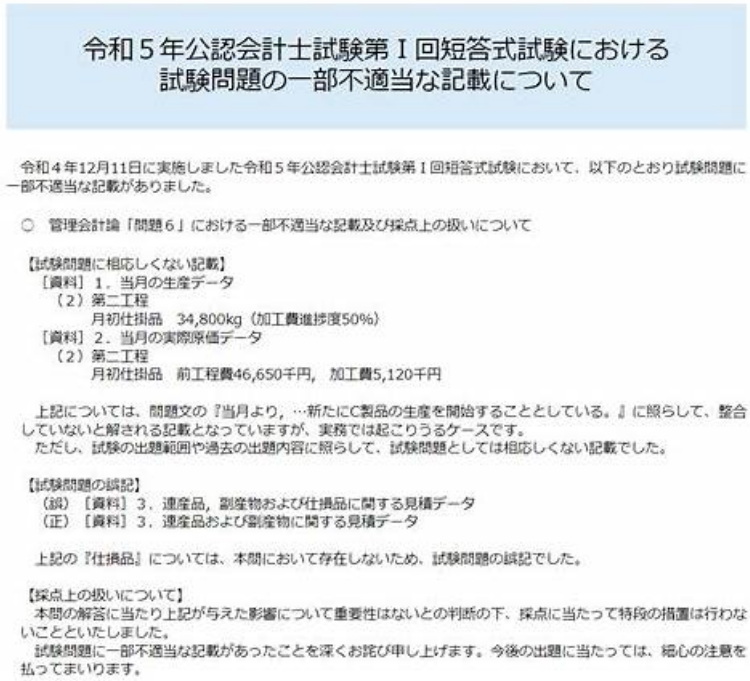
完璧なCCOA入門知識試験-試験の準備方法-正確的なCCOA対応資料


令和５年公認会計士試験第Ⅰ回短答式試験における
試験問題の一部不適当な記載について

令和４年12月11日に実施しました令和５年公認会計士試験第Ⅰ回短答式試験において、以下のとおり試験問題に一部不適当な記載がありました。

○　管理会計論「問題６」における一部不適当な記載及び採点上の扱いについて

【試験問題に相応しくない記載】
［資料］１．当月の生産データ
（２）第二工程
月初仕掛品　34,800kg（加工費進捗度50%）
［資料］２．当月の実際原価データ
（２）第二工程
月初仕掛品　前工程費46,650千円，加工費5,120千円

上記については、問題文の『当月より，…新たにC製品の生産を開始することとしている。』に照らして、整合していないと解される記載となっていますが、実務では起こりうるケースです。
ただし、試験の出題範囲や過去の出題内容に照らして、試験問題としては相応しくない記載でした。

【試験問題の誤記】
（誤）［資料］３．連産品，副産物および仕損品に関する見積データ
（正）［資料］３．連産品および副産物に関する見積データ

上記の『仕損品』については、本問において存在しないため、試験問題の誤記でした。

【採点上の扱いについて】
本問の解答に当たり上記が与えた影響について重要性はないとの判断の下、採点に当たって特段の措置は行わないこととといたしました。
試験問題に一部不適当な記載があったことを深くお詫び申し上げます。今後の出題に当たっては、細心の注意を払ってまいります。

P.S. PassTestがGoogle Driveで共有している無料かつ新しいCCOAダンプ：https://drive.google.com/open?id=13Sjq7fgcZkUlyeEncBV8JHpAsvVrfTLo

IT職員の皆さんにとって、ISACAのCCOA資格を持っていないならちょっと大変ですね。この認証資格はあなたの仕事にたくさんのメリットを与えられ、あなたの昇進にも助けになることができます。とにかく、CCOA試験は皆さんのキャリアに大きな影響をもたらせる試験です。CCOA試験に合格したいなら、我々の商品を入手してください。あなたの要求を満たすことができます。

すべての顧客のニーズを満たすために、当社はこの分野で多くの主要な専門家と教授を採用しました。これらの専門家と教授は、お客様向けに高品質のCCOA試験問題を設計しました。当社の製品がすべての人々に適していると約束できます。 CCOA実践教材を購入して真剣に検討する限り、短時間で試験に合格して認定を取得することをお約束します。 CCOA試験の質問を選択してレビューに役立ててください。CCOAスタディガイドから多くのメリットを得ることができます。

