[UPDATED 2024 CTPRP dumps Free Test Engine Verified By Certified Experts [Q62-Q83

[UPDATED 2024] CTPRP dumps Free Test Engine Verified By Certified Experts
Realistic CTPRP Accurate & Verified Answers As Experienced in the Actual Test!

NEW QUESTION 62

Which statement BEST describes the methods of performing due diligence during third party risk assessments?
* Inspecting physical and environmental security controls by conducting a facility tour
* Reviewing status of findings from the questionnaire and defining remediation plans
* interviewing subject matter experts or control owners, reviewing compliance artifacts, and validating controls
* Reviewing and assessing only the obligations that are specifically defined in the contract
Performing due diligence during third party risk assessments is a process of verifying and validating the information provided by the third parties, as well as identifying and assessing any potential risks or issues that may arise from the relationship. Due diligence methods may vary depending on the type, scope, and complexity of the third party engagement, but they generally involve the following steps123:

* Interviewing subject matter experts or control owners: This method involves engaging with the relevant stakeholders from both the organization and the third party, such as business owners, project managers, legal counsel, compliance officers, security analysts,

etc. The purpose of the interviews is to gather more information about the third party’s capabilities, processes, policies, performance, and challenges, as well as to clarify any questions or concerns that may arise from the questionnaire or other sources. The interviews can also help to establish rapport and trust between the parties, and to identify any gaps or discrepancies in the information provided.

* Reviewing compliance artifacts: This method involves examining the evidence or documentation that supports the third party’s claims or assertions, such as certifications, accreditations, audit reports, policies, procedures, contracts, SLAs, etc. The purpose of the review is to verify the accuracy, completeness, and validity of the artifacts, as well as to assess the level of compliance with the applicable standards, regulations, and best practices. The review can also help to identify any areas of improvement or weakness in the third party’s controls or processes.

* Validating controls: This method involves testing or inspecting the actual implementation and effectiveness of the third party’s controls or processes, such as security measures, quality assurance, data protection, incident response, etc. The purpose of the validation is to confirm that the controls are operating as intended and expected, and that they are sufficient to mitigate the risks or issues identified in the assessment. The validation can also help to identify any vulnerabilities or gaps in the third party’s controls or processes.

The other options are not as comprehensive or accurate as the methods described above, as they may not cover all the aspects or dimensions of the third party risk assessment, or they may rely on incomplete or outdated information. Inspecting physical and environmental security controls by conducting a facility tour is only one part of the validation method, and it may not be applicable or feasible for all types of third parties, such as cloud service providers or remote workers. Reviewing status of findings from the questionnaire and defining remediation plans is more of a follow-up or monitoring activity, rather than a due diligence method, as it assumes that the questionnaire has already been completed and analyzed. Reviewing and assessing only the obligations that are specifically defined in the contract is a narrow and limited approach, as it may not capture the full scope or complexity of the third party relationship, or the dynamic and evolving nature of the risks or issues involved. References:

* Third Party Due Diligence – a vital but challenging process

* The guide to risk based third party due diligence – VinciWorks

* Third Party Risk Assessment – Checklist & Best Practices

NEW QUESTION 63

Which statement is NOT a method of securing web applications?
* Ensure appropriate logging and review of access and events
* Conduct periodic penetration tests
* Adhere to web content accessibility guidelines
* Include validation checks in SDLC for cross site scripting and SOL injections

Web content accessibility guidelines (WCAG) are a set of standards that aim to make web content more accessible to people with disabilities, such as visual, auditory, cognitive, or motor impairments. While WCAG is a good practice for web development and usability, it is not directly related to web application security.

WCAG does not address the common security risks that web applications face, such as injection, broken authentication, misconfiguration, or vulnerable components. Therefore, adhering to WCAG is not a method of securing web applications, unlike the other options. References:

* 4: OWASP Top 10, a standard awareness document for web application security, lists the most critical security risks to web applications and provides best practices to prevent or mitigate them.

* 5: SANS Institute, a leading provider of cybersecurity training and certification, offers a security checklist for web application technologies (SWAT) that covers best practices for error handling, data protection, configuration, authentication, session management, input and output handling, and access control.

* 6: Built In, a platform for tech professionals, provides 13 web application security best practices, such as using a web application firewall, keeping track of APIs, enforcing expected application behaviors, and following the OWASP Top 10.

NEW QUESTION 64

Which of the following BEST reflects the risk of a ‘shadow IT” function?
* “Shadow IT” functions often fail to detect unauthorized use of information assets
* “Shadow IT” functions often lack governance and security oversight
* inability to prevent “shadow IT’ functions from using unauthorized software solutions
* Failure to implement strong security controls because IT is executed remotely
Shadow IT refers to the use of IT systems, services, or devices that are not authorized, approved, or supported by the official IT department. Shadow IT can pose significant risks to an organization’s data security, compliance, performance, and reputation. One of the main risks of shadow IT is that it often lacks governance and security oversight. This means that the shadow IT functions may not follow the established policies, standards, and best practices for IT management, such as data protection, access control, encryption, backup, patching, auditing, and reporting. This can expose the organization to various threats, such as data breaches, cyberattacks, malware infections, legal liabilities, regulatory fines, and reputational damage. Additionally, shadow IT can create operational inefficiencies, compatibility issues, duplication of efforts, and increased costs for the organization.

