Isaca.CCAK.vMay-2024.by.An.82q

Number: CCAK
Passing Score: 800
Time Limit: 120
File Version: 5.0

Exam Code: CCAK
Exam Name: Certificate of Cloud Auditing Knowledge

Exam A

QUESTION 1
Which of the following is a fundamental concept of FedRAMP that intends to save costs, time, and staff conducting superfluous agency security assessments?

A. Use often, provide many times
B. Be economical, act deliberately
C. Use existing, provide many times
D. Do once, use many times

Correct Answer: D
Section:
Explanation:
Reference: https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf (2)

QUESTION 2
In all three cloud deployment models, (IaaS, PaaS, and SaaS), who is responsible for the patching of the hypervisor layer?

A. Cloud service customer
B. Shared responsibility
C. Cloud service provider
D. Patching on hypervisor layer is not required

Correct Answer: A
Section:

QUESTION 3
In an organization, how are policy violations MOST likely to occur?

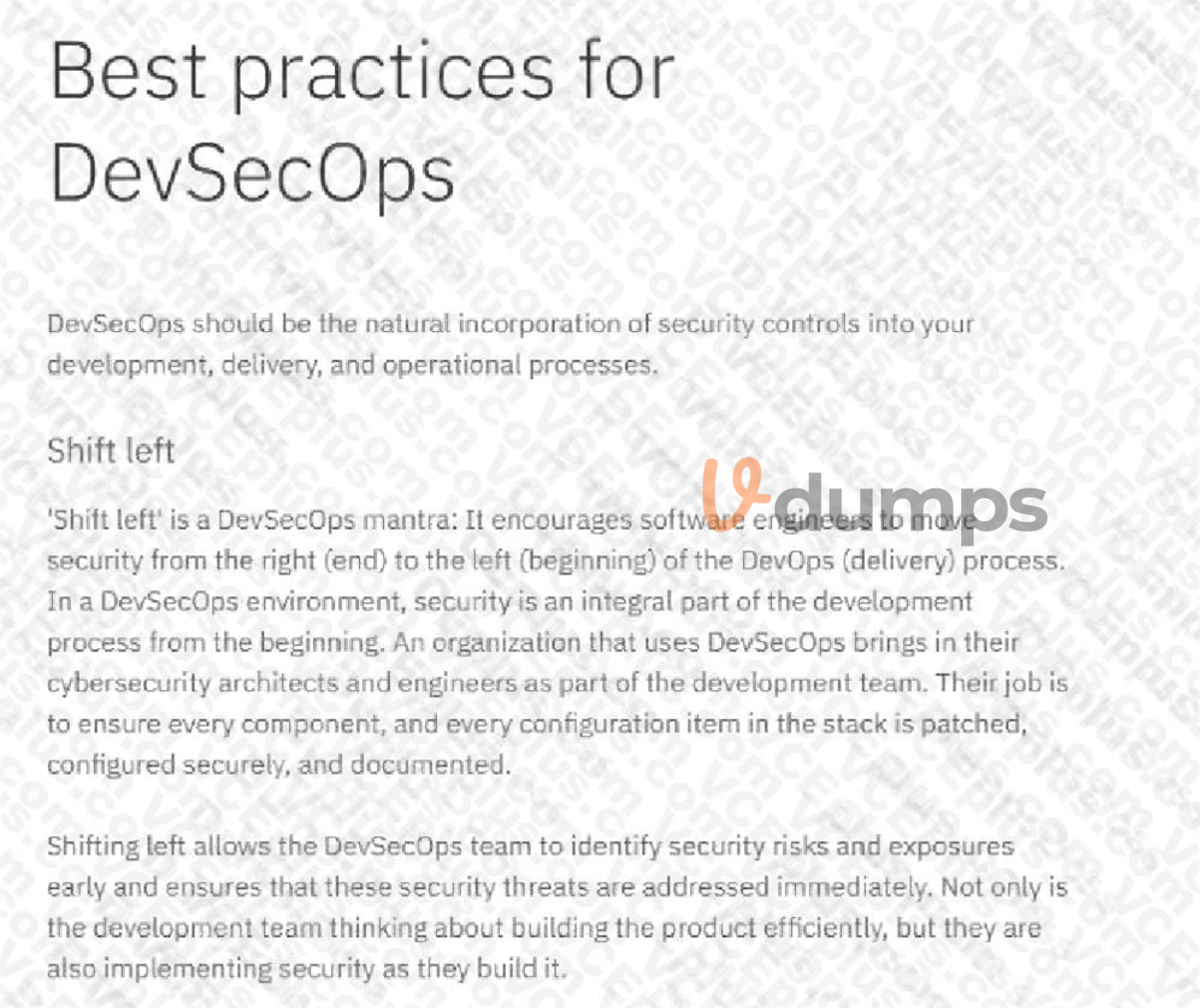
A. By accident
B. Deliberately by the ISP
C. Deliberately
D. Deliberately by the cloud provider

Correct Answer: A
Section:

QUESTION 4
What is a sign of an organization that has adopted a shift-left concept of code release cycles?

A. A waterfall model to move resources through the development to release phases
B. Incorporation of automation to identify and address software code problems early
C. Maturity of start-up entities with high-iteration to low-volume code commits
D. Large entities with slower release cadences and geographical dispersed systems

Correct Answer: B
Section:
Explanation:
Reference: https://www.ibm.com/cloud/learn/devsecops



Best practices for DevSecOps

DevSecOps should be the natural incorporation of security controls into your development, delivery, and operational processes.

Shift left

'Shift left' is a DevSecOps mantra: It encourages software engineers to move security from the right (end) to the left (beginning) of the DevOps (delivery) process. In a DevSecOps environment, security is an integral part of the development process from the beginning. An organization that uses DevSecOps brings in their cybersecurity architects and engineers as part of the development team. Their job is to ensure every component, and every configuration item in the stack is patched, configured securely, and documented.

Shifting left allows the DevSecOps team to identify security risks and exposures early and ensures that these security threats are addressed immediately. Not only is the development team thinking about building the product efficiently, but they are also implementing security as they build it.

QUESTION 5
An organization that is utilizing a community cloud is contracting an auditor to conduct a review on behalf of the group of organizations within the cloud community. From the following, to whom should the auditor report the

findings?

A. Public
B. Management of organization being audited
C. Shareholders/interested parties
D. Cloud service provider

Correct Answer: D
Section:

QUESTION 6
After finding a vulnerability in an internet-facing server of an organization, a cybersecurity criminal is able to access an encrypted file system and successfully manages to overwrite part of some files with random data. In reference to the Top Threats Analysis methodology, how would you categorize the technical impact of this incident?

A. As an integrity breach
B. As control breach
C. As an availability breach
D. As a confidentiality breach

Correct Answer: B
Section:

QUESTION 7
Which of the following configuration change controls is acceptable to a cloud auditor?

A. Development, test and production are hosted in the same network environment.
B. Programmers have permanent access to production software.
C. The Head of Development approves changes requested to production.
D. Programmers cannot make uncontrolled changes to the source code production version.

Correct Answer: D
Section:

QUESTION 8
Which best describes the difference between a type 1 and a type 2 SOC report?

A. A type 2 SOC report validates the operating effectiveness of controls whereas a type 1 SOC report validates the suitability of the design of the controls.
B. A type 2 SOC report validates the suitability of the design of the controls whereas a type 1 SOC report validates the operating effectiveness of controls.
C. A type 1 SOC report provides an attestation whereas a type 2 SOC report offers a certification.
D. There is no difference between a type 2 and type 1 SOC report.

Correct Answer: C
Section:
Explanation:
Reference: https://www.accountingtools.com/articles/2019/8/30/the-difference-between-soc-type-1-and-type-2-reports

QUESTION 9

To ensure that cloud audit resources deliver the best value to the organization, the PRIMARY step would be to:

A. develop a cloud audit plan on the basis of a detailed risk assessment.
B. schedule the audits and monitor the time spent on each audit.
C. train the cloud audit staff on current technology used in the organization.
D. monitor progress of audits and initiate cost control measures.

Correct Answer: A
Section:
Explanation:
It delivers value to the organization are the resources and efforts being dedicated to, and focused on, the higher-risk areas.

QUESTION 10
The BEST way to deliver continuous compliance in a cloud environment is to:

A. decrease the interval between attestations of compliance.
B. combine point-in-time assurance approaches with continuous monitoring.
C. increase the frequency of external audits from annual to quarterly.
D. combine point-in-time assurance approaches with continuous auditing.

Correct Answer: B
Section:

QUESTION 11
Which of the following is an example of integrity technical impact?

A. The cloud provider reports a breach of customer personal data from an unsecured server.
B. A hacker using a stolen administrator identity alerts the discount percentage in the product database.
C. A DDoS attack renders the customer's cloud inaccessible for 24 hours.
D. An administrator inadvertently clicked on Phish bait exposing his company to a ransomware attack.

Correct Answer: D
Section:
Explanation:
Reference: https://www.kroll.com/en/insights/publications/technology-impact-on-integrity-and-business-practices

QUESTION 12
Which of the following would be the GREATEST governance challenge to an organization where production is hosted in a public cloud and backups are held on the premises?

A. Aligning the cloud service delivery with the organization's objective
B. Aligning the cloud provider's SLA with the organization's policy
C. Aligning shared responsibilities between provider and customer
D. Aligning the organization's activity with the cloud provider's policy

Correct Answer: A
Section:
Explanation:

Reference: https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf

QUESTION 13
Which of the following BEST ensures adequate restriction on the number of people who can access the pipeline production environment?

A. Ensuring segregation of duties in the production and development pipelines.
B. Role-based access controls in the production and development pipelines.
C. Separation of production and development pipelines.
D. Periodic review of the CI/CD pipeline audit logs to identify any access violations.

Correct Answer: C
Section:
Explanation:
Reference: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2016/volume-2/journal-volume-2-2016

QUESTION 14
Which of the following metrics are frequently immature?

A. Metrics around Infrastructure as a Service (IaaS) storage and network environments
B. Metrics around Platform as a Service (PaaS) development environments
C. Metrics around Infrastructure as a Service (IaaS) computing environments
D. Metrics around specific Software as a Service (SaaS) application services

Correct Answer: A
Section:

QUESTION 15
Which of the following should be the FIRST step to establish a cloud assurance program during a cloud migration?

A. Design
B. Stakeholder identification
C. Development
D. Risk assessment

Correct Answer: C
Section:

QUESTION 16
From the perspective of a senior cloud security audit practitioner in an organization of a mature security program with cloud adoption, which of the following statements BEST describes the DevSecOps concept?

