ISO-IEC-27001-Foundation必殺問題集、ISO-IEC-27001-Foundationトレーニング資料

さらに、Tech4Exam ISO-IEC-27001-Foundationダンプの一部が現在無料で提供されています：https://drive.google.com/open?id=17dfibDS6_0pU5NjjkXYjy8HeG5xKdJ6k

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Tech4Examは一番効果的な方法を探してあなたにAPMG-InternationalのISO-IEC-27001-Foundation試験に合格させます。弊社のAPMG-InternationalのISO-IEC-27001-Foundation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APMG-InternationalのISO-IEC-27001-Foundation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。

APMG-International ISO-IEC-27001-Foundation 認定試験の出題範囲：

トピック	出題範囲
トピック 1	• 自信: 自信とは、自分の能力、能力、価値を信じることです。確信感と内面の強さを反映します。
トピック 2	• コンプライアンス: 規制コンプライアンスとは、組織が適用される法律、ポリシー、規制を理解して遵守し、確立された法的および倫理的基準の範囲内で運営するという取り組みを指します。
トピック 3	• 継続的改善プロセス (CI、CIP): 継続的または継続的改善プロセス (CIP または CI) には、時間の経過とともにより高い効率性と有効性を達成するために、製品、サービス、または運用プロセスを強化する継続的かつ体系的な取り組みが含まれます。
トピック 4	• サイバーセキュリティ: サイバーセキュリティは、IT セキュリティまたはコンピュータ セキュリティとも呼ばれ、コンピュータ システム、ネットワーク、およびデータを不正アクセス、盗難、損傷、または中断から保護し、デジタル情報の整合性と可用性を確保することを目的としています。

最新のISO-IEC-27001-Foundation必殺問題集 & 合格スムーズISO-IEC-27001-Foundationトレーニング資料 | 100％合格率のISO-IEC-27001-Foundation専門知識

日常生活の低生産性と低効率にまだ圧倒されていますか？答えが「はい」の場合、ISO-IEC-27001-Foundationガイド急流に注意してください。バランスのとれた一流のサービスを提供するため、夢のISO-IEC-27001-Foundation証明書を取得し、希望の職業に就くことができます。当社の製品にはいくつかの主要な機能があり、ISO-IEC-27001-Foundationテストの質問に満足していただけると信じています。そして、ISO-IEC-27001-Foundation試験問題を一度試してみると、きっと気に入るはずです。

APMG-International ISO/IEC 27001 (2022) Foundation Exam 認定 ISO-IEC-27001-Foundation 試験問題 (Q19-Q24):

質問 # 19
Which statement about the conduct of audits is true?

- A. During Stage 1 of a certification audit, evidence is collected by observing activities
- B. The certificate issued after a successful re-certification audit in typical schemes lasts for one year
- C. One of the focus areas for a surveillance audit is the output from internal audits and management reviews
- D. Third party audits are conducted by a customer of the organization

正解：C

解説：
Clause 9.2 (Internal Audit) and Clause 9.3 (Management Review) highlight that audit outputs and management reviews are key inputs for evaluating ISMS performance. Surveillance audits, conducted by Certification Bodies, check ongoing compliance and effectiveness. ISO certification schemes (per ISO/IEC
17021) require surveillance audits to verify whether corrective actions and continuous improvements are being made. A critical focus area is theresults of internal audits and management reviews, ensuring that the organization maintains its ISMS between certification cycles.
Option A is incorrect - third-party audits are performed by independent Certification Bodies, not customers.
Option B is incorrect - certificates are typically valid forthree yearswith annual surveillance. Option D is incorrect - Stage 1 is primarily adocumentation and readiness review, not evidence observation.
Therefore, the verified correct answer isC.

質問 # 20
What is the name of the control clause used to control information security breaches within Annex A of ISO
/IEC 27001?

- A. Response to information security events
- B. Reporting information security incidents
- C. Information security event management
- D. Information security event reporting

正解：D

解説：
Comprehensive and Detailed Explanation From Exact Extract ISO/IEC 27002:2022 standards:
Annex A in ISO/IEC 27001 refers directly to ISO/IEC 27002 for control guidance. In ISO/IEC 27002:2022, Clause 6.8 is titled: "Information security event reporting - Information security events should be reported through appropriate management channels as quickly as possible." This control ensures breaches, incidents, or suspected issues are reported for action. The other options (B, C, D) are not the exact titles in Annex A. The official title isInformation security event reporting, confirming

質問 # 21

To whom are the information security policies required to be communicated, according to the control in Annex A of ISO/IEC 27001?

- A. Relevant personnel and relevant interested parties
- B. Only staff with accountability for ISMS operation
- C. Employees within the scope of the ISMS
- D. Top management

正解：A

解説：
Comprehensive and Detailed Explanation From Exact Extract ISO/IEC 27002:2022 standards:
Annex A.5.1 (Policies for information security) clearly specifies:
"Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties..." This means the communication obligation is not limited to top management (A) or only ISMS staff (B), nor does it stop at employees only (C). Instead, ISO/IEC 27001/27002 mandate a broader scope: allrelevant personnel and relevant interested partiesmust be informed. This ensures both internal stakeholders (employees, contractors, temporary staff) and external interested parties (suppliers, partners, regulators, customers, etc.) receive the right policy communications where applicable. Therefore, the correct and verified answer isD.

質問 # 22
Which activity is a required element of information security risk identification?

- A. Determine the risk owners
- B. Prioritize the risk for treatment
- C. Determine the level of risk
- D. Consider the likelihood of the occurrence

正解：A

解説：
Clause 6.1.2 defines the mandatory elements of risk assessment. Under risk identification, the standard requires: "identifies the information security risks:1) apply the information security risk assessment process to identify risks...; and2) identify the risk owners."
By contrast, considering likelihood and determining levels of risk (options B and D) are part ofrisk analysis(6.1.2 d) "assess the realistic likelihood...";
"determine the levels of risk"), and prioritization for treatment (option C) is part ofrisk evaluation(6.1.2 e)
"prioritize the analysed risks for risk treatment"). Therefore, the specific activity that belongs torisk identificationis toidentify the risk owners. This sequencing is prescribed to ensure each risk has a designated owner responsible for decisions on treatment and acceptance downstream.

質問 # 23
Which trend in information security performance is required to be considered during a management review of the ISMS?

- A. Validity of information continuity controls
- B. Achievement of information security objectives
- C. Decisions related to continual improvement opportunities
- D. Relevant external and internal requirements changes

正解：B

解説：
Clause 9.3.2 (Management Review Inputs) states that management reviews shall include:
"c) information on the information security performance, including trends in: (1) nonconformities and corrective actions; (2) monitoring and measurement results; (3) audit results; and (4) fulfilment of information security objectives." This makesachievement of information security objectives(option A) a required trend to be considered.
While external/internal requirements (C) and continual improvement opportunities (D) are also part of management review inputs, they are not specifically listed under "trends in performance." Option B is outside the direct requirement.
Thus, the verified answer isA.

質問 # 24
......

APMG-InternationalのISO-IEC-27001-Foundation試験はIT領域で人気がある重要な試験です。我々はIT領域の人々にショートカットを提供するために、最高のスタディガイドと最高のオンラインサービスを用意して差し上げます。Tech4Examの APMG-InternationalのISO-IEC-27001-Foundation試験問題集は全ての試験の内容と答案に含まれています。Tech4Examの模擬テストを利用したら、これはあなたがずっと全力を尽くてもらいたいもののことが分かって、しかもそれは正に試験の準備をすることを意識します。