According to the web search results from the search_web tool, shadow IT is a common and growing phenomenon in many organizations, especially with the proliferation of cloud-based services and applications. Some of the articles suggest the following best practices for managing and mitigating shadow IT risks123:

* Performing SaaS assessments to proactively detect shadow IT

* Prioritizing user experience (UX) and providing support for integrating tools

* Streamlining user account and identity management

* Using operating systems and devices with which employees are comfortable

* Compromising and collaborating with users to minimize shadow IT risks

* Educating and training users on the security risks and consequences of shadow IT

* Establishing clear policies and guidelines for IT procurement and usage

* Creating a culture of trust and transparency between IT and business units Therefore, the verified answer to the question is B. “Shadow IT” functions often lack governance and security oversight.

References:

* Shadow IT Explained: Risks & Opportunities – BMC Software

* Start reducing your organization’s Shadow IT risk in 3 steps

* What is shadow IT? – Article | SailPoint

NEW QUESTION 65

Which statement is FALSE regarding analyzing results from a vendor risk assessment?
* The frequency for conducting a vendor reassessment is defined by regulatory obligations
* Findings from a vendor risk assessment may be defined at the entity level, and are based o na Specific topic or control
* Identifying findings from a vendor risk assessment can occur at any stage in the contract lifecycle
* Risk assessment findings identified by controls testing or validation should map back to the information gathering questionnaire and agreed upon framework
The frequency for conducting a vendor reassessment is not necessarily defined by regulatory obligations, but rather by the risk rating and criticality of the vendor, as well as the changes in the vendor’s environment, performance, and controls. Regulatory obligations may provide some guidance or minimum requirements for vendor reassessment, but they are not the sole determinant of the reassessment frequency. According to the Shared Assessments Program Tools User Guide, “The frequency of reassessment should be based on the risk rating and criticality of the vendor, as well as any changes in the vendor’s environment, performance, or controls. Regulatory guidance may also influence the frequency of reassessment.”1 Similarly, the CTPRP Study Guide states, “The frequency of reassessment should be based on the risk rating and criticality of the vendor, as well as any changes in the vendor’s environment, performance, or controls. Regulatory guidance may also influence the frequency of reassessment.”2 References:

* Shared Assessments Program Tools User Guide

* CTPRP Study Guide

NEW QUESTION 66

Which requirement is NOT included in IT asset end-of-life (EOL) processes?
* The requirement to conduct periodic risk assessments to determine end-of-life
* The requirement to track status using a change initiation request form
* The requirement to track updates to third party provided systems or applications for any planned end-of-life support
* The requirement to establish defined procedures for secure destruction al sunset of asset
In IT asset end-of-life (EOL) processes, the requirement to conduct periodic risk assessments specifically to determine end-of-life is not typically included. EOL processes generally focus on managing the decommissioning and secure disposal of IT assets that have reached the end of their useful life or support period. This includes tracking the status of assets, managing updates and support for third-party systems and applications, and establishing procedures for the secure destruction of assets at sunset. While risk assessments are crucial in overall IT asset management, they are not usually a direct component of determining an asset’s EOL status, which is more often based on operational effectiveness, manufacturer support, and technological obsolescence.

References:

* IT asset management and disposal best practices, such as those outlined in the NIST Guidelines for Media Sanitization (NIST SP 800-88), focus on the secure and environmentally responsible disposal of IT assets without specifically mandating periodic risk assessments for EOL determination.

* The “IT Asset Disposal (ITAD) Best Practice Guide” by the International Association of IT Asset Managers (IAITAM) provides insights into effective EOL processes, including tracking, updating, and securely destroying IT assets.

NEW QUESTION 67

Physical access procedures and activity logs should require all of the following EXCEPT:
* Require multiple access controls for server rooms and data centers

* Require physical access logs to be retained indefinitely for audit purposes
* Record successful and unsuccessful attempts including investigation of unsuccessful access attempts
* Include a process to trigger review of the logs after security events

Physical access procedures and activity logs are important components of third-party risk management, as they help to ensure the security and integrity of the physical assets and data of the organization and its third parties.

However, requiring physical access logs to be retained indefinitely for audit purposes is not a best practice, as it may pose legal, regulatory, and operational challenges. According to the Supplemental Examination Procedures for Risk Management of Third-Party Relationships, physical access logs should be retained for a reasonable period of time, consistent with the organization’s policies and procedures, and in compliance with applicable laws and regulations1. Retaining physical access logs indefinitely may increase the risk of unauthorized access, data breaches, privacy violations, and litigation2. Therefore, the statement B is the correct answer, as it is the only one that does not reflect a best practice for physical access procedures and activity logs.

References:

* 1: How to Write Third-Party Risk Management (TPRM) Policies and Procedures – SecurityScorecard Blog

* 2: Five Best Practices to Manage and Control Third-Party Risk – Broadcom Inc.

* 3: A checklist for third-party risk management platforms – Crowe LLP

* 4: Supplemental Examination Procedures for Risk Management of Third-Party Relationships

* 5: Third Party Risk Management: Why It’s Important And What Features To Look For – Expert Insights

NEW QUESTION 68

Which of the following BEST describes the distinction between a regulation and a standard?

* A regulation must be adhered to by all companies subject to its requirements, but companies “can voluntarily choose to follow standards.
* There is no distinction, regulations and standards are the same and have equal impact
* Standards are always a subset of a regulation
* A standard must be adhered to by companies based on the industry they are in, while regulations are voluntary.

