techmanic implemented a practice of reviewing previous surveillance audit reports. This proactive approach not only facilitated identifying and resolving potential nonconformities but also aimed to streamline the recertification process in the IT consultancy sector.
During the surveillance audit, several nonconformities were found. The ISMS continued to fulfill the ISO/IEC 27001*s requirements, but Techmanic failed to resolve the nonconformities related to the hosting services, as reported by its internal auditor. In addition, the internal audit report had several inconsistencies, which questioned the independence of the internal auditor during the audit of hosting services. Based on this, the extension certification was not granted. As a result. Techmanic requested a transfer to another certification body. In the meantime, the company released a statement to its clients stating that the ISO/IEC 27001 certification covers the IT services, as well as the hosting services.
Based on the scenario above, answer the following question:
Which of the options below does an internal audit program NOT allow?

- A. Verification of the effectiveness of corrective actions
- B. The prevention of nonconformities
- C. The reduction of manual audit tasks

正解：B

解説：
Comprehensive and Detailed In-Depth
C . Correct answer:
Internal audits detect nonconformities but do not actively prevent them.
A . Incorrect:
Internal audits verify corrective actions.
B . Incorrect:
Technology can reduce manual tasks in internal audits.
Relevant Standard Reference:

質問 # 291
.....

る：https://drive.google.com/open?id=1NfH0Eu9kY9-zr-rkPJJeRgu_g7hUNjQA