A. Process of security integration using automation in software development
B. Development standards for addressing integration, testing, and deployment issues
C. Operational framework that promotes software consistency through automation
D. Making software development simpler, faster, and easier using automation

Correct Answer: B
Section:

Explanation:
Reference: https://www.synopsys.com/blogs/software-security/devsecops-challenges-benefits/

QUESTION 17
The Open Certification Framework is structured on three levels of trust. Those three levels of trust are:

A. CSA STAR Self-Assessment, STAR Certification & Attestation (Third-party Assessment), STAR Compliance

B. CSA STAR Audit, STAR Certification & Attestation (Third-party Assessment), STAR Continuous

C. CSA STAR Self-Assessment, STAR Certification & Attestation (Third-party Assessment), STAR Monitoring and Control

D. CSA STAR Self-Assessment, STAR Certification & Attestation (Third-party Assessment), STAR Continuous

Correct Answer: D
Section:
Explanation:
Reference: https://www.cloudwatchhub.eu/cloud-security-alliance-open-certification-framework

QUESTION 18
Due to cloud audit team resource constraints, an audit plan as initially approved cannot be completed. Assuming that the situation is communicated in the cloud audit report, which course of action is MOST relevant?

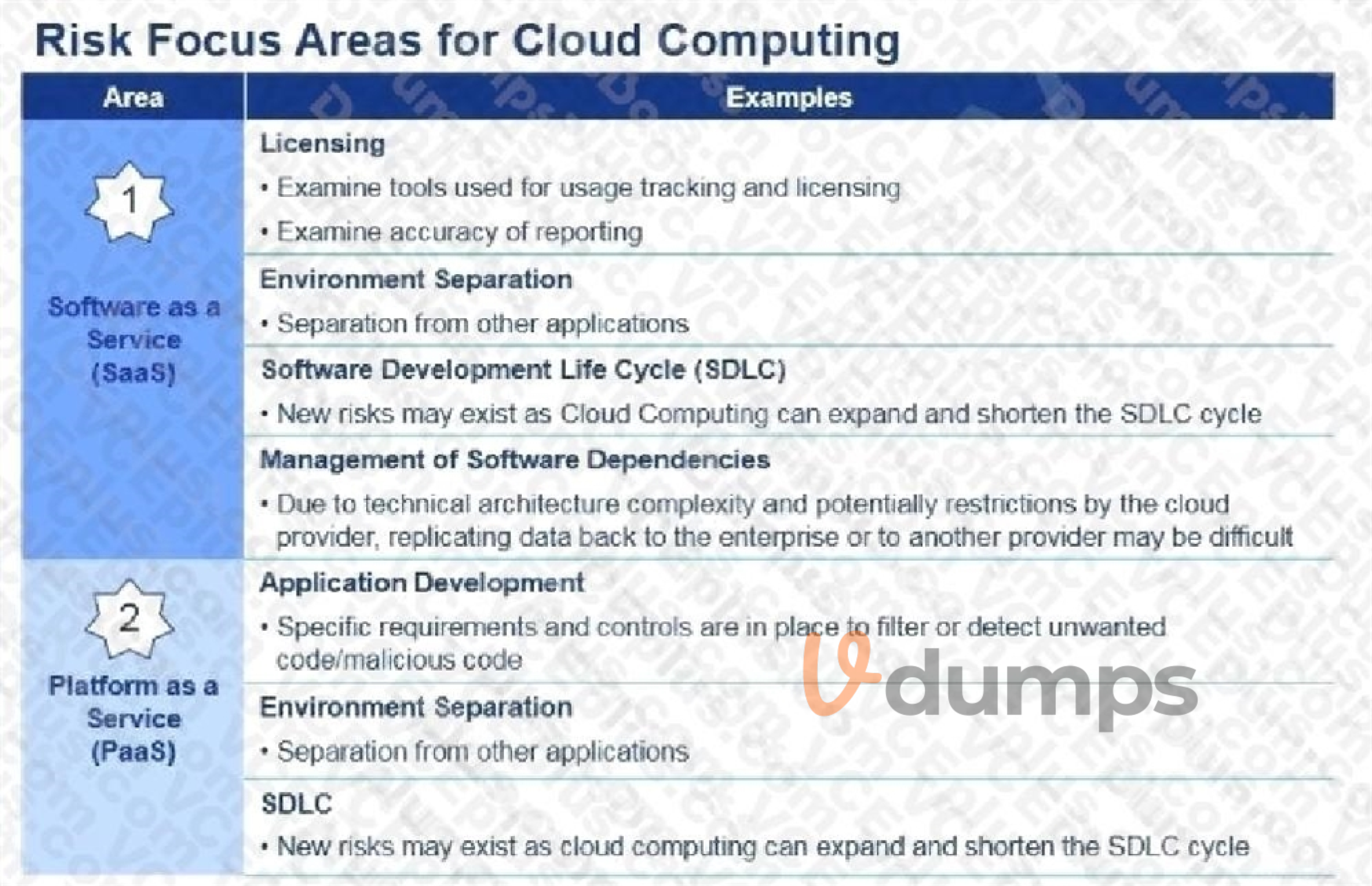
A. Focusing on auditing high-risk areas

B. Testing the adequacy of cloud controls design

C. Relying on management testing of cloud controls

D. Testing the operational effectiveness of cloud controls

Correct Answer: A
Section:
Explanation:
Reference: https://www.ucop.edu/ethics-compliance-audit-services/_files/webinars/10-14-16-cloudcomputing/cloudcomputing.pdf (31)



Risk Focus Areas for Cloud Computing

Area	Examples
1 Software as a Service (SaaS)	**Licensing** • Examine tools used for usage tracking and licensing • Examine accuracy of reporting
	Environment Separation • Separation from other applications
	Software Development Life Cycle (SDLC) • New risks may exist as Cloud Computing can expand and shorten the SDLC cycle
	Management of Software Dependencies • Due to technical architecture complexity and potentially restrictions by the cloud provider, replicating data back to the enterprise or to another provider may be difficult
2 Platform as a Service (PaaS)	**Application Development** • Specific requirements and controls are in place to filter or detect unwanted code/malicious code
	Environment Separation • Separation from other applications
	SDLC • New risks may exist as cloud computing can expand and shorten the SDLC cycle

QUESTION 19
Which of the following is a corrective control that may be identified in a SaaS service provider?

A. Log monitoring
B. Penetration testing
C. Incident response plans
D. Vulnerability scan

Correct Answer: D
Section:

QUESTION 20
The criteria for limiting services allowing non-critical services or services requiring high availability and resilience to be moved to the cloud is an important consideration to be included PRIMARILY in the:

A. risk management policy.

B. cloud policy.
C. business continuity plan.
D. information security standard for cloud technologies.

Correct Answer: C
Section:

QUESTION 21
When applying the Top Threats Analysis methodology following an incident, what is the scope of the technical impact identification step?

A. Determine the impact on the controls that were selected by the organization to respond to identified risks.
B. Determine the impact on confidentiality, integrity and availability of the information system.
C. Determine the impact on the financial, operational, compliance and reputation of the organization.
D. Determine the impact on the physical and environmental security of the organization, excluding informational assets.

Correct Answer: D
Section:

QUESTION 22
An organization deploying the Cloud Control Matrix (CCM) to perform a compliance assessment will encompass the use of the "Corporate Governance Relevance" feature to filter out those controls:

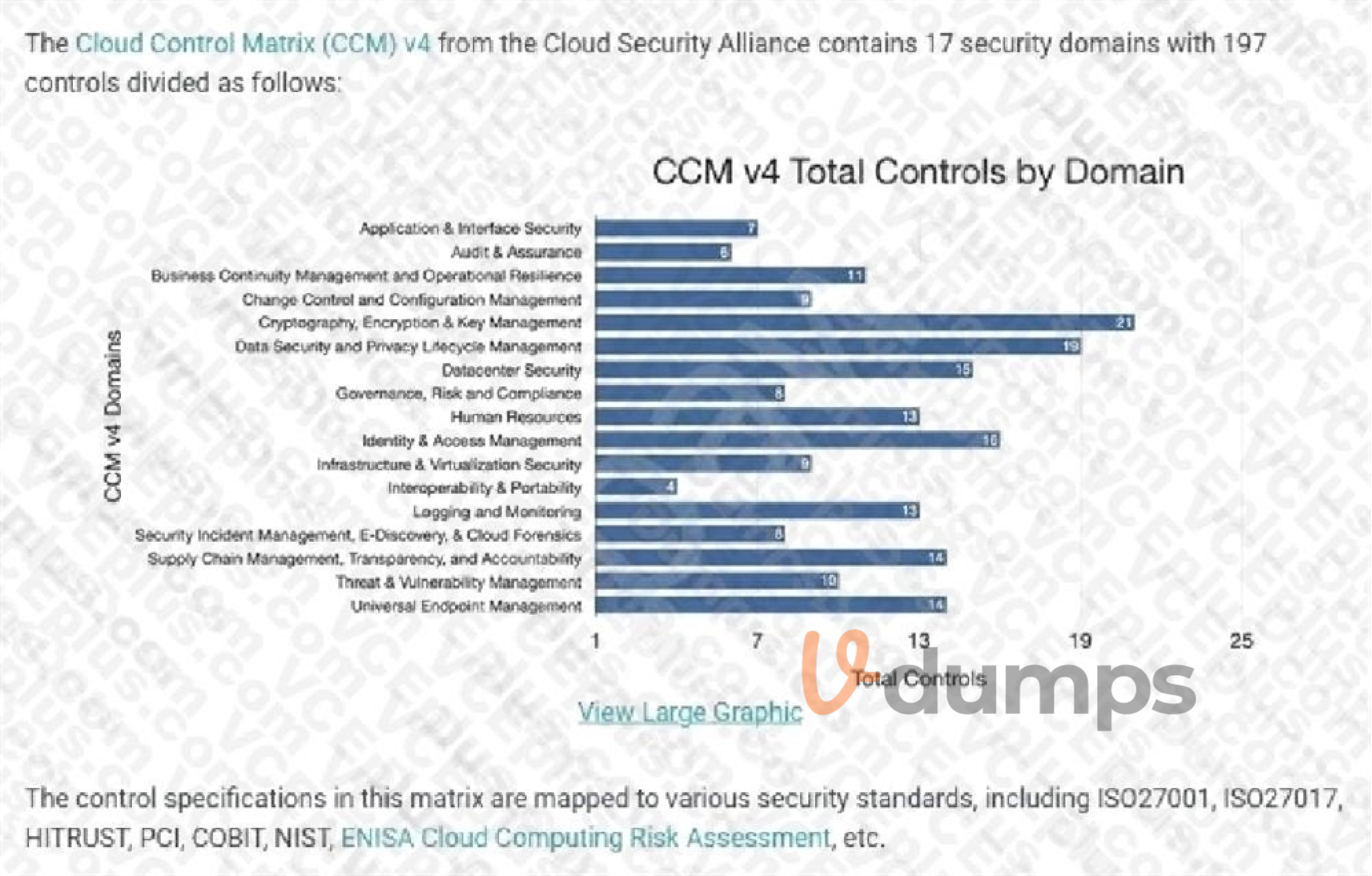
A. relating to policies, processes, laws, regulations, and institutions conditioning the way an organization is managed, directed, or controlled.
B. that can be either of a management or of a legal nature, therefore requiring an approval from the Change Advisory Board.
C. that require the prior approval from the Board of Directors to be funded (for either make or buy), implemented, and reported on.
D. that can be either of an administrative or of a technical nature, therefore requiring an approval from the Change Advisory Board.

Correct Answer: A
Section:

QUESTION 23
Which of the following is the BEST tool to perform cloud security control audits?