A regulation is a rule of order having the force of law, prescribed by a superior or competent authority, relating to the actions of those under the authority’s control. Regulations are issued by various government departments and agencies to carry out the intent of legislation enacted by the legislature of the applicable jurisdiction. Regulations also function to ensure uniform application of the law. A standard is a guideline established generally by private-sector bodies and that are available for use by any person or organization, private or government. The term includes what are commonly referred to as ‘industry standards’ as well as

‘consensus standards’. Standards are developed through a voluntary process of collaboration and consensus among stakeholders, such as manufacturers, consumers, regulators, and experts. Standards may reflect best practices, technical specifications, performance criteria, or quality requirements. Standards do not have the force of law unless they are adopted or referenced by a regulation. Therefore, a regulation must be adhered to by all companies subject to its requirements, but companies can voluntarily choose to follow standards that are relevant and beneficial to their operations, products, or services. References:

* The Difference Between Regulations and Standards

* Regulations vs Standards: Clearing Up the Confusion – AEM

* Standards vs. Regulations

* Certified Third Party Risk Professional (CTPRP) Study Guide

NEW QUESTION 69

Which policy requirement is typically NOT defined in an Asset Management program?
* The Policy states requirements for the reuse of physical media (e.9., devices, servers, disk drives, etc.)
* The Policy requires that employees and contractors return all company data and assets upon termination of their employment, contract or agreement
* The Policy defines requirements for the inventory, identification, and disposal of equipment “and/or physical media
* The Policy requires visitors (including other tenants and maintenance personnel) to sign-in and sign-out of the facility, and to be escorted at all times
An Asset Management program is a set of policies, procedures, and practices that aim to optimize the value, performance, and lifecycle of the organization’s assets, such as physical, financial, human, or information assets123. An Asset Management program typically defines policy requirements for the following aspects of asset management:

* The Policy states requirements for the reuse of physical media (e.g., devices, servers, disk drives, etc.):

This requirement ensures that the organization follows proper procedures for sanitizing, wiping, or destroying physical media that contain sensitive or confidential data before reusing, recycling, or disposing of them123. This requirement helps prevent data leakage, theft, or loss, and protects the organization’s reputation and compliance123.

* The Policy requires that employees and contractors return all company data and assets upon termination of their employment, contract or agreement: This requirement ensures that the organization recovers all the data and assets that were assigned, loaned, or accessed by the employees and contractors during their employment, contract, or agreement123. This requirement helps maintain the security, integrity, and availability of the organization’s data and assets, and prevents unauthorized or inappropriate use or disclosure of them123.

* The Policy defines requirements for the inventory, identification, and disposal of equipment and/or physical media: This requirement ensures that the organization maintains an accurate and up-to-date

* record of all the equipment and physical media that it owns, leases, or uses, and assigns unique identifiers to them123. This requirement also ensures that the organization follows proper procedures for disposing of equipment and physical media that are no longer needed, useful, or functional123. This requirement helps improve the efficiency, effectiveness, and accountability of the organization’s asset management processes, and reduces the risks of waste, fraud, or misuse of the organization’s resources123.

However, option D, a policy requirement that requires visitors (including other tenants and maintenance personnel) to sign-in and sign-out of the facility, and to be escorted at all times, is typically not defined in an Asset Management program. Rather, this requirement is more likely to be defined in a Physical Security program, which is a set of policies, procedures, and practices that aim to protect the organization’s premises, assets, and personnel from unauthorized access, damage, or harm . A Physical Security program typically defines policy requirements for the following aspects of physical security:

* The Policy requires visitors (including other tenants and maintenance personnel) to sign-in and sign-out of the facility, and to be escorted at all times: This requirement ensures that the organization controls and monitors the access of visitors to the facility, and verifies their identity, purpose, and authorization .

This requirement also ensures that the organization prevents visitors from accessing restricted or sensitive areas, equipment, or information, and escorts them throughout their visit . This requirement helps enhance the security, safety, and compliance of the

organization’s facility, assets, and personnel, and prevents potential threats, incidents, or breaches .

* The Policy defines requirements for the locking, alarming, and surveillance of the facility and its entrances and exits: This requirement ensures that the organization secures the perimeter and the interior of the facility, and detects and responds to any unauthorized or suspicious activity or intrusion . This requirement also ensures that the organization uses appropriate and effective physical security measures, such as locks, alarms, cameras, guards, or barriers, to deter, prevent, or delay unauthorized access . This requirement helps protect the organization’s facility, assets, and personnel from theft, vandalism, sabotage, or attack .

* The Policy specifies requirements for the emergency preparedness and response of the facility and its occupants: This requirement ensures that the organization plans and implements procedures for dealing with emergencies, such as fire, flood, earthquake, power outage, or active shooter, that may affect the facility and its occupants . This requirement also ensures that the organization provides adequate and accessible equipment, resources, and training for the emergency preparedness and response, such as fire extinguishers, first aid kits, evacuation routes, emergency contacts, or drills . This requirement helps ensure the safety, health, and continuity of the organization’s facility, assets, and personnel, and minimizes the impact and damage of emergencies .