>> CCOA入門知識 <<

CCOA対応資料 & CCOAトレーニング費用

ISACAのCCOA試験準備が高い合格率であるだけでなく、当社のサービスも完璧であるため、当社の製品を購入すると便利です。 さらに、このアップデートでは、最新かつ最も有用なISACA Certified Cybersecurity Operations Analyst試験ガイドを提供し、より多くのことを学び、さらにマスターすることができます。 PassTest販売前後のさまざまなバージョンを選択できる優れたカスタマーサービスを提供しています。無料デモをダウンロードして、購入前にCCOAガイドトレントの品質を確認できます。 CCOA試験問題の購入に失望することはありません。

ISACA CCOA 認定試験の出題範囲：

トピック	出題範囲

トピック 1	• Securing Assets: This section of the exam measures skills of a Cybersecurity Specialist and covers the methods and strategies used to secure organizational assets. It includes topics like endpoint security, data protection, encryption techniques, and securing network infrastructure. The goal is to ensure that sensitive information and resources are properly protected from external and internal threats.
トピック 2	• Technology Essentials: This section of the exam measures skills of a Cybersecurity Specialist and covers the foundational technologies and principles that form the backbone of cybersecurity. It includes topics like hardware and software configurations, network protocols, cloud infrastructure, and essential tools. The focus is on understanding the technical landscape and how these elements interconnect to ensure secure operations.
トピック 3	• Incident Detection and Response: This section of the exam measures the skills of a Cybersecurity Analyst and focuses on detecting security incidents and responding appropriately. It includes understanding security monitoring tools, analyzing logs, and identifying indicators of compromise. The section emphasizes how to react to security breaches quickly and efficiently to minimize damage and restore operations.
トピック 4	• Adversarial Tactics, Techniques, and Procedures: This section of the exam measures the skills of a Cybersecurity Analyst and covers the tactics, techniques, and procedures used by adversaries to compromise systems. It includes identifying methods of attack, such as phishing, malware, and social engineering, and understanding how these techniques can be detected and thwarted.
トピック 5	• Cybersecurity Principles and Risk: This section of the exam measures the skills of a Cybersecurity Specialist and covers core cybersecurity principles and risk management strategies. It includes assessing vulnerabilities, threat analysis, and understanding regulatory compliance frameworks. The section emphasizes evaluating risks and applying appropriate measures to mitigate potential threats to organizational assets.

ISACA Certified Cybersecurity Operations Analyst 認定 CCOA 試験問題 (Q130-Q135):

質問 # 130
Which of the following MOST directly supports the cybersecurity objective of integrity?

- A. Data backups
- B. Encryption
- C. Digital signatures
- D. Least privilege

正解： C

解説：
The cybersecurity objective ofintegrityensures that data isaccurate, complete, and unaltered. The most direct method to support integrity is the use ofdigital signaturesbecause:
* Tamper Detection:A digital signature provides a way to verify that data has not been altered after signing.
* Authentication and Integrity:Combines cryptographic hashing and public key encryption to validate both the origin and the integrity of data.
* Non-Repudiation:Ensures that the sender cannot deny having sent the message.
* Use Case:Digital signatures are commonly used in secure email, software distribution, and document verification.
Other options analysis:
* A. Data backups:Primarily supports availability, not integrity.
* C. Least privilege:Supports confidentiality by limiting access.
* D. Encryption:Primarily supports confidentiality by protecting data from unauthorized access.
CCOA Official Review Manual, 1st Edition References:
* Chapter 5: Data Integrity Mechanisms:Discusses the role of digital signatures in preserving data integrity.
* Chapter 8: Cryptographic Techniques:Explains how signatures authenticate data.

質問 # 131
Which of the following risks is MOST relevant to cloud auto-scaling?

- A. Unforeseen expenses
- B. Data breaches
- C. Loss of integrity
- D. Loss of confidentiality

正解：A

解説：
One of the most relevant risks associated withcloud auto-scalingisunforeseen expenses:
* Dynamic Resource Allocation:Auto-scaling automatically adds resources based on demand, which can increase costs unexpectedly.
* Billing Surprises:Without proper monitoring, auto-scaling can significantly inflate cloud bills, especially during traffic spikes.
* Mitigation:Implementing budget controls and alerts helps manage costs.
* Financial Risk:Organizations may face budget overruns if auto-scaling configurations are not properly optimized.
Incorrect Options:
* A. Loss of confidentiality:Not directly related to auto-scaling.
* B. Loss of integrity:Auto-scaling does not inherently affect data integrity.
* C. Data breaches:More related to security misconfigurations rather than scaling issues.
Exact Extract from CCOA Official Review Manual, 1st Edition:
Refer to Chapter 3, Section "Cloud Security Challenges," Subsection "Cost Management in Auto-Scaling" - Uncontrolled auto-scaling can lead to significant and unexpected financial impact.

