DUMPSBOSS.

Certified Third-Party Risk Professional (CTPRP)

Shared Assessments CTPRP

Version Demo

Total Demo Questions: 14

Total Premium Questions: 145

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

An outsourcer ' s vendor risk assessment process includes all of the following EXCEPT:

A. Establishing risk evaluation criteria based on company policy

B. Developing risk-tiered due diligence standards

C. Setting remediation timelines based on the severity level of findings

D. Defining assessment frequency based on resource capacity

ANSWER: D

Explanation:

Defining assessment frequency based on resource capacity is the exception because a mature third-party risk management program schedules initial and recurring due diligence according to the third party's inherent and residual risk, criticality, access to sensitive information, service scope, and the potential business impact of a failure. Resource planning is necessary to operate the program, but it must support—rather than determine—the risk-based assessment cadence. A high-risk or critical provider may require more frequent monitoring, reassessment, or targeted review when its risk profile, control environment, services, or relevant threat landscape changes. Conversely, lower-risk relationships may appropriately receive less frequent reassessment. This risk-based approach enables an outsourcer to focus oversight on the relationships that could create the greatest operational, information-security, compliance, financial, or resilience impact. Shared Assessments promotes a risk-based, scalable approach to third-party risk management, including use of standardized assessment tools and risk-focused due diligence. The program should document its tiering methodology and use the resulting tier to establish proportionate assessment and monitoring expectations. See Shared Assessments' Program Tools and its overview of Third-Party Risk Management.

QUESTION NO: 2

Which of the following components is NOT typically included in external continuous monitoring solutions?

A. Status updates on localized events based on geolocation

B. Alerts on legal and regulatory actions involving the vendor

C. Metrics that track SLAs for performance management

D. Reports that identify changes in vendor financial viability

ANSWER: C

Explanation:

Metrics that track SLAs for performance management are not typically included in an external continuous monitoring solution. External monitoring generally uses independently observable, outside-in information to identify developing third-party risk indicators, such as public legal or regulatory developments, adverse events, geographic disruption indicators, and signs of financial distress. This intelligence supports an organization's ongoing risk assessment by providing timely awareness of conditions that could affect a third party's ability to operate securely and reliably.

SLA performance metrics, by contrast, measure whether a supplier is meeting the specific service commitments negotiated in its contract, such as uptime, response times, transaction-processing performance, or incident-resolution targets. Obtaining and assessing those measurements is part of supplier relationship, contract, and performance management. The information commonly comes from supplier operational reporting, customer-side service data, governance meetings, or audit and assurance activities—not from an external monitoring provider's public- and intelligence-source collection. Shared Assessments emphasizes ongoing monitoring as a component of a mature third-party risk program, while contractual requirements and accountability are managed through the organization's supplier governance processes. See Shared Assessments and NIST's guidance on continuous monitoring at NIST SP 800-137.

QUESTION NO: 3

Information classification of personal information may trigger specific regulatory obligations. Which statement is the BEST response from a privacy perspective:

A. Personally identifiable financial information includes only consumer report information

B. Public personal information includes only web or online identifiers

C. Personally identifiable information and personal data are similar in context, but may have different legal definitions based upon jurisdiction

D. Personally Identifiable Information and Protected Healthcare Information require the exact same data protection safequards

ANSWER: C

Explanation:

Personally identifiable information and personal data are similar in context, but may have different legal definitions based upon jurisdiction is the best response because privacy classification must account for the laws governing the data, the individuals involved, and the processing context. Both terms generally concern information that identifies, relates to, or can reasonably be linked to an individual, whether directly or indirectly. However, the precise statutory scope, exclusions, and associated obligations differ across jurisdictions and regulatory regimes.

For example, the EU General Data Protection Regulation defines personal data broadly as any information relating to an identified or identifiable natural person. This can include direct identifiers as well as indirect identifiers, such as online identifiers, where they can be used to identify a person. Organizations therefore need to classify information according to applicable legal definitions and ensure that their third parties apply controls appropriate to the relevant jurisdiction, data category, and processing purpose. This approach supports accurate risk assessments, contractual requirements, data-handling procedures, and regulatory compliance. See the GDPR definition in GDPR Article 4 and the California definition of personal information in California Civil Code §1798.140.