Therefore, option D is the correct answer, as it is the only one that does not reflect a policy requirement that is typically defined in an Asset Management program. References: The following resources support the verified answer and explanation:

* 1: Asset Management Policy Guide + Free Template | Fiix

* 2: Asset Management Policy: How to Build One From Scratch – Limble CMMS

* 3: How to develop an asset management policy, strategy and governance framework: Set up a consistent approach to asset management in your municipality

* : Physical Security Policy – SANS

* : Physical Security Policy – IT Governance

NEW QUESTION 70

An outsourcer’s vendor risk assessment process includes all of the following EXCEPT:
* Establishing risk evaluation criteria based on company policy
* Developing risk-tiered due diligence standards
* Setting remediation timelines based on the severity level of findings
* Defining assessment frequency based on resource capacity

An outsourcer’s vendor risk assessment process should include all the steps mentioned in options A, B, and C, as they are essential for ensuring a consistent, comprehensive, and effective evaluation of the vendor’s performance, compliance, and risk profile. However, option D is not a necessary or recommended part of the vendor risk assessment process, as it does not reflect the actual level of risk posed by the vendor, but rather the availability of resources within the outsourcer’s organization. Defining assessment frequency based on resource capacity could lead to under-assessing or over-assessing vendors, depending on the outsourcer’s workload, budget, and staff. This could result in missing critical issues, wasting time and money, or creating gaps in the vendor oversight program. Therefore, option D is the correct answer, as it is the only one that does not belong to the vendor risk assessment process. References: The following resources support the verified answer and explanation:

* Shared Assessments’ CTPRP Job Guide, page 10, section 2.1.1, states that “The frequency of assessments should be based on the risk tier of the third party, not on the availability of resources.”

* Guide to Vendor Risk Assessment, section “Step 3: Determine the Frequency of Vendor Risk Assessments”, explains that “The frequency of vendor risk assessments should be based on the level of risk each vendor poses to your

organization, not on the availability of resources or convenience.”

* How to Conduct a Successful Vendor Risk Assessment in 9 Steps, section “Step 8: Determine the Frequency of Vendor Risk Assessments”, advises that “The frequency of vendor risk assessments should be based on the level of risk each vendor poses to your organization, not on the availability of resources or convenience.”

NEW QUESTION 71

Which cloud deployment model is focused on the management of hardware equipment?
* Function as a service
* Platform as a service
* Software as a service
* Infrastructure as a service

Infrastructure as a service (IaaS) is a cloud deployment model that provides users with access to virtualized hardware resources, such as servers, storage, and network devices. Users can install and run their own operating systems and applications on the cloud infrastructure, and have full control over the configuration and management of the hardware equipment. IaaS is suitable for organizations that need high scalability, flexibility, and customization of their cloud environment. IaaS is different from other cloud deployment models, such as function as a service (FaaS), platform as a service (PaaS), and software as a service (SaaS), which provide users with higher-level services and abstract away the underlying hardware details. References:

* Cloud Infrastructure: 4 Key Components and Deployment Models

* Cloud Deployment Models – GeeksforGeeks

* On-Premises Cloud Deployment Model: Organization-Owned Hardware Explained

NEW QUESTION 72

At which level of reporting are changes in TPRM program metrics rare and exceptional?
* Business unit
* Executive management
* Risk committee
* Board of Directors

TPRM program metrics are the indicators that measure the performance, effectiveness, and maturity of the TPRM program. They help to monitor and communicate the progress, achievements, and challenges of the TPRM program to various stakeholders, such as business units, executive management, risk committees, and board of directors. However, the level of reporting and the frequency of changes in TPRM program metrics vary depending on the stakeholder’s role, responsibility, and interest123:

* Business unit: This level of reporting is focused on the operational aspects of the TPRM program, such as the status of vendor assessments, remediation actions, issues, and incidents. The changes in TPRM program metrics at this level are frequent and granular, as they reflect the day-to-day activities and outcomes of the TPRM program.

* Executive management: This level of reporting is focused on the strategic aspects of the TPRM program, such as the alignment with the business objectives, the compliance with the regulatory requirements, the management of the key risks, and the optimization of the resources and costs. The changes in TPRM program metrics at this level are less frequent and more aggregated, as they reflect the overall direction and performance of the TPRM program.

* Risk committee: This level of reporting is focused on the oversight aspects of the TPRM program, such as the evaluation of the risk appetite, the review of the risk profile, the approval of the risk policies, and the escalation of the risk issues. The changes in TPRM program metrics at this level are occasional and more analytical, as they reflect the governance and assurance of the TPRM

program.

* Board of Directors: This level of reporting is focused on the advisory aspects of the TPRM program, such as the endorsement of the risk strategy, the awareness of the risk trends, the guidance of the risk culture, and the support of the risk initiatives. The changes in TPRM program metrics at this level are rare and exceptional, as they reflect the high-level and long-term vision and value of the TPRM program.

Therefore, the correct answer is D. Board of Directors, as this is the level of reporting where changes in TPRM program metrics are rare and exceptional. References:

* 1: 15 KPIs & Metrics to Measure the Success of Your TPRM Program | UpGuard

* 2: Third-party risk management metrics: Best practices to enhance your … | Diligent

* 3: TPRM Metrics – Telling Your Risk Story – Shared Assessments | Shared Assessments

NEW QUESTION 73

A contract clause that enables each party to share the amount of information security risk is known as:
* Limitation of liability
* Cyber Insurance
* Force majeure
* Mutual indemnification

Indemnification is a contractual obligation by which one party agrees to compensate another party for any losses or damages that may arise from a specified event or circumstance. Mutual indemnification means that both parties agree to indemnify each other for certain losses or damages, such as those caused by a breach of contract, negligence, or violation of law. Mutual indemnification can enable each party to share the amount of information security risk, as it can provide a mechanism for allocating the responsibility and liability for any security incidents or breaches that may affect either party or their customers. Mutual indemnification can also incentivize each party to maintain adequate security controls and practices, as well as to cooperate and communicate effectively in the event of a security incident or breach.