A. General Data Protection Regulation (GDPR)
B. ISO 27001
C. Federal Information Processing Standard (FIPS) 140-2
D. CSA Cloud Control Matrix (CCM)

Correct Answer: D
Section:
Explanation:
Reference: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-22/preventing-the-nextcybersecurity-attack-with-effective-cloud-security-audits



The Cloud Control Matrix (CCM) v4 from the Cloud Security Alliance contains 17 security domains with 197 controls divided as follows:

CCM v4 Total Controls by Domain
CCM v4 Domains
Application & Interface Security 7
Audit & Assurance 6
Business Continuity Management and Operational Resilience 11
Change Control and Configuration Management 9
Cryptography, Encryption & Key Management 21
Data Security and Privacy Lifecycle Management 19
Datacenter Security 15
Governance, Risk and Compliance 8
Human Resources 13
Identity & Access Management 16
Infrastructure & Virtualization Security 9
Interoperability & Portability 4
Logging and Monitoring 13
Security Incident Management, E-Discovery, & Cloud Forensics 8
Supply Chain Management, Transparency, and Accountability 14
Threat & Vulnerability Management 10
Universal Endpoint Management 14
1
7
13
19
25
Total Controls
View Large Graphic

The control specifications in this matrix are mapped to various security standards, including ISO27001, ISO27017, HITRUST, PCI, COBIT, NIST, ENISA Cloud Computing Risk Assessment, etc.

QUESTION 24
Which of the following is an example of a corrective control?

A. A central anti-virus system installing the latest signature files before allowing a connection to the network
B. Unsuccessful access attempts being automatically logged for investigation
C. Privileged access to critical information systems requiring a second factor of authentication using soft token
D. All new employees having standard access rights until their manager approves privileged rights

Correct Answer: C
Section:

QUESTION 25
When developing a cloud compliance program, what is the PRIMARY reason for a cloud customer to review which cloud services will be deployed?

A. To determine how those services will fit within its policies and procedures

B. To determine the total cost of the cloud services to be deployed
C. To confirm which vendor will be selected based on the compliance with security requirements
D. To confirm if the compensating controls implemented are sufficient for the cloud

Correct Answer: A
Section:
Explanation:
Reference: https://www.isaca.org/credentialing/certificate-of-cloud-auditing-knowledge

QUESTION 26
The Cloud Computing Compliance Controls Catalogue (C5) framework is maintained by which of the following agencies?

A. Agence nationale de la sécurité des systèmes d'information (ANSSI)
B. National Institute of Standards and Technology (NIST)
C. National Security Agency (NSA)
D. Bundesamt für Sicherheit in der Informationstechnik (BSI)

Correct Answer: D
Section:
Explanation:
Reference: https://docs.microsoft.com/en-us/compliance/regulatory/offering-c5-germany

QUESTION 27
Which of the following is the MOST feasible way to validate the performance of CSPs for the delivery of technology resources?

A. Cloud compliance program
B. Legacy IT compliance program
C. Internal audit program
D. Service organization controls report

Correct Answer: D
Section:

QUESTION 28
Which of the following would be the MOST critical finding of an application security and DevOps audit?

A. The organization is not using a unified framework to integrate cloud compliance with regulatory requirements.
B. Application architecture and configurations did not consider security measures.
C. Outsourced cloud service interruption, breach or loss of data stored at the cloud service provider.
D. Certifications with global security standards specific to cloud are not reviewed and the impact of noted findings are not assessed.

Correct Answer: B
Section:

QUESTION 29
During an audit it was identified that a critical application hosted in an off-premises cloud is not part of the organization's DRP (Disaster Recovery Plan).
Management stated that it is responsible for ensuring that the cloud service provider (CSP) has a plan that is tested annually. What should be the auditor's NEXT course of action?

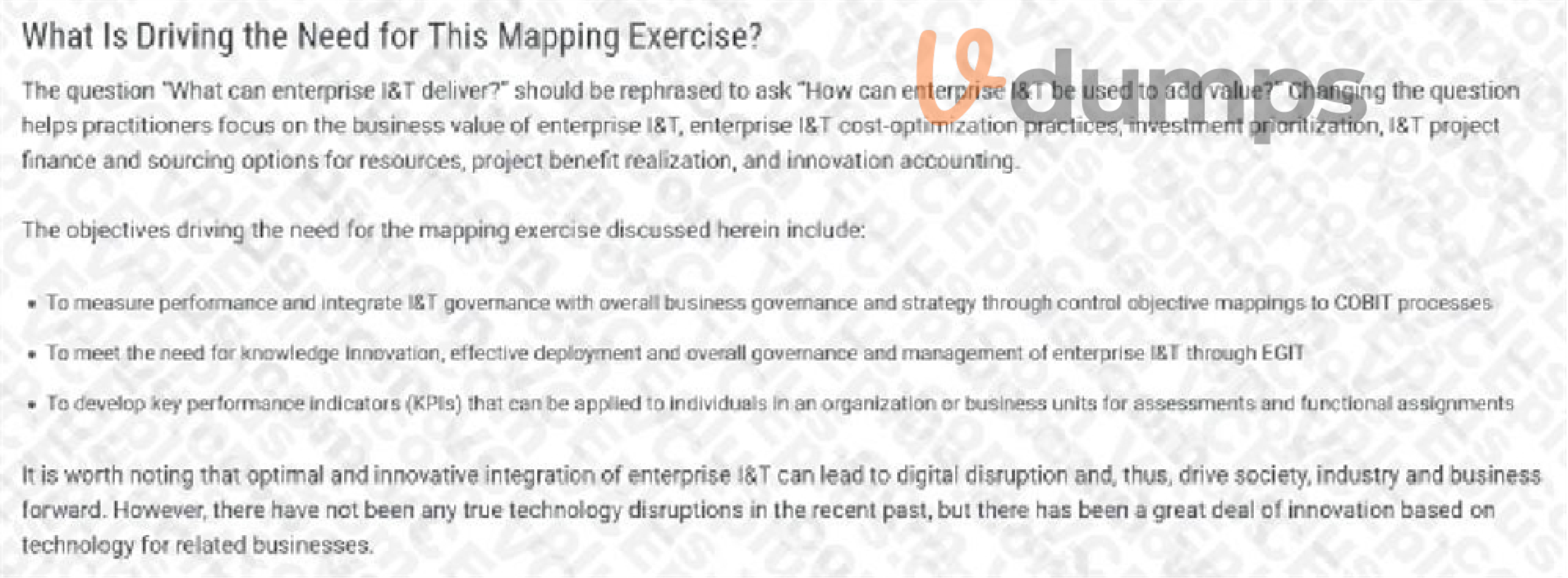
A. Review the CSP audit reports.
B. Review the security white paper of the CSP.
C. Review the contract and DR capability.
D. Plan an audit of the CSP.

Correct Answer: B
Section:

QUESTION 30
Organizations maintain mappings between the different control frameworks they adopt to:

A. help identify controls with common assessment status.
B. avoid duplication of work when assessing compliance.
C. help identify controls with different assessment status.
D. start a compliance assessment using latest assessment.

Correct Answer: C
Section:
Explanation:
Reference: https://www.isaca.org/resources/news-and-trends/industry-news/2019/employing-cobit-2019-for-enterprisegovernance-strategy



What Is Driving the Need for This Mapping Exercise?

The question "What can enterprise I&T deliver?" should be rephrased to ask "How can enterprise I&T be used to add value?" Changing the question helps practitioners focus on the business value of enterprise I&T, enterprise I&T cost-optimization practices, investment prioritization, I&T project finance and sourcing options for resources, project benefit realization, and innovation accounting.

The objectives driving the need for the mapping exercise discussed herein include:

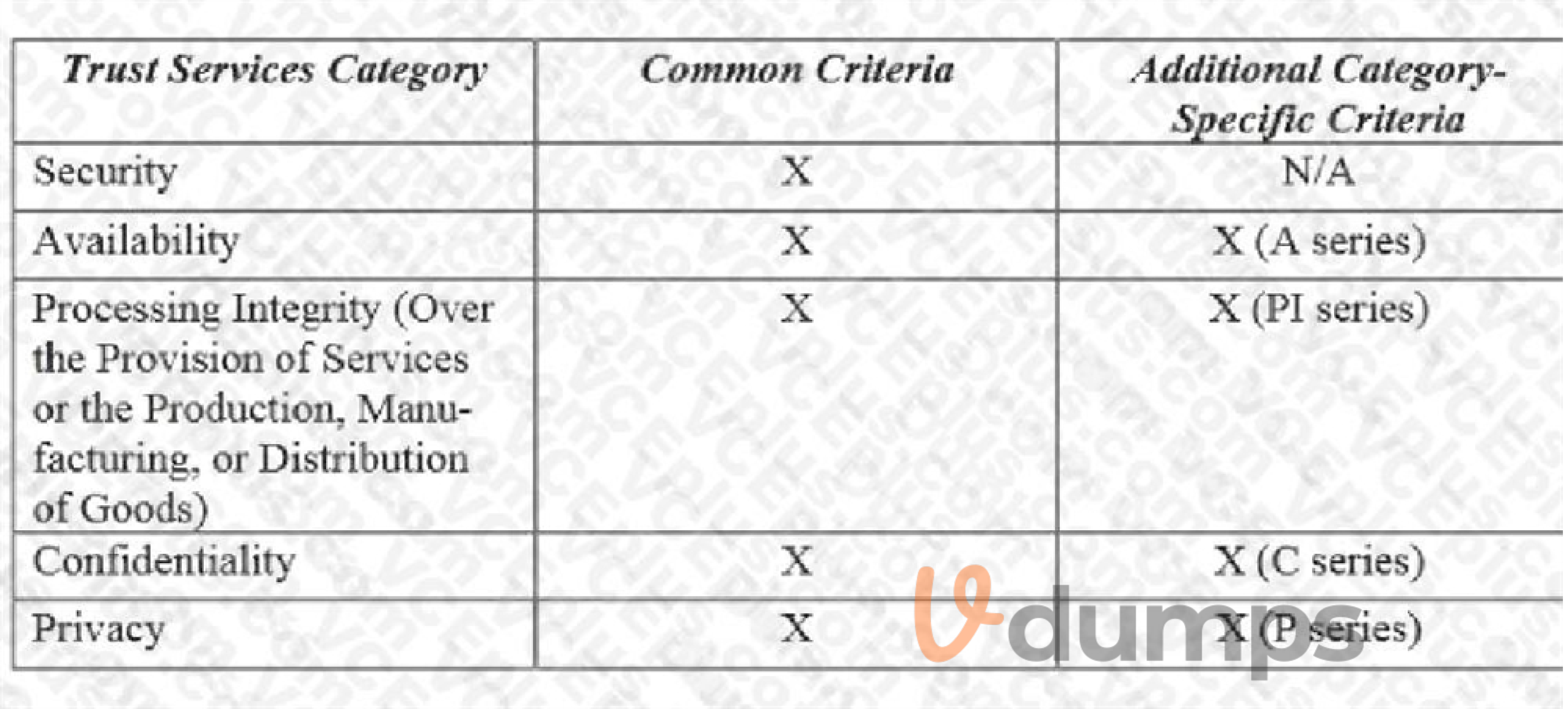
- To measure performance and integrate I&T governance with overall business governance and strategy through control objective mappings to COBIT processes
- To meet the need for knowledge innovation, effective deployment and overall governance and management of enterprise I&T through EGIT
- To develop key performance indicators (KPIs) that can be applied to individuals in an organization or business units for assessments and functional assignments

It is worth noting that optimal and innovative integration of enterprise I&T can lead to digital disruption and, thus, drive society, industry and business forward. However, there have not been any true technology disruptions in the recent past, but there has been a great deal of innovation based on technology for related businesses.