質問 # 132
Your enterprise has received an alert bulletin fromnational authorities that the network has beencompromised at approximately 11:00 PM (Absolute) onAugust 19, 2024. The alert is located in the alerts folderwith filename, alert_33.pdf.
Use the IOCs to find the compromised host. Enter thehost name identified in the keyword agent.name fieldbelow.

正解：

解説：
See the solution in Explanation.
Explanation:
To identify the compromised host using thekeyword agent.name, follow these steps:
Step 1: Access the Alert Bulletin
* Navigate to thealerts folderon your system.
* Locate the alert file:
alert_33.pdf
* Open the file with a PDF reader and review its contents.
Key Information to Extract:
* Indicators of Compromise (IOCs) provided in the bulletin:
* File hashes
* IP addresses
* Hostnames
* Keywords related to the compromise
Step 2: Log into SIEM or Log Management System
* Access your organization'sSIEMor centralized log system.
* Make sure you have the appropriate permissions to view log data.
Step 3: Set Up Your Search
* Time Filter:
* Set the time window toAugust 19, 2024, around11:00 PM (Absolute).
* Keyword Filter:
* Use the keywordagent.nameto search for host information.
* IOC Correlation:
* Incorporate IOCs from thealert_33.pdffile (e.g., IP addresses, hash values).
Example SIEM Query:
index=host_logs
| search "agent.name" AND (IOC_from_alert OR "2024-08-19T23:00:00")

| table _time, agent.name, host.name, ip_address, alert_id
Step 4: Analyze the Results
* Review the output for any host names that appear unusual or match the IOCs from the alert bulletin.
* Focus on:
* Hostnames that appeared at 11:00 PM
* Correlation with IOC data(hash, IP, filename)
Example Output:
_time agent.name host.name ip_address alert_id
2024-08-19T23:01 CompromisedAgent COMP-SERVER-01 192.168.1.101 alert_33 Step 5: Verify the Host
* Cross-check the host name identified in the logs with the information fromalert_33.pdf.
* Ensure the host name corresponds to the malicious activity noted.
The host name identified in the keyword agent.name field is: COMP-SERVER-01 Step 6: Mitigation and Response
* Isolate the Compromised Host:
* Remove the affected system from the network to prevent lateral movement.
* Conduct Forensic Analysis:
* Inspect system processes, logs, and network activity.
* Patch and Update:
* Apply security updates and patches.
* Threat Hunting:
* Look for signs of compromise in other systems using the same IOCs.
Step 7: Document and Report
* Create a detailed incident report:
* Date and Time:August 19, 2024, at 11:00 PM
* Compromised Host Name:COMP-SERVER-01
* Associated IOCs:(as per alert_33.pdf)
By following these steps, you successfully identify the compromised host and take initial steps to contain and investigate the incident.
Let me know if you need further assistance!

質問 # 133
Which of the following is the BEST way for an organization to balance cybersecurity risks and address compliance requirements?

- A. Implement only the compliance requirements that do not Impede business functions or affect cybersecurity risk.
- B. Accept that compliance requirements may conflict with business needs and operate in a diminished capacity to achieve compliance.
- C. Evaluate compliance requirements in thecontext at business objectives to ensure requirements can be implemented appropriately.
- D. Meet the minimum standards for the compliance requirements to ensure minimal impact to business operations,

正解：C

解説：
Balancingcybersecurity riskswithcompliance requirementsrequires a strategic approach that aligns security practices with business goals. The best way to achieve this is to:
* Contextual Evaluation:Assess compliance requirements in relation to the organization's operational needs and objectives.
* Risk-Based Approach:Instead of blindly following standards, integrate them within the existing risk management framework.
* Custom Implementation:Tailor compliance controls to ensure they do not hinder critical business functions while maintaining security.
* Stakeholder Involvement:Engage business units to understand how compliance can be integrated smoothly.
Other options analysis:
* A. Accept compliance conflicts:This is a defeatist approach and does not resolve the underlying issue.
* B. Meet minimum standards:This might leave gaps in security and does not foster a comprehensive risk-based approach.
* D. Implement only non-impeding requirements:Selectively implementing compliance controls can lead to critical vulnerabilities.
CCOA Official Review Manual, 1st Edition References:
* Chapter 2: Governance and Risk Management:Discusses aligning compliance with business objectives.
* Chapter 5: Risk Management Strategies:Emphasizes a balanced approach to security and compliance.