The other options are not contract clauses that enable each party to share the amount of information security risk, because:

* A. Limitation of liability is a contract clause that limits the amount or type of damages that one party can claim from another party in the event of a breach of contract or other legal action. Limitation of liability does not enable each party to share the amount of information security risk, as it can reduce or cap the liability of one party, but not necessarily distribute or balance the risk between both parties.

* B. Cyber insurance is a type of insurance policy that covers the costs and losses resulting from cyberattacks, data breaches, or other cyber incidents. Cyber insurance does not enable each party to

* share the amount of information security risk, as it can transfer or mitigate the risk to a third-party insurer, but not necessarily allocate or share the risk between both parties.

* C. Force majeure is a contract clause that excuses one or both parties from performing their contractual obligations in the event of an unforeseen or unavoidable event or circumstance that is beyond their control, such as a natural disaster, war, or pandemic. Force majeure does not enable each party to share the amount of information security risk, as it can suspend or terminate the contract in the event of a force majeure event, but not necessarily distribute or balance the risk between both parties.

References:

* Shared Assessments CTPRP Study Guide, page 62, section 5.2.2: Contractual Terms

* Third-Party Risk Management: Vendor Contract Terms and Conditions, section: Indemnification

* Cybersecurity risks from third party vendors: PwC, section: Contractual terms and conditions

* [Third-Party Risk Management: The 3rd Party Ecosystem: How to Manage the Risk While Keeping the Benefit], section: Contractual Terms and Conditions

NEW QUESTION 74

You receive a call from a vendor that two laptops and a tablet are missing that were used to process your company data. The asset loss occurred two years ago, but was only recently discovered. That statement may indicate that this vendor is lacking an adequate:
* Asset Management Program
* Physical and Environmental Security Program
* Data Loss Prevention Program
* Information Security Incident Notification Policy
The scenario described indicates a lack in the vendor’s Asset Management Program. An effective Asset Management Program includes maintaining an accurate inventory of hardware and devices, monitoring their status, and promptly identifying and responding to any losses or discrepancies. The failure to discover the loss of laptops and a tablet that processed company data for two years suggests deficiencies in tracking and managing physical assets. This lapse can lead to risks associated with data security, regulatory compliance, and operational integrity. A robust Asset Management Program should ensure that all assets are accounted for, their usage is monitored, and any anomalies or losses are quickly identified and addressed.

References:

* IT asset management standards, such as ISO/IEC 27001 (Information Security Management), emphasize the importance of maintaining an inventory of assets and implementing appropriate controls to safeguard

* organizational assets.

* The “IT Asset Management Handbook” by the International Association of IT Asset Managers (IAITAM) provides guidelines on establishing a comprehensive Asset Management Program, including best practices for asset tracking, monitoring, and loss prevention.

NEW QUESTION 75

You are updating the inventory of regulations that impact your TPRM program during the company’s annual risk assessment. Which statement provides the optimal approach to prioritizing the regulations?
* identify the applicable regulations that require an extension of specific obligations to service providers
* Narrow the focus only on the regulations that directly apply to personal information
* Include the regulations that have the greater risk of triggering enforcement or fines/penalties
* Emphasize the federal regulations since they supersede state regulations
Third-party risk management (TPRM) is the process of identifying, assessing, and mitigating the risks associated with outsourcing business activities or functions to external entities. TPRM is influenced by various regulations that aim to protect the interests of customers, stakeholders, and regulators from the potential harm caused by third-party failures or misconduct. These regulations may vary depending on the industry, jurisdiction, and nature of the third-party relationship. Therefore, it is important for organizations to update their inventory of regulations that impact their TPRM program during their annual risk assessment, and prioritize the regulations that are most relevant and critical for their business objectives and risk appetite.

The optimal approach to prioritizing the regulations is to identify the applicable regulations that require an extension of specific obligations to service providers. This means that the organization should focus on the regulations that impose certain requirements or expectations on the organization and its third-party partners, such as data protection, security, compliance, reporting, auditing, or performance standards. These regulations may also specify the roles and responsibilities of the organization and the service provider, the scope and frequency of due diligence and monitoring activities, the contractual clauses and terms, and the remediation and termination procedures. By identifying these regulations, the organization can ensure that its TPRM program is aligned with the regulatory expectations and obligations, and that it can effectively manage and mitigate the risks associated with its third-party relationships.

Some examples of regulations that require an extension of specific obligations to service providers are:

* The General Data Protection Regulation (GDPR): This is a European Union regulation that governs the collection, processing, and transfer of personal data of individuals in the EU. The GDPR requires organizations to implement appropriate technical and organizational measures to protect the personal data, and to only engage with service providers that can provide sufficient guarantees of data protection.

The GDPR also requires organizations to enter into written contracts with their service providers that specify the subject matter, duration, nature, and purpose of the data processing, as well as the rights and obligations of both parties. The GDPR also imposes strict notification and reporting requirements in case of data breaches or violations.

* The Health Insurance Portability and Accountability Act (HIPAA): This is a US federal law that regulates the privacy and security of health information of individuals. The HIPAA requires covered entities, such as health care providers, health plans, and health care clearinghouses, to safeguard the health information of their patients, and to only disclose or share it with authorized parties. The HIPAA also requires covered entities to enter into business associate agreements with their service providers that handle or access the health information on their behalf. These agreements must specify the permitted and required uses and disclosures of the health information, the safeguards and measures to protect the health information, and the reporting and notification obligations in case of breaches or incidents.