QUESTION 31
Which of the following defines the criteria designed by the American Institute of Certified Public Accountants (AICPA) to specify trusted services?

A. Security, confidentiality, availability, privacy and processing integrity
B. Security, applicability, availability, privacy and processing integrity
C. Security, confidentiality, availability, privacy and trustworthiness
D. Security, data integrity, availability, privacy and processing integrity

Correct Answer: A
Section:
Explanation:
Reference:
https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-servicescriteria.pdf



Trust Services Category	*Common Criteria*	*Additional Category-Specific Criteria*
Security	X	N/A
Availability	X	X (A series)
Processing Integrity (Over the Provision of Services or the Production, Manufacturing, or Distribution of Goods)	X	X (PI series)
Confidentiality	X	X (C series)
Privacy	X	X (P series)

QUESTION 32
While performing the audit, the auditor found that an object storage bucket containing PII could be accessed by anyone on the Internet. Given this discovery, what should be the most appropriate action for the auditor to perform?

A. Highlighting the gap to the audit sponsor at the sponsor's earliest possible availability
B. Asking the organization's cloud administrator to immediately close the gap by updating the configuration settings and making the object storage bucket private and hence inaccessible from the Internet
C. Documenting the finding in the audit report and sharing the gap with the relevant stakeholders
D. Informing the organization's internal audit manager immediately about the gap

Correct Answer: C
Section:
Explanation:
Reference: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-1/is-audit-basics-the-components-of-the-itaudit-report

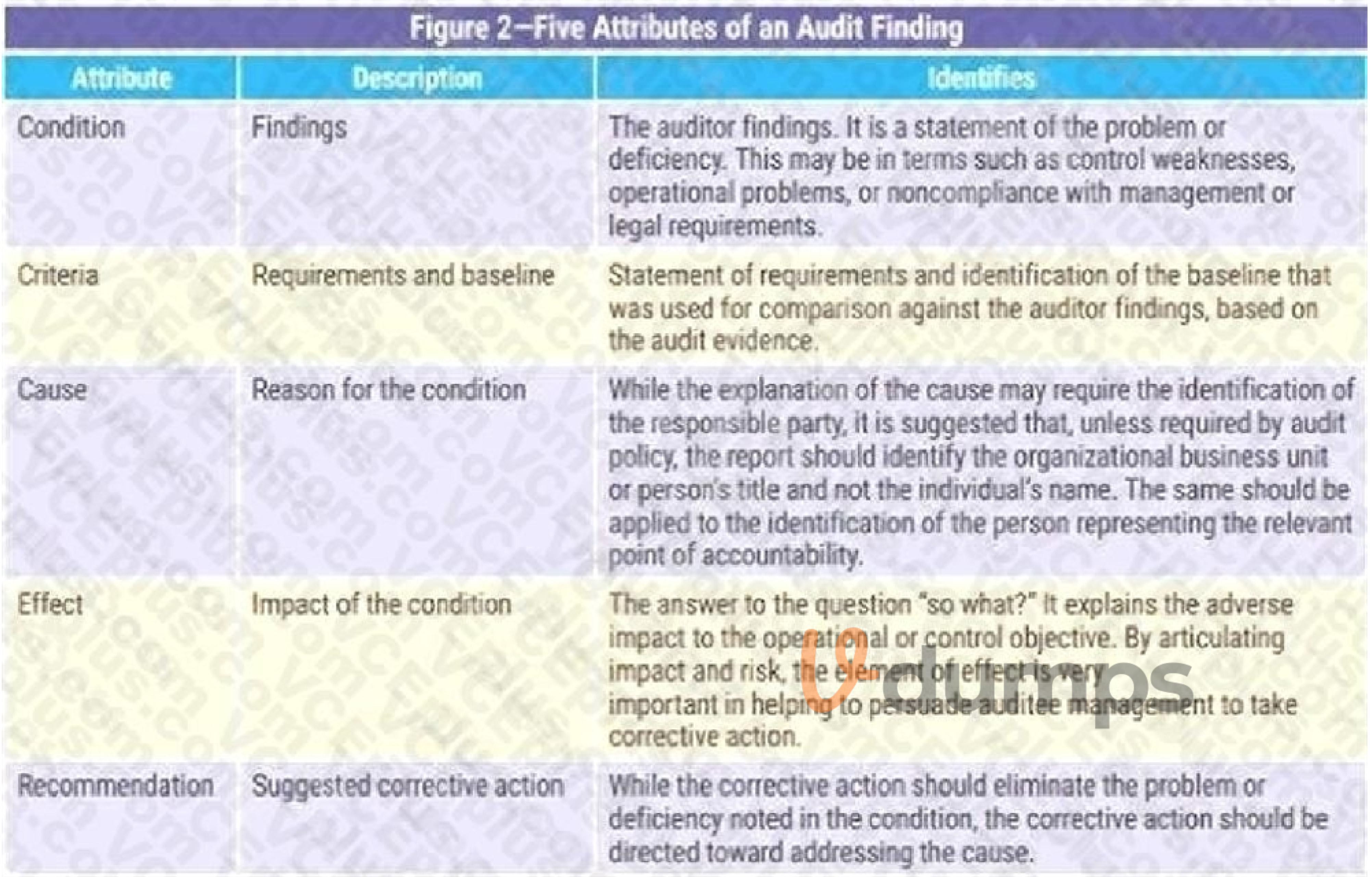


Figure 2—Five Attributes of an Audit Finding

Attribute	Description	Identifies
Condition	Findings	The auditor findings. It is a statement of the problem or deficiency. This may be in terms such as control weaknesses, operational problems, or noncompliance with management or legal requirements.
Criteria	Requirements and baseline	Statement of requirements and identification of the baseline that was used for comparison against the auditor findings, based on the audit evidence.
Cause	Reason for the condition	While the explanation of the cause may require the identification of the responsible party, it is suggested that, unless required by audit policy, the report should identify the organizational business unit or person's title and not the individual's name. The same should be applied to the identification of the person representing the relevant point of accountability.
Effect	Impact of the condition	The answer to the question "so what?" It explains the adverse impact to the operational or control objective. By articulating impact and risk, the element of effect is very important in helping to persuade auditee management to take corrective action.
Recommendation	Suggested corrective action	While the corrective action should eliminate the problem or deficiency noted in the condition, the corrective action should be directed toward addressing the cause.

QUESTION 33

Which of the following is the common cause of misconfiguration in a cloud environment?

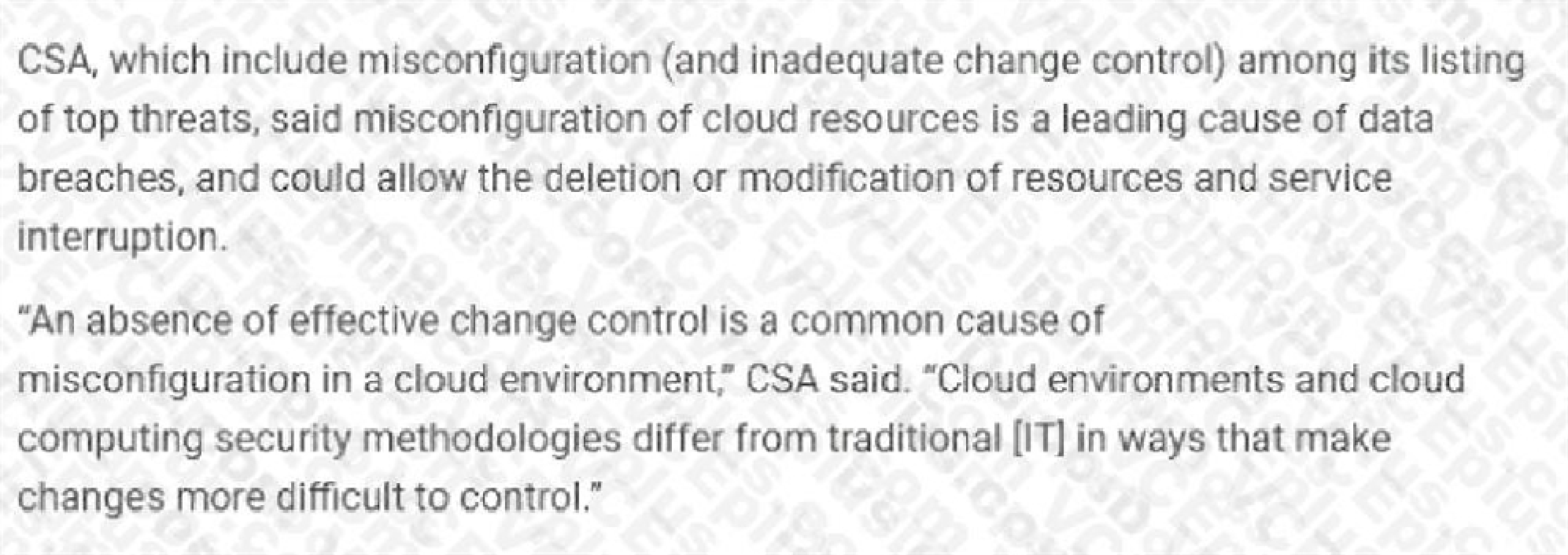
A. Absence of effective change control

B. Using multiple cloud service providers

C. New cloud computing techniques

D. Traditional change process mechanisms

Correct Answer: A
Section:
Explanation:
Reference: https://businessinsights.bitdefender.com/the-top-5-cloud-threats-that-smbs-need-to-address