質問 # 134
The CISO has received a bulletin from law enforcementauthorities warning that the enterprise may be at risk ofattack from a specific

threat actor. Review the bulletin named CCOA Threat Bulletin.pdf on the Desktop.
Which of the following domain name(s) from the CCOAThreat Bulletin.pdf was contacted between 12:10 AMto 12:12 AM (Absolute) on August 17, 2024?

正解：

解説：
See the solution in Explanation.
Explanation:
Step 1: Understand the Objective
Objective:
* Identify thedomain name(s)that werecontactedbetween:
12:10 AM to 12:12 AM on August 17, 2024
* Source of information:
CCOA Threat Bulletin.pdf
* File location:
~/Desktop/CCOA Threat Bulletin.pdf
Step 2: Prepare for Investigation
2.1: Ensure Access to the File
* Check if the PDF exists:
ls ~/Desktop | grep "CCOA Threat Bulletin.pdf"
* Open the file to inspect:
xdg-open ~/Desktop/CCOA\ Threat\ Bulletin.pdf
* Alternatively, convert to plain text for easier analysis:
pdftotext ~/Desktop/CCOA\ Threat\ Bulletin.pdf ~/Desktop/threat_bulletin.txt cat ~/Desktop/threat_bulletin.txt
2.2: Analyze the Content
* Look for domain names listed in the bulletin.
* Make note ofany domainsorURLsmentioned as IoCs (Indicators of Compromise).
* Example:
suspicious-domain.com
malicious-actor.net
threat-site.xyz
Step 3: Locate Network Logs
3.1: Find the Logs Directory
* The logs could be located in one of the following directories:
/var/log/
/home/administrator/hids/logs/
/var/log/httpd/
/var/log/nginx/
* Navigate to the likely directory:
cd /var/log/
ls -l
* Identify relevant network or DNS logs:
ls -l| grep -E "dns|network|http|nginx"
Step 4: Search Logs for Domain Contacts
4.1: Use the Grep Command to Filter Relevant Timeframe
* Since we are looking for connections between12:10 AM to 12:12 AMonAugust 17, 2024:
grep "2024-08-17 00:1[0-2]" /var/log/dns.log
* Explanation:
* grep "2024-08-17 00:1[0-2]": Matches timestamps between00:10and00:12.
* Replace dns.log with the actual log file name, if different.
4.2: Further Filter for Domain Names
* To specifically filter out the domains listed in the bulletin:
grep -E "(suspicious-domain.com|malicious-actor.net|threat-site.xyz)" /var/log/dns.log
* If the logs are in another file, adjust the file path:
grep -E "(suspicious-domain.com|malicious-actor.net|threat-site.xyz)" /var/log/nginx/access.log Step 5: Correlate Domains and Timeframe
5.1: Extract and Format Relevant Results
* Combine the commands to get time-specific domain hits:
grep "2024-08-17 00:1[0-2]" /var/log/dns.log | grep -E "(suspicious-domain.com|malicious-actor.net|threat- site.xyz)"
* Sample Output:

2024-08-17 00:11:32 suspicious-domain.com accessed by 192.168.1.50
2024-08-17 00:12:01 malicious-actor.net accessed by 192.168.1.75
* Interpretation:
* The command revealswhich domain(s)were contacted during the specified time.
Step 6: Verification and Documentation
6.1: Verify Domain Matches
* Cross-check the domains in the log output against those listed in theCCOA Threat Bulletin.pdf.
* Ensure that the time matches the specified range.
6.2: Save the Results for Reporting
* Save the output to a file:
grep "2024-08-17 00:1[0-2]" /var/log/dns.log | grep -E "(suspicious-domain.com|malicious-actor.net|threat- site.xyz)" > ~/Desktop/domain_hits.txt
* Review the saved file:
cat ~/Desktop/domain_hits.txt
Step 7: Report the Findings
Final Answer:
* Domain(s) Contacted:
* suspicious-domain.com
* malicious-actor.net
* Time of Contact:
* Between 12:10 AM to 12:12 AM on August 17, 2024
* Reasoning:
* Matched thelog timestampsanddomain nameswith the threat bulletin.
Step 8: Recommendations:
* Immediate Block:
* Add the identified domains to theblockliston firewalls and intrusion detection systems.
* Monitor for Further Activity:
* Keep monitoring logs for any further connection attempts to the same domains.
* Perform IOC Scanning:
* Check hosts that communicated with these domains for possible compromise.
* Incident Report:
* Document the findings and mitigation actions in theincident response log.

質問 # 135
.....

今働いている受験者たちは悩んでいるのでしょう。時間と精力の不足を感じますか？CCOA試験は重要な試験だから、十分の時間と精力を利用して試験を準備します。弊社の問題集は質高いので、お客様はPassTestのCCOA問題集を利用したら、少ない時間と精力で試験に気楽に合格することができます。躊躇わずに我々のCCOA問題集を購入してください。

CCOA対応資料: https://www.passtest.jp/ISACA/CCOA-shiken.html

- 素敵なCCOA入門知識一回合格-信頼的なCCOA対応資料 □ 「 www.jpshiken.com 」に移動し、➠ CCOA □□を検索して、無料でダウンロード可能な試験資料を探しますCCOA日本語受験教科書
- CCOA試験の準備方法｜ハイパスレートのCCOA入門知識試験｜更新するISACA Certified Cybersecurity Operations Analyst対応資料 □ 「 www.goshiken.com 」の無料ダウンロード➡ CCOA □□□ページが開きますCCOA PDF問題サンプル
- CCOA試験関連赤本 ☯ CCOA対応問題集 □ CCOA関連資格知識 □ ➽ www.japancert.com □には無料の《 CCOA 》問題集がありますCCOA受験準備
- CCOA資格問題対応 □ CCOA過去問 □ CCOA前提条件 ❣ ⇛ www.goshiken.com ⇚に移動し、➡ CCOA □□□を検索して、無料でダウンロード可能な試験資料を探しますCCOA受験トレーリング
- CCOA試験の準備方法｜ハイパスレートのCCOA入門知識試験｜更新するISACA Certified Cybersecurity Operations Analyst対応資料 □☀ www.passtest.jp □☀□サイトにて【 CCOA 】問題集を無料で使おうCCOA PDF問題サンプル
- 有難いCCOA入門知識試験-試験の準備方法-ハイパスレートのCCOA対応資料 □ 時間限定無料で使える➡ CCOA □の試験問題は□ www.goshiken.com □サイトで検索CCOA関連合格問題
- CCOA試験内容 □ CCOA前提条件 □ CCOA前提条件 □ ➡ www.passtest.jp □□□を開き、[CCOA]を入力して、無料でダウンロードしてくださいCCOA試験情報
- ユニークCCOA｜正確的なCCOA入門知識試験｜試験の準備方法ISACA Certified Cybersecurity Operations

Analyst対応資料 □ ➤ www.goshiken.com □を開き、□ CCOA □を入力して、無料でダウンロードしてくださいCCOA資格問題対応

- 素敵なCCOA入門知識一回合格-信頼的なCCOA対応資料 □ サイト➤ www.mogiexam.com □で【 CCOA 】問題集をダウンロードCCOA対応内容
- 有難いCCOA入門知識試験-試験の準備方法-ハイパスレートのCCOA対応資料 ✇ “CCOA”を無料でダウンロード□ www.goshiken.com □ウェブサイトを入力するだけCCOA受験練習参考書
- CCOA受験対策書 □ CCOA試験情報 □ CCOA試験情報 □ URL 《 www.xhs1991.com 》をコピーして開き、▶CCOA◀を検索して無料でダウンロードしてくださいCCOA参考書勉強
- study.stcs.edu.np, stackblitz.com, gettr.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, lms.ait.edu.za, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes

無料でクラウドストレージから最新のPassTest CCOA PDFダンプをダウンロードする：https://drive.google.com/open?id=13Sjq7fgcZkUlyeEncBV8JHpAsvVrfTLo