* The Sarbanes-Oxley Act (SOX): This is a US federal law that aims to improve the accuracy and reliability of corporate financial reporting and disclosure. The SOX requires public companies to establish and maintain internal controls over their financial reporting processes, and to assess and report on the effectiveness of these controls. The SOX also requires public companies to ensure that their external auditors are independent and qualified, and to disclose any material weaknesses or deficiencies in their internal controls. The SOX also applies to the service providers that perform or support the financial reporting functions of the public companies, such as accounting firms, information technology vendors, or consultants. The SOX requires public companies to evaluate and monitor the internal controls of their service providers, and to include them in their scope of audit and reporting.

References:

* Third-Party Risk Management and Mitigation | Gartner

* Best Practices to Jumpstart Third-Party Risk Management Program

* Third-party risk management best practices and why they matter

* GDPR and Third-Party Risk Management

* HIPAA Compliance for Business Associates and Third-Party Service Providers

* SOX Compliance Requirements for Third-Party Service Providers

NEW QUESTION 76

When defining due diligence requirements for the set of vendors that host web applications which of the following is typically NOT part of evaluating the vendor’s patch management controls?
* The capability of the vendor to apply priority patching of high-risk systems
* Established procedures for testing of patches, service packs, and hot fixes prior to installation
* A documented process to gain approvals for use of open source applications
* The existence of a formal process for evaluation and prioritization of known vulnerabilities

A documented process to gain approvals for use of open source applications is typically not part of evaluating the vendor’s patch management controls, because it is not directly related to the patching process. Patch management controls are the policies, procedures, and tools that enable an organization to identify, acquire, install, and verify patches for software vulnerabilities. Patch management controls aim to reduce the risk of exploitation of known software flaws and ensure the functionality and compatibility of the patched systems. A documented process to gain approvals for use of open source applications is more relevant to the software development and procurement processes, as it involves assessing the legal, security, and operational implications of using open source software components in the vendor’s products or services. Open source software may have different licensing terms, quality standards, and support levels than proprietary software, and may introduce additional vulnerabilities or dependencies that need to be managed. Therefore, a documented process to gain approvals for use of open source applications is a good practice for vendors, but it is not a patch management control per se. References:

* Guide to Enterprise Patch Management Planning

* Governance of Key Aspects of System Patch Management

* Certified Third Party Risk Professional (CTPRP) Study Guide

NEW QUESTION 77

Which of the following components are typically NOT part of a cloud hosting vendor assessment program?
* Reviewing the entity’s image snapshot approval and management process
* Requiring security services documentation and audit attestation reports
* Requiring compliance evidence that provides the definition of patching responsibilities
* Conducting customer performed penetration tests

A cloud hosting vendor assessment program is a process of evaluating the security, compliance, and performance of a cloud service provider (CSP) that hosts an organization’s data or applications. A cloud hosting vendor assessment program typically includes the following components123:

* Reviewing the entity’s image snapshot approval and management process: This component involves verifying how the CSP creates, approves, stores, and deletes image snapshots of the virtual machines or containers that run the organization’s workloads. Image snapshots can contain sensitive data or configuration settings that need to be protected from unauthorized access or modification.

* Requiring security services documentation and audit attestation reports: This component involves requesting and reviewing the CSP’s documentation and reports that demonstrate the security controls and practices that the CSP implements to protect the organization’s data and applications. These may include service level agreements (SLAs), security policies and procedures, security certifications and standards, vulnerability scanning and patching reports, incident response and disaster recovery plans, and independent audit reports such as SOC 2 or ISO 27001.

* Requiring compliance evidence that provides the definition of patching responsibilities: This component involves asking and verifying how the CSP handles the patching of the operating systems, applications, and libraries that run on the cloud infrastructure.

Patching is a critical activity to prevent security breaches and ensure compliance with regulatory requirements. The organization needs to understand the roles and responsibilities of the CSP and the organization in patching the cloud environment, and the frequency and scope of patching activities.

The component that is typically NOT part of a cloud hosting vendor assessment program is conducting customer performed penetration tests. Penetration testing is a method of simulating a cyberattack on a system or network to identify and exploit vulnerabilities and weaknesses. While penetration testing can be a valuable tool to assess the security posture of a CSP, it is not usually included in a cloud hosting vendor assessment program for the following reasons :

* Penetration testing may violate the CSP’s terms of service or acceptable use policy, which may prohibit or restrict the customer from performing any unauthorized or disruptive activities on the cloud infrastructure. The customer may face legal or contractual consequences if they conduct penetration testing without the CSP’s consent or knowledge.

* Penetration testing may interfere with the CSP’s normal operations or affect the availability and performance of the cloud services for other customers. The customer may cause unintended damage or disruption to the CSP’s systems or networks, or trigger false alarms or alerts that may divert the CSP’s resources or attention.

* Penetration testing may not provide a comprehensive or accurate assessment of the CSP’s security, as the customer may have limited visibility or access to the CSP’s internal systems or networks, or may encounter security mechanisms or countermeasures that prevent or limit the penetration testing activities. The customer may also face ethical or legal issues if they access or compromise the data or systems of other customers or the CSP.

Therefore, the verified answer to the question is D. Conducting customer performed penetration tests.