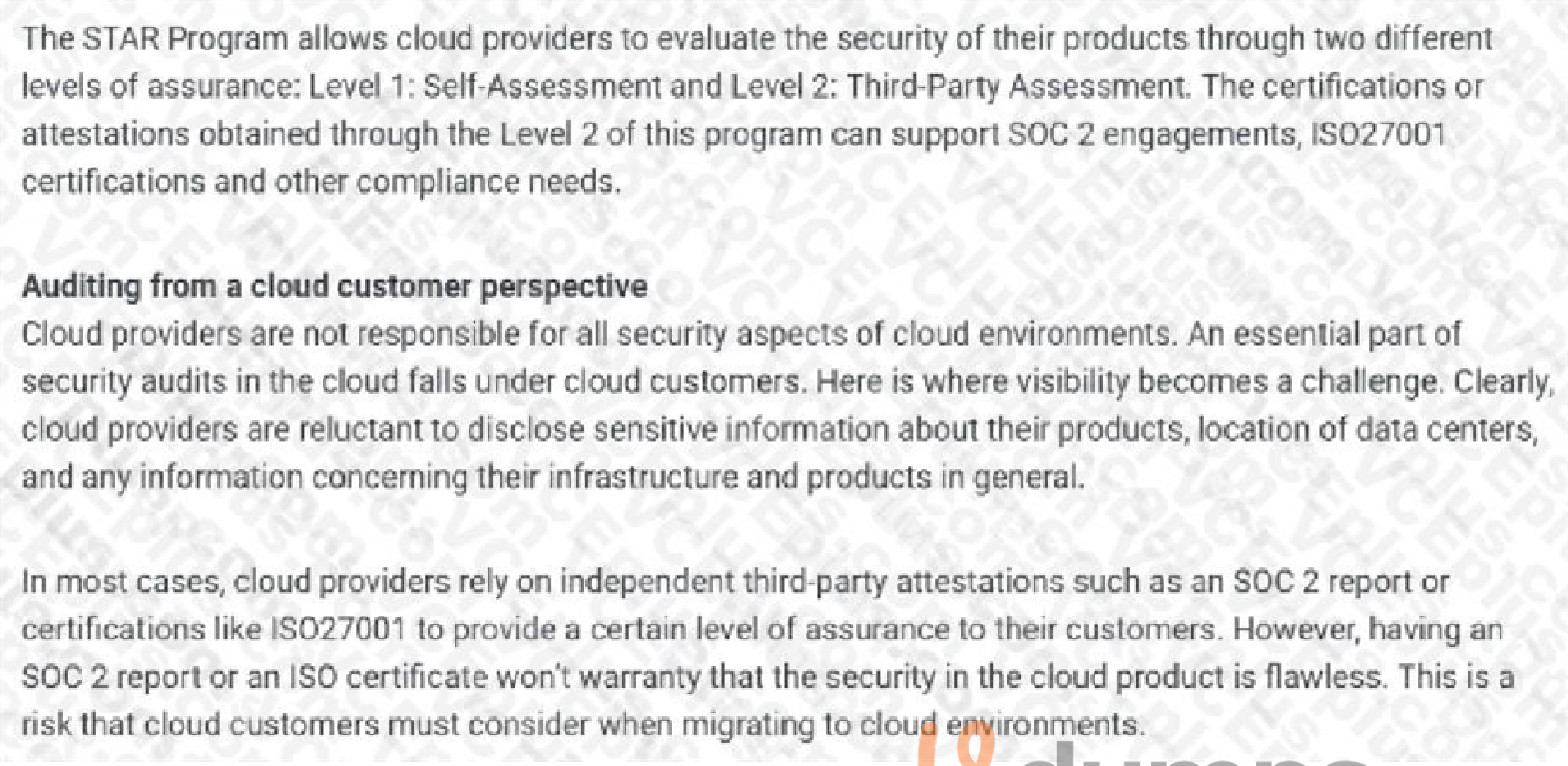
CSA, which include misconfiguration (and inadequate change control) among its listing of top threats, said misconfiguration of cloud resources is a leading cause of data breaches, and could allow the deletion or modification of resources and service interruption.

"An absence of effective change control is a common cause of misconfiguration in a cloud environment," CSA said. "Cloud environments and cloud computing security methodologies differ from traditional [IT] in ways that make changes more difficult to control."

QUESTION 34
Which of the following controls framework should the cloud customer use to assess the overall security risk of a cloud provider?

A. SOC3 - Type2
B. Cloud Control Matrix (CCM)
C. SOC2 - Type1
D. SOC1 - Type1

Correct Answer: C
Section:
Explanation:
Reference: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-22/preventing-the-nextcybersecurity-attack-with-effective-cloud-security-audits



The STAR Program allows cloud providers to evaluate the security of their products through two different levels of assurance: Level 1: Self-Assessment and Level 2: Third-Party Assessment. The certifications or attestations obtained through the Level 2 of this program can support SOC 2 engagements, ISO27001 certifications and other compliance needs.

Auditing from a cloud customer perspective

Cloud providers are not responsible for all security aspects of cloud environments. An essential part of security audits in the cloud falls under cloud customers. Here is where visibility becomes a challenge. Clearly, cloud providers are reluctant to disclose sensitive information about their products, location of data centers, and any information concerning their infrastructure and products in general.

In most cases, cloud providers rely on independent third-party attestations such as an SOC 2 report or certifications like ISO27001 to provide a certain level of assurance to their customers. However, having an SOC 2 report or an ISO certificate won't warranty that the security in the cloud product is flawless. This is a risk that cloud customers must consider when migrating to cloud environments.

QUESTION 35

The BEST method to report continuous assessment of a cloud provider's services to the CSA is through:

A. a set of dedicated application programming interfaces (APIs).

B. SOC 2 Type 2 attestation.

C. CCM assessment by a third-party auditor on a periodic basis.

D. tools selected by the third-party auditor.

Correct Answer: C
Section:
Explanation:
Reference: https://cloudsecurityalliance.org/press-releases/2019/03/04/csa-launches-star-continuous-complianceassessment-program-for-cloud-service-providers/

QUESTION 36

Which of the following is the MOST important audit scope document when conducting a review of a cloud service provider?

A. Updated audit/work program

B. Documentation criteria for the audit evidence

C. Processes and systems to be audited

D. Testing procedure to be performed

Correct Answer: B
Section:

QUESTION 37
Which of the following is a cloud-native solution designed to counter threats that do not exist within the enterprise?

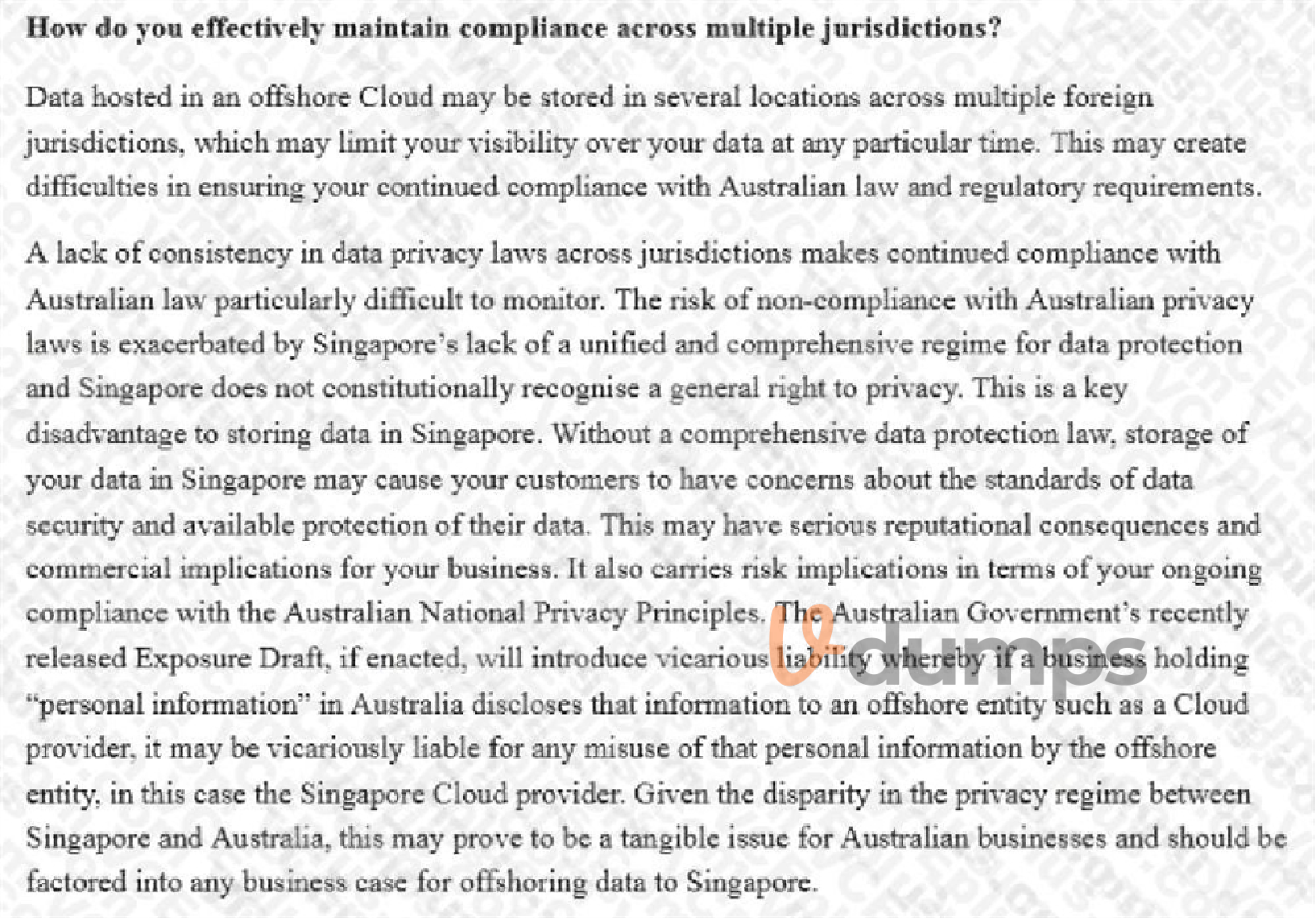
A. Policy based access control
B. Attribute based access control
C. Rule based access control
D. Role based access control

Correct Answer: C
Section:

QUESTION 38
Which of the following is the risk associated with storing data in a cloud that crosses jurisdictions?

A. Compliance risk
B. Provider administration risk
C. Audit risk
D. Virtualization risk

Correct Answer: A
Section:
Explanation:
Reference: http://webcache.googleusercontent.com/search?q=cache:9OK2cQSAR3oJ:www.aph.gov.au/DocumentStore.ashx%3Fid%3 D88403640-14b5-4c3e-8dd7-315bb5067ba4 +&cd=1&hl=en&ct=clnk&gl=pk



How do you effectively maintain compliance across multiple jurisdictions?

Data hosted in an offshore Cloud may be stored in several locations across multiple foreign jurisdictions, which may limit your visibility over your data at any particular time. This may create difficulties in ensuring your continued compliance with Australian law and regulatory requirements.

A lack of consistency in data privacy laws across jurisdictions makes continued compliance with Australian law particularly difficult to monitor. The risk of non-compliance with Australian privacy laws is exacerbated by Singapore's lack of a unified and comprehensive regime for data protection and Singapore does not constitutionally recognise a general right to privacy. This is a key disadvantage to storing data in Singapore. Without a comprehensive data protection law, storage of your data in Singapore may cause your customers to have concerns about the standards of data security and available protection of their data. This may have serious reputational consequences and commercial implications for your business. It also carries risk implications in terms of your ongoing compliance with the Australian National Privacy Principles. The Australian Government's recently released Exposure Draft, if enacted, will introduce vicarious liability whereby if a business holding "personal information" in Australia discloses that information to an offshore entity such as a Cloud provider, it may be vicariously liable for any misuse of that personal information by the offshore entity, in this case the Singapore Cloud provider. Given the disparity in the privacy regime between Singapore and Australia, this may prove to be a tangible issue for Australian businesses and should be factored into any business case for offshoring data to Singapore.

QUESTION 39

Prioritizing assurance activities for an organization's cloud services portfolio depends PRIMARILY on an organization's ability to:

A. schedule frequent reviews with high-risk cloud service providers.

B. develop plans using a standardized risk-based approach.

C. maintain a comprehensive cloud service inventory.

D. collate views from various business functions using cloud services.

Correct Answer: A

Section:

QUESTION 40

Which of the following has the MOST substantial impact on how aggressive or conservative the cloud approach of an organization will be?

A. Internal policies and technical standards

B. Risk scoring criteria

C. Applicable laws and regulations

D. Risk appetite and budget constraints

Correct Answer: C
Section:

QUESTION 41
Policies and procedures shall be established, and supporting business processes and technical measures implemented, for maintenance of several items ensuring continuity and availability of operations and support personnel. Which of the following controls BEST matches this control description?

A. Operations Maintenance

B. System Development Maintenance

C. Equipment Maintenance

D. System Maintenance

Correct Answer: A
Section:
Explanation:
Reference: https://www.sapidata.sm/img/cms/CAIQ_v3-1_2020-01-13.pdf (2)

QUESTION 42
The Cloud Octagon Model was developed to support organizations:

A. risk assessment methodology.

B. risk treatment methodology.

C. incident response methodology.

D. incident detection methodology.

Correct Answer: A
Section:

QUESTION 43
To ensure that integration of security testing is implemented on large code sets in environments where time to completion is critical, what form of validation should an auditor expect?

A. Parallel testing

B. Full application stack unit testing

C. Regression testing

D. Functional verification

Correct Answer: B
Section:
Explanation:
Reference: https://www.sciencedirect.com/topics/computer-science/black-box-testing

QUESTION 44
When performing audits in relation to Business Continuity Management and Operational Resilience strategy, what would be the MOST critical aspect to audit in relation to the strategy of the cloud customer that should be formulated jointly with the cloud service provider?

A. Validate if the strategy covers unavailability of all components required to operate the business-as-usual or in disrupted mode, in parts or total- when impacted by a disruption.

B. Validate if the strategy covers all aspects of Business Continuity and Resilience planning, taking inputs from the assessed impact and risks, to consider activities for before, during, and after a disruption.

C. Validate if the strategy covers all activities required to continue and recover prioritized activities within identified time frames and agreed capacity, aligned to the risk appetite of the organization including the invocation of continuity plans and crisis management capabilities.

D. Validate if the strategy is developed by both cloud service providers and cloud service consumers within the acceptable limits of their risk appetite.

Correct Answer: B
Section:

QUESTION 45
Which of the following standards is designed to be used by organizations for cloud services that intend to select controls within the process of implementing an Information Security Management System based on ISO/IEC 27001?

A. ISO/IEC 27017:2015

B. CSA Cloud Control Matrix (CCM)

C. NIST SP 800-146

D. ISO/IEC 27002

Correct Answer: D
Section:
Explanation:
Reference: https://cyber.gc.ca/en/guidance/guidance-cloud-security-assessment-and-authorization-itsp50105

QUESTION 46
Which of the following aspects of risk management involves identifying the potential reputational harm and/or financial harm when an incident occurs?

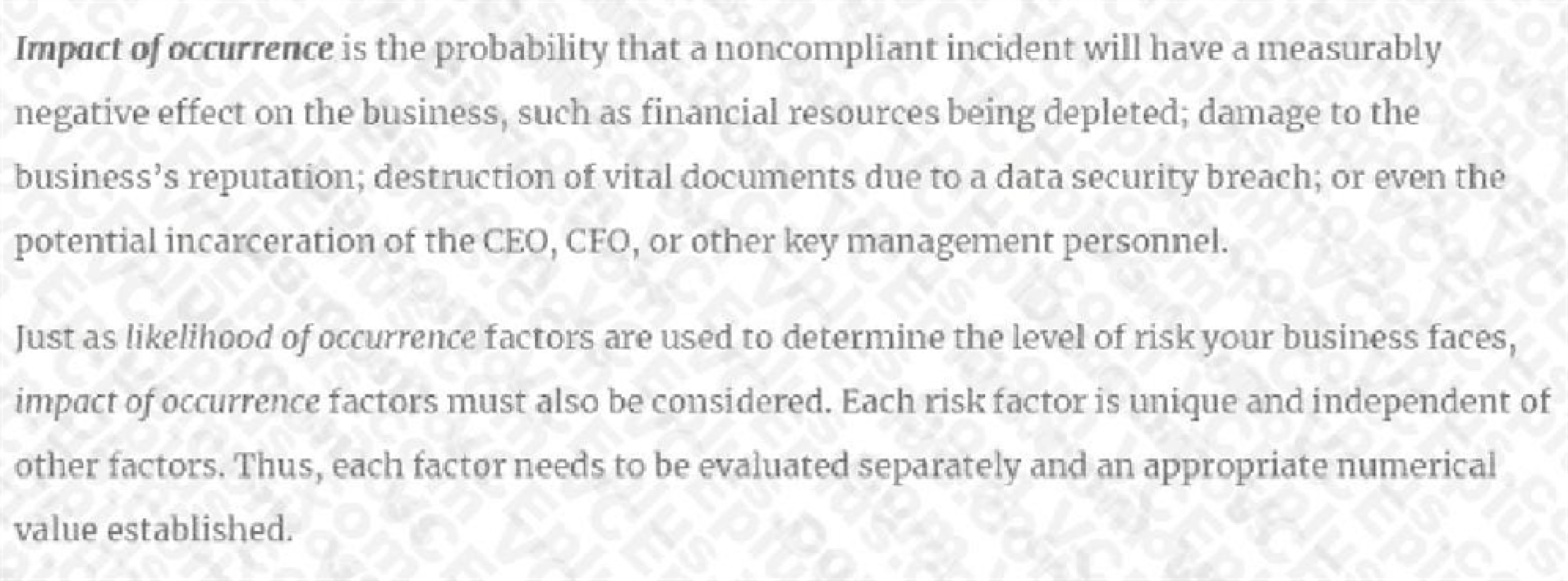
A. Mitigations

B. Residual risk

C. Likelihood

D. Impact Analysis

Correct Answer: D
Section:
Explanation:
Reference: https://compliancecosmos.org/chapter-5-step-three-determining-impact-occurrence



Impact of occurrence is the probability that a noncompliant incident will have a measurably negative effect on the business, such as financial resources being depleted; damage to the business's reputation; destruction of vital documents due to a data security breach; or even the potential incarceration of the CEO, CFO, or other key management personnel.

Just as *likelihood of occurrence* factors are used to determine the level of risk your business faces, *impact of occurrence* factors must also be considered. Each risk factor is unique and independent of other factors. Thus, each factor needs to be evaluated separately and an appropriate numerical value established.

QUESTION 47
You have been assigned the implementation of an ISMS, whose scope must cover both on premise and cloud infrastructure.
Which of the following is your BEST option?

A. Implement ISO/IEC 27002 and complement it with additional controls from the CCM.
B. Implement ISO/IEC 27001 and complement it with additional controls from ISO/IEC 27017.
C. Implement ISO/IEC 27001 and complement it with additional controls from ISO/IEC 27002.
D. Implement ISO/IEC 27001 and complement it with additional controls from the NIST SP 800-145.

Correct Answer: B
Section:

QUESTION 48
To identify key actors and requirements, which of the following MUST be considered when designing a cloud compliance program?

A. Cloud service provider, internal and external audit perspectives
B. Business/organizational, governance, cloud and risk perspectives
C. Enterprise risk management, data protection, privacy and legal perspectives
D. Key stakeholders, enterprise risk management, and Internal audit perspectives

Correct Answer: B
Section:

QUESTION 49
Which of the following data destruction methods is the MOST effective and efficient?

A. Crypto-shredding
B. Degaussing

C. Multi-pass wipes
D. Physical destruction

Correct Answer: B
Section:
Explanation:
Reference: https://man.fas.org/dod-101/sys/ship/weaps/degaussing.htm

QUESTION 50
Which of the following is MOST important to consider when developing an effective threat model during the introduction of a new SaaS service into a customer organization's architecture? The threat model:

A. recognizes the shared responsibility for risk management between the customer and the CSP.
B. leverages SaaS threat models developed by peer organizations.
C. is developed by an independent third-party with expertise in the organization's industry sector.
D. considers the loss of visibility and control from transitioning to the cloud.

Correct Answer: A
Section:

QUESTION 51
Your company is purchasing an application from a vendor. They do not allow you to perform an on-site audit on their information system. However, they say, they will provide the third-party audit attestation on the adequate control design within their environment. Which report is the vendor providing you?

A. SOC 3
B. SOC 2, TYPE 2
C. SOC 1
D. SOC 2, TYPE 1

Correct Answer: B
Section:
Explanation:
Reference: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-6/soc-reports-for-cloud-security-and-privacy

QUESTION 52
When establishing cloud governance, an organization should FIRST test by migrating:

A. all applications at once to the cloud.
B. complex applications to the cloud.
C. legacy applications to the cloud.
D. a few applications to the cloud.

Correct Answer: D
Section:

QUESTION 53
When building a cloud governance model, which of the following requirements will focus more on the cloud service provider's evaluation and control checklist?

A. Security requirements
B. Legal requirements
C. Compliance requirements
D. Operational requirements

Correct Answer: D
Section:

QUESTION 54
Which of the following would be considered as a factor to trust in a cloud service provider?

A. The level of exposure for public information
B. The level of proved technical skills
C. The level of willingness to cooperate
D. The level of open source evidence available

Correct Answer: C
Section:

QUESTION 55
A certification target helps in the formation of a continuous certification framework by incorporating:

A. CSA STAR level 2 attestation.
B. service level objective and service qualitative objective.
C. frequency of evaluating security attributes.
D. scope description and security attributes to be tested.

Correct Answer: B
Section:

QUESTION 56
Since CCM allows cloud customers to build a detailed list of requirements and controls to be implemented by the CSP as part of their overall third-party risk management and procurement program, will CCM alone be enough to define all the items to be considered when operating/using cloud services?

A. No. CCM must be completed with definitions established by the CSP because of its relevance to service continuity.
B. Yes. CCM suffices since it maps a huge library of widely accepted frameworks.
C. Yes. When implemented in the right manner, CCM alone can help to measure, assess and monitor the risk associated with a CSP or a particular service.
D. No. CCM can serve as a foundation for a cloud assessment program, but it needs to be completed with requirements applicable to each company.

Correct Answer: C
Section:

QUESTION 57
Which of the following cloud models prohibits penetration testing?

A. Hybrid Cloud
B. Private Cloud

C. Public Cloud

D. Community Cloud

Correct Answer: B
Section:
Explanation:
Reference: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf

QUESTION 58
Which statement about compliance responsibilities and ownership of accountability is correct?

A. Organizations may be able to transfer their accountability for compliance with various regulatory requirements to their CSPs, but they retain the ownership of responsibility.

B. Organizations may be able to transfer their responsibility for compliance with various regulatory requirements to their CSPs, but they retain the ownership of accountability.

C. Organizations may transfer their responsibility and accountability for compliance with various regulatory requirements to their CSPs.