References:

* Four Important Best Practices for Assessing Cloud Vendors

* Top 11 Questionnaires for IT Vendor Assessment in 2024

* Cloud Vendor Assessments | Done The Right Way

* [Penetration Testing in the Cloud: What You Need to Know]

* [Cloud Penetration Testing: Challenges and Best Practices]

NEW QUESTION 78

Which activity BEST describes conducting due diligence of a lower risk vendor?
* Accepting a service providers self-assessment questionnaire responses
* Preparing reports to management regarding the status of third party risk management and remediation activities
* Reviewing a service provider’s self-assessment questionnaire and external audit report(s)
* Requesting and filing a service provider’s external audit report(s) for future reference

Due diligence is the process of evaluating the risks and opportunities associated with a potential or existing third-party vendor. Due diligence can vary in scope and depth depending on the level of risk that the vendor poses to the organization. Lower risk vendors are those that have minimal impact on the organization’s operations, reputation, or compliance, and that do not handle sensitive or confidential data or systems. For lower risk vendors, conducting due diligence may involve accepting the service provider’s self-assessment questionnaire responses as sufficient evidence of their capabilities, performance, and compliance. A self-assessment questionnaire is a tool that allows the vendor to provide information about their organization, services, processes, controls, and policies. The organization can use the questionnaire to verify the vendor’s identity, qualifications, references,

and certifications, and to assess the vendor’s alignment with the organization’s standards and expectations. Accepting the vendor’s self-assessment questionnaire responses as the primary source of due diligence can save time and resources for the organization, and can also demonstrate trust and confidence in the vendor. However, the organization should also ensure that the questionnaire is comprehensive, relevant, and updated, and that the vendor’s responses are accurate, complete, and consistent.

The organization should also reserve the right to request additional information or documentation from the vendor if needed, and to conduct periodic reviews or audits of the vendor’s performance and compliance.

The other options do not best describe conducting due diligence of a lower risk vendor, because they either involve more extensive or rigorous methods of due diligence, or they are not directly related to due diligence.

Preparing reports to management regarding the status of third party risk management and remediation activities is an important part of monitoring and managing the vendor relationship, but it is not a due diligence activity per se. Reviewing a service provider’s self-assessment questionnaire and external audit report(s) is a more thorough way of conducting due diligence, but it may not be necessary or feasible for lower risk vendors, especially if the external audit report(s) are not readily available or relevant. Requesting and filing a service provider’s external audit report(s) for future reference is a good practice for maintaining documentation and evidence of due diligence, but it is not a due diligence activity itself.

References:

* Third Party Risk Management (TPRM) | Shared Assessments

* Vendor Due Diligence Strategy Guide and Checklist | Prevalent

* Vendor due diligence: a practical guide and checklist

NEW QUESTION 79

Select the risk type that is defined as: “A third party may not be able to meet its obligations due to inadequate systems or processes”.
* Reliability risk
* Performance risk
* Competency risk
* Availability risk

Performance risk, defined as the risk that a third party may not be able to meet its obligations due to inadequate systems or processes, accurately describes the situation. This type of risk involves concerns about the third party’s ability to deliver services or products at the required performance level, potentially due to limitations in their technology infrastructure, operational procedures, or management practices. Identifying and managing performance risk is essential in Third-Party Risk Management (TPRM) to ensure that third-party vendors can reliably meet contractual and service-level agreements, thereby minimizing the impact on the organization’s operations and service delivery.

References:

* TPRM guidelines, such as those from the Office of the Comptroller of the Currency (OCC) and the Federal Financial Institutions Examination Council (FFIEC), highlight the importance of assessing and

* managing performance risks associated with third-party relationships.

* The “Third-Party Risk Management Guide” by ISACA discusses various types of risks, including performance

risk, associated with engaging third-party service providers, emphasizing the need for thorough due diligence and ongoing monitoring.

NEW QUESTION 80

Which statement is FALSE when describing the third party risk assessors’ role when conducting a controls evaluation using an industry framework?
* The Assessor’s role is to conduct discovery with subject matter experts to understand the control environment
* The Assessor’s role is to conduct discovery and validate responses from the risk assessment questionnaire by testing or validating controls
* The Assessor’s role is to provide an opinion on the effectiveness of controls conducted over a period of time in their report
* The Assessor’s role is to review compliance artifacts and identify potential control gaps based on evaluation of the presence of control attributes
According to the Shared Assessments Certified Third Party Risk Professional (CTPRP) Study Guide, the third party risk assessor’s role is to evaluate the design and operating effectiveness of the third party’s controls based on an industry framework, such as ISO, NIST, COBIT, or COSO1. The assessor’s role is not to provide an opinion on the effectiveness of controls, but rather to report the results of the evaluation in a factual and objective manner2. The assessor’s role is also to conduct discovery with subject matter experts to understand the control environment, to conduct discovery and validate responses from the risk assessment questionnaire by testing or validating controls, and to review compliance artifacts and identify potential control gaps based on evaluation of the presence of control attributes1. These are all true statements that describe the assessor’s role when conducting a controls evaluation using an industry framework.