D. Organizations are not able to transfer their responsibility nor accountability for compliance with various regulatory requirements to their CSPs.

Correct Answer: D
Section:
Explanation:
Reference: https://searchcloudsecurity.techtarget.com/tip/Top-cloud-security-challenges-and-how-to-combat-them

QUESTION 59
Which of the following attestation allows for immediate adoption of the Cloud Control Matrix (CCM) as additional criteria to AICPA Trust Service Criteria and provides the flexibility to update the criteria as technology and market requirements change?

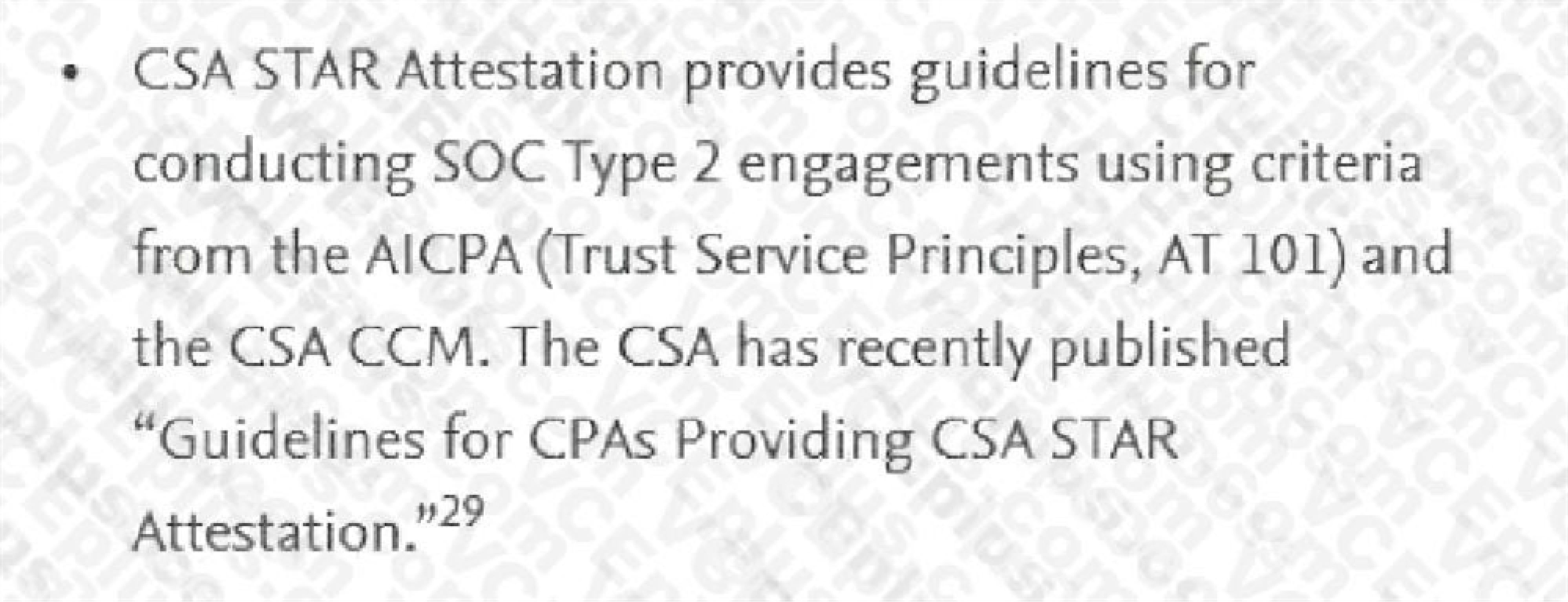
A. PC-IDSS

B. CSA STAR Attestation

C. MTCS

D. BSI Criteria Catalogue C5

Correct Answer: B
Section:
Explanation:
Reference: https://www.sciencedirect.com/topics/computer-science/cloud-controls-matrix



- CSA STAR Attestation provides guidelines for conducting SOC Type 2 engagements using criteria from the AICPA (Trust Service Principles, AT 101) and the CSA CCM. The CSA has recently published "Guidelines for CPAs Providing CSA STAR Attestation."[29]

QUESTION 60
Which of the following approaches encompasses social engineering of staff, bypassing of physical access controls and penetration testing?

A. Blue team
B. White box
C. Gray box
D. Red team

Correct Answer: B
Section:
Explanation:
Reference: https://www.isaca.org/resources/isaca-journal/issues/2016/volume-5/planning-for-information-security-testingapractical-approach

QUESTION 61
Which of the following is MOST important to consider when an organization is building a compliance program for the cloud?

A. The rapidly changing service portfolio and architecture of the cloud.
B. Cloud providers should not be part of the compliance program.
C. The fairly static nature of the service portfolio and architecture of the cloud.
D. The cloud is similar to the on-premise environment in terms of compliance.

Correct Answer: A
Section:

QUESTION 62
A CSP providing cloud services currently being used by the United States federal government should obtain which of the following to assure compliance to stringent government standards?

A. Multi-Tier Cloud Security (MTCS) Attestation

B. FedRAMP Authorization
C. ISO/IEC 27001:2013 Certification
D. CSA STAR Level Certificate

Correct Answer: B
Section:
Explanation:
Reference: https://www.ftptoday.com/blog/benefits-using-fedramp-authorized-cloud-service-provider

QUESTION 63
To qualify for CSA STAR attestation for a particular cloud system, the SOC 2 report must cover:

A. ISO/I?? 27001: 2013 controls.
B. maturity model criteria.
C. all Cloud Control Matrix (CCM) controls and TSPC security principles.
D. Cloud Control Matrix (CCM) and ISO/IEC 27001:2013 controls.

Correct Answer: C
Section:
Explanation:
Reference: https://downloads.cloudsecurityalliance.org/star/attestation/GuidelinesforCPAsv2.pdf (8)

QUESTION 64
When a client's business process changes, the CSP SLA should:

A. be reviewed, but the SLA cannot be updated.
B. not be reviewed, but the cloud contract should be cancelled immediately.
C. not be reviewed as the SLA cannot be updated.
D. be reviewed and updated if required.

Correct Answer: D
Section:
Explanation:
Reference: http://www.diva-portal.org/smash/get/diva2:1312384/FULLTEXT01.pdf

QUESTION 65
When migrating to a cloud environment, which of the following should be the PRIMARY driver for the use of encryption?

A. Cloud Service Provider encryption capabilities
B. The presence of PII
C. Organizational security policies
D. Cost-benefit analysis

Correct Answer: A
Section:

QUESTION 66

What type of termination occurs at the initiative of one party, and without the fault of the other party?

A. Termination for cause
B. Termination for convenience
C. Termination at the end of the term
D. Termination without the fault

Correct Answer: C
Section:

QUESTION 67
Which of the following is the BEST control framework for a European manufacturing corporation that is migrating to the cloud?

A. NIST SP 800-53
B. CSA's GDPR CoC
C. PCI-DSS
D. EU GDPR

Correct Answer: D
Section:
Explanation:
Reference: https://ec.europa.eu/info/sites/default/files/ec_cloud_strategy.pdf

QUESTION 68
Under GDPR, an organization should report a data breach within what time frame?

A. 72 hours
B. 2 weeks
C. 1 week
D. 48 hours

Correct Answer: A
Section:
Explanation:
Reference: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulationgdpr/personal-data-breaches/

QUESTION 69
Which plan will guide an organization on how to react to a security incident that might occur on the organization's systems, or that might be affecting one of their service providers?

A. Incident Response Plans
B. Security Incident Plans
C. Unexpected Event Plans
D. Emergency Incident Plans

Correct Answer: A
Section:

QUESTION 70
The rapid and dynamic rate of changes found in a cloud environment affects the organization's:

A. risk profile.
B. risk appetite.
C. risk scoring.
D. risk communication.

Correct Answer: B
Section:

QUESTION 71
Which of the following parties should have accountability for cloud compliance requirements?

A. Customer
B. Equally shared between customer and provider
C. Provider
D. Either customer or provider, depending on requirements

Correct Answer: B
Section:

QUESTION 72
A cloud customer configured and developed a solution on top of the certified cloud services. Building on top of a compliant CSP:

A. means that the cloud customer is also compliant.
B. means that the cloud customer and client are both compliant.
C. means that the cloud customer is compliant but their client is not compliant.
D. does not necessarily mean that the cloud customer is also compliant.

Correct Answer: D
Section:

QUESTION 73
An independent contractor is assessing security maturity of a SaaS company against industry standards. The SaaS company has developed and hosted all their products using the cloud services provided by a third-party cloud service provider (CSP). What is the optimal and most efficient mechanism to assess the controls
CSP is responsible for?

A. Review third-party audit reports.
B. Review CSP's published questionnaires.
C. Directly audit the CSP.
D. Send supplier questionnaire to the CSP.

Correct Answer: B
Section:
Explanation:
Reference: https://www.sapidata.sm/img/cms/CAIQ_v3-1_2020-01-13.pdf

QUESTION 74
One of the Cloud Control Matrix's (CCM's) control specifications states that "Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations." Which of the following controls under the Audit Assurance and Compliance domain does this match to?

A. Audit planning
B. Information system and regulatory mapping
C. GDPR auditing
D. Independent audits

Correct Answer: B
Section:

QUESTION 75
What data center and physical security measures should a cloud customer consider when assessing a cloud service provider?

A. Assess use of monitoring systems to control ingress and egress points of entry to the data center.
B. Implement physical security perimeters to safeguard personnel, data and information systems.
C. Conduct a due diligence to verify the cloud provider applies adequate physical security measures.
D. Review internal policies and procedures for relocation of hardware and software to an offsite location.