References:

* 1: Shared Assessments Certified Third Party Risk Professional (CTPRP) Study Guide, page 29

* 2: What is a Third-Party Risk Assessment? – RiskOptics

NEW QUESTION 81

Which of the following factors is LEAST likely to trigger notification obligations in incident response?
* Regulatory requirements
* Data classification or sensitivity
* Encryption of data
* Contractual terms
Notification obligations in incident response are the legal or contractual duties to inform relevant parties about a security breach or incident that affects their data or systems. These obligations may vary depending on the type, scope, and impact of the incident, as well as the jurisdiction, industry, and contractual agreements involved. The factors that are most likely to trigger notification obligations are:

* Regulatory requirements: Different laws and regulations may impose different notification obligations on organizations that experience or cause a security incident. For example, the General Data Protection Regulation (GDPR) requires data controllers to notify the supervisory authority within 72 hours of becoming aware of a personal data breach, and to notify the affected data subjects without undue delay if the breach poses a high risk to their rights and freedoms1. Similarly, the Computer-Security Incident Notification Rule requires banks and their service providers to notify their primary federal regulator as soon as possible, but no later than 36 hours, after a computer-security incident that materially disrupts, degrades, or impairs their operations, services, or customers2.

* Data classification or sensitivity: The type and sensitivity of the data involved in a security incident may also affect the notification

obligations. For example, if the data contains personally identifiable information (PII), health information, financial information, or other confidential or sensitive information, the organization may have to notify the data owners, regulators, law enforcement, or other stakeholders about the incident and the potential risks to their privacy or security3. The data classification or sensitivity may also determine the content and timing of the notification, as well as the appropriate communication channels to use.

* Contractual terms: The contractual agreements between an organization and its third-party vendors or service providers may also specify the notification obligations in case of a security incident. For example, the contract may define the roles and responsibilities of each party, the notification procedures and timelines, the information to be shared, the remediation actions to be taken, and the penalties or liabilities for breach of contract. The contractual terms may also reflect the regulatory requirements or industry standards that apply to the organization or the third party.

The factor that is least likely to trigger notification obligations is:

* Encryption of data: Encryption of data is a security measure that protects the data from unauthorized access, modification, or disclosure. Encryption of data may reduce the impact or severity of a security incident, as it may prevent or limit the exposure of the data to malicious actors. However, encryption of data does not eliminate the notification obligations, as the organization still has to assess the nature and extent of the incident, and determine whether the encryption was effective or compromised. Moreover, encryption of data may not be sufficient to protect the data from other types of threats, such as deletion, corruption, or ransomware. Therefore, encryption of data is not a factor that influences the notification obligations in incident response.

References:

* 1: GDPR Article 33: Notification of a personal data breach to the supervisory authority

* 2: Computer-Security Incident Notification Rule

* 3: Third-Party Incident Management (TPIM): How to Balance IRPs with Third Parties

* : [Improving Third-Party Incident Response]

* : [Third-Party Incident Response Playbook]

* : [Does Encryption Protect You From a Data Breach?]

NEW QUESTION 82

The BEST way to manage Fourth-Nth Party risk is:
* Include a provision in the vender contract requiring the vendor to provide notice and obtain written consent before outsourcing any service
* Include a provision in the contract prohibiting the vendor from outsourcing any service which includes access to confidential data or systems
* Incorporate notification and approval contract provisions for subcontracting that require evidence of due diligence as defined by a TPRM program
* Require the vendor to maintain a cyber-insurance policy for any service that is outsourced which includes access to confidential data or systems
Fourth-Nth party risk refers to the potential threats and vulnerabilities associated with the subcontractors, vendors, or service providers of an organization’s direct third-party partners. This can create a complex network of dependencies and exposures that can affect the organization’s security, data protection, and business resilience. To manage this risk effectively, organizations should conduct comprehensive due diligence on their extended vendor and supplier network, and include contractual stipulations that require notification and approval for any subcontracting activities. This way, the organization can ensure that the

subcontractors meet the same standards and expectations as the direct third-party partners, and that they have adequate controls and safeguards in place to protect the organization’s data and systems. Additionally, the organization should monitor and assess the performance and compliance of the subcontractors on a regular basis, and update the contract provisions as needed to reflect any changes in the risk environment. References:

* Understanding 4th- and Nth-Party Risk: What Do You Need to Know?

* Best Practices for Fourth and Nth Party Management

* Fourth-Party Risk Management: Best Practices

NEW QUESTION 83

Which factor in patch management is MOST important when conducting postcybersecurity incident analysis related to systems and applications?
* Configuration
* Log retention
* Approvals
* Testing
In patch management, testing is the most crucial factor when conducting post-cybersecurity incident analysis related to systems and applications. Proper testing of patches before deployment ensures that they effectively address vulnerabilities without introducing new issues or incompatibilities that could impact system functionality or security. Testing allows organizations to verify that the patch resolves the identified security issue without adversely affecting the system or application’s performance. It also helps in identifying potential conflicts with existing configurations or dependencies. Effective testing strategies include regression testing, performance testing, and security testing to ensure comprehensive validation of the patch’s effectiveness and safety before widespread deployment. This approach aligns with best practices in patch management, emphasizing the importance of thorough testing to mitigate the risk of unintended consequences and ensure the continued security and stability of systems and applications.

References:

* Industry standards such as ISO/IEC 27001 (Information Security Management) highlight the importance of a systematic approach to managing patches, including the role of testing in assessing the effectiveness and impact of patches.

* Resources like “Patch Management Best Practices” from the Center for Internet Security (CIS) provide guidance on developing and implementing a patch management program that includes rigorous testing procedures to ensure patches are safely and effectively applied.

Latest Shared Assessments CTPRP Practice Test Questions:
https://www.examslabs.com/Shared-Assessments/Third-Party-Risk-Management/best-CTPRP-exam-dumps.html]