Correct Answer: C
Section:
Explanation:
Reference: https://www.omg.org/cloud/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

QUESTION 76
To assist an organization with planning a cloud migration strategy to execution, an auditor should recommend the use of:

A. object-oriented architecture.
B. software architecture.
C. service-oriented architecture.
D. enterprise architecture.

Correct Answer: C
Section:

QUESTION 77
Account design in the cloud should be driven by:

A. security requirements.
B. organizational structure.
C. business continuity policies.
D. management structure.

Correct Answer: A
Section:

QUESTION 78
In the context of Infrastructure as a Service (IaaS), a vulnerability assessment will scan virtual machines to identify vulnerabilities in:

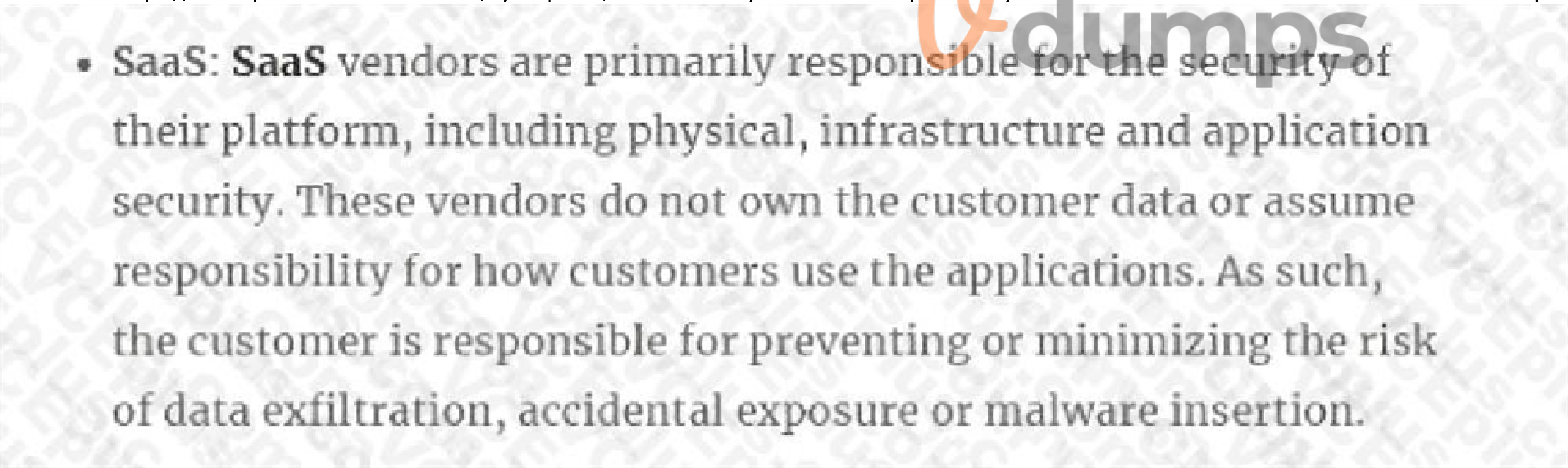
A. both operating system and application infrastructure contained within the CSP's instances.
B. both operating system and application infrastructure contained within the customer's instances
C. only application infrastructure contained within the CSP's instances.
D. only application infrastructure contained within the customer's instances.

Correct Answer: C
Section:

QUESTION 79
When using a SaaS solution, who is responsible for application security?

A. The cloud service provider only
B. The cloud service consumer only
C. Both cloud consumer and the enterprise
D. Both cloud provider and the consumer

Correct Answer: A
Section:
Explanation:
Reference: https://www.paloaltonetworks.com/cyberpedia/cloud-security-is-a-sharedresponsibility#:~:text=SaaS%3A%20SaaS%20vendors%20are%20primarily,how%20customers%20use%20the%20applications



- SaaS: **SaaS** vendors are primarily responsible for the security of their platform, including physical, infrastructure and application security. These vendors do not own the customer data or assume responsibility for how customers use the applications. As such, the customer is responsible for preventing or minimizing the risk of data exfiltration, accidental exposure or malware insertion.

QUESTION 80
The PRIMARY objective for an auditor to understand the organization's context for a cloud audit is to:

A. determine whether the organization has carried out control self-assessment and validated audit reports of the cloud service providers (CSP).
B. validate an understanding of the organization's current state and how the cloud audit plan fits into the existing audit approach.
C. validate whether an organization has a cloud audit plan in place.
D. validate the organization's performance effectiveness utilizing cloud service providers (CSP) solutions.

Correct Answer: B

Section:

QUESTION 81

A cloud service provider does not allow audits using automated tools as these tools could be considered destructive techniques for the cloud environment. Which of the following aspects of the audit will be constrained?

A. Purpose

B. Objectives

C. Nature of relationship

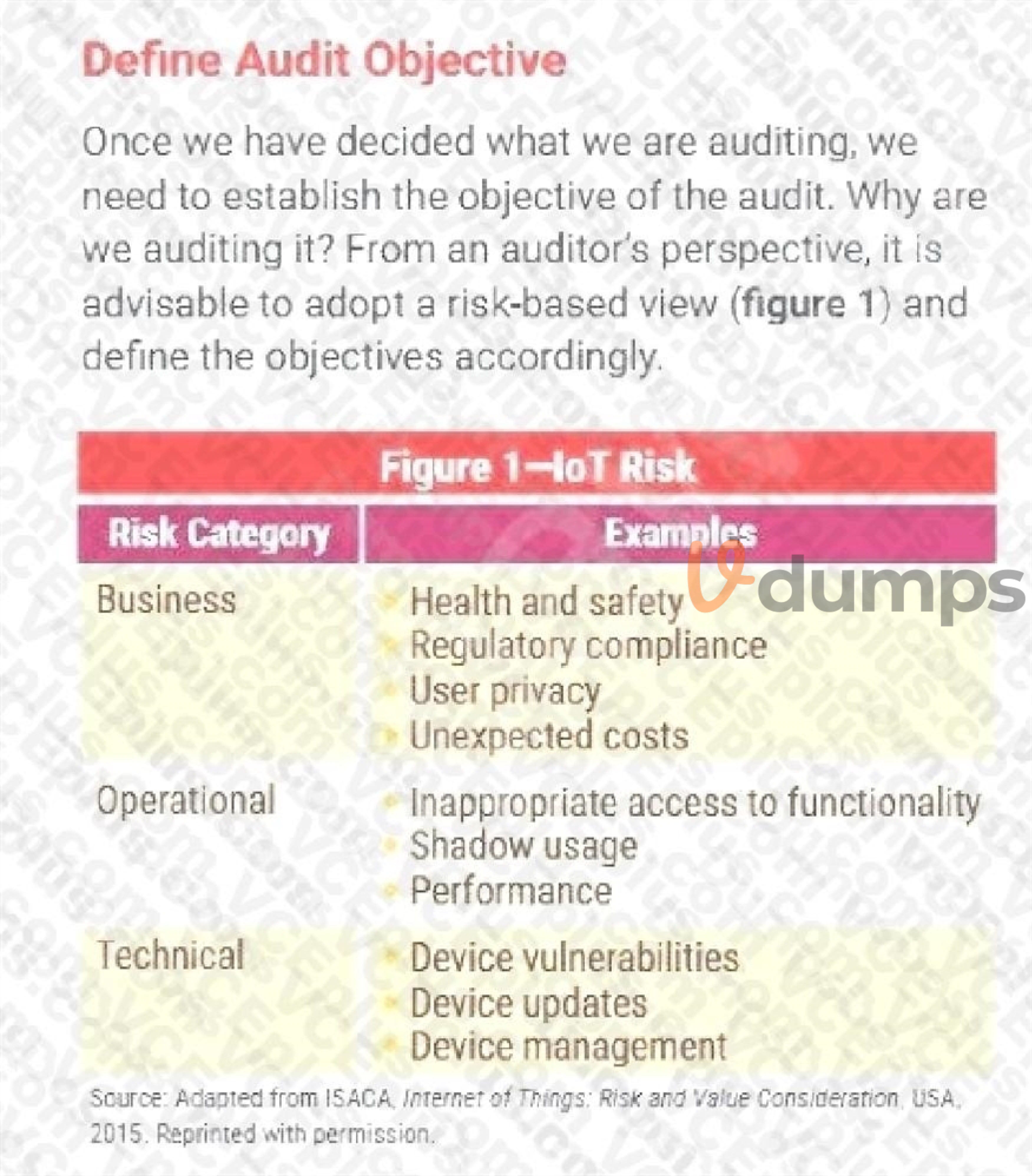
D. Scope

Correct Answer: B

Section:

Explanation:

Reference: https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2018/volume-5/journal-volume-5-2018



Define Audit Objective

Once we have decided what we are auditing, we need to establish the objective of the audit. Why are we auditing it? From an auditor's perspective, it is advisable to adopt a risk-based view (**figure 1**) and define the objectives accordingly.

Figure 1—IoT Risk

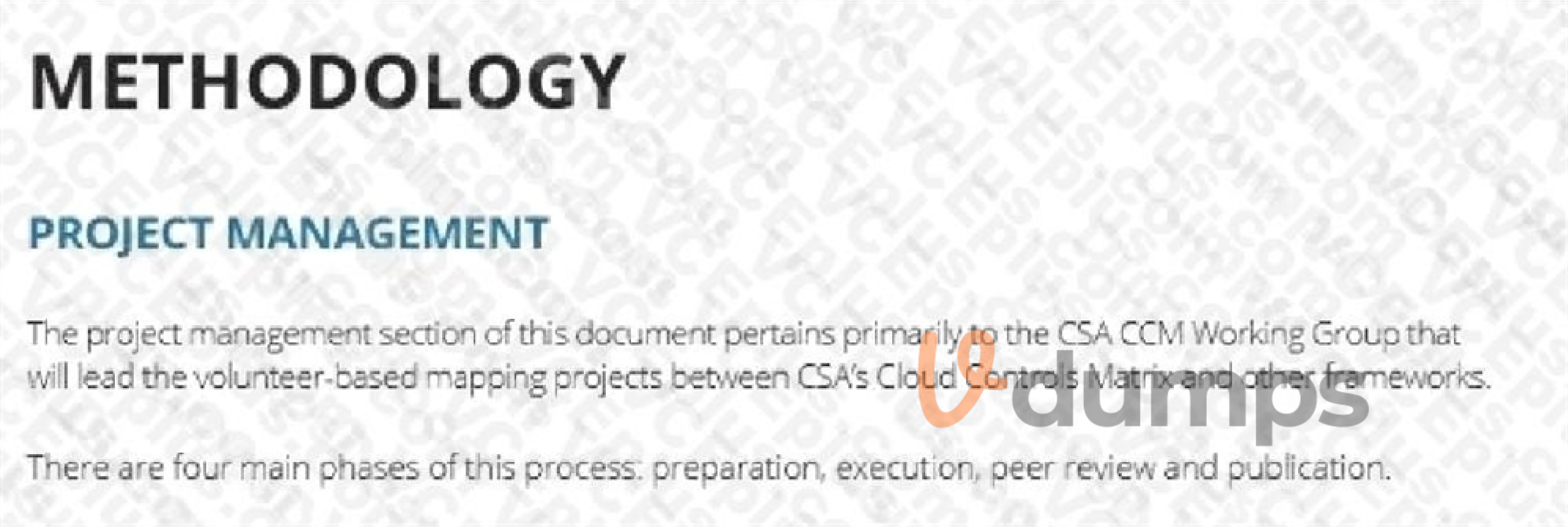
Risk Category	Examples
Business	- Health and safety - Regulatory compliance - User privacy - Unexpected costs
Operational	- Inappropriate access to functionality - Shadow usage - Performance
Technical	- Device vulnerabilities - Device updates - Device management

Source: Adapted from ISACA, *Internet of Things: Risk and Value Consideration*, USA, 2015. Reprinted with permission.

QUESTION 82
Which of the following are the three MAIN phases of the cloud controls matrix (CCM) mapping methodology?

A. Plan --> Develop --> Release
B. Deploy --> Monitor --> Audit
C. Initiation --> Execution --> Monitoring and Controlling
D. Preparation --> Execution --> Peer Review and Publication

Correct Answer: D
Section:
Explanation:
Reference: https://docplayer.net/153476370-Methodology-for-the-mapping-of-the-cloud-controls-matrix-ccm.html (page 5)



METHODOLOGY

PROJECT MANAGEMENT

The project management section of this document pertains primarily to the CSA CCM Working Group that will lead the volunteer-based mapping projects between CSA's Cloud Controls Matrix and other frameworks.

There are four main phases of this process: preparation, execution, peer review and publication.