QUESTION NO: 4

A third party will process customer information through a subcontracted cloud platform. Which contract requirement provides the BEST evidence that the third party remains accountable for the downstream service provider's control obligations?

A. A service-level agreement defining uptime and support-response targets

B. A flow-down provision requiring equivalent obligations for subcontractors

C. An indemnification provision for losses arising from a security incident

D. A right-to-audit provision applicable only to the primary third party

ANSWER: B

Explanation:

A flow-down requirement obligates the third party to impose applicable security, privacy, confidentiality, incident-notification, and data-handling requirements on its subcontractors while retaining responsibility for performance. This creates a contractual mechanism for extending relevant obligations throughout the service delivery chain.

A right to audit can support oversight but does not itself require the third party to bind its subcontractors to the customer's requirements. Indemnification allocates certain losses, and an SLA addresses service performance; neither establishes the necessary downstream control obligations.

QUESTION NO: 5

Your company has been alerted that an IT vendor began utilizing a subcontractor located in a country restricted by company policy. What is the BEST approach to handle this situation?

A. Notify management to approve an exception and ensure that contract provisions require prior “notification and evidence of subcontractor due diligence

B. inform the business unit and recommend that the company cease future work with the IT vendor due to company policy

C. Update the vender inventory with the mew location information in order to schedule a reassessment

D. Inform the business unit and ask the vendor to replace the subcontractor at their expense in “order to move the processing back to an approved country

ANSWER: D

Explanation:

“Inform the business unit and ask the vendor to replace the subcontractor at their expense in “order to move the processing back to an approved country” is the best response because the vendor has introduced a subcontracting arrangement that conflicts with an established geographic-risk policy. Restricted-country requirements commonly address risks associated with legal jurisdiction, regulatory obligations, data access, government access, resilience, sanctions, and the organization’s defined risk appetite. Once the issue is identified, the organization should promptly engage the accountable business owner and require the vendor to remediate the nonconforming arrangement. Moving the processing to an approved country restores alignment with the organization’s policy and preserves the intended control over where subcontracted services and information processing occur.

Third-party contracts should establish requirements for subcontractor oversight, including approved locations, notification or approval conditions, and responsibility for the vendor’s downstream providers. Requiring remediation at the vendor’s expense appropriately places accountability with the party that changed the subcontracting model and ensures that the organization does not absorb the cost of correcting vendor noncompliance. This response also supports ongoing monitoring: the business relationship can continue only after the geographic exposure has been returned to an approved state and the corrective action is validated. Shared Assessments describes resources for managing third-party risk through governance, due diligence, contracting, and monitoring in its Third Party Risk Management resources. The Standardized Information Gathering questionnaire also addresses assessment of third-party and subcontractor controls.

QUESTION NO: 6

You are reviewing assessment results of workstation and endpoint security. Which result should trigger more investigation due to greater risk potential?

A. Use of multi-tenant laptops

B. Disabled printing and USB devices

C. Use of desktop virtualization

D. Disabled or blocked access to internet

ANSWER: A

Explanation:

Use of multi-tenant laptops should trigger additional investigation because a single endpoint is used by more than one tenant, user population, or organizational boundary. This arrangement increases the importance of confirming that identities, data, operating-system sessions, applications, storage, and administrative privileges are reliably separated. The assessment should establish who administers the device; whether each tenant can access only its own data and resources; how endpoint detection, patching, encryption, and logging are consistently applied; and how the device is securely reset, reimaged, or deprovisioned between users. A compromise, configuration weakness, or inadequate separation on a shared endpoint can potentially expose information or credentials belonging to another tenant and can expand the scope of an incident. The reviewer should also verify that contractual responsibilities, acceptable-use requirements, incident notification processes, and forensic-access arrangements address the shared-device model. This is consistent with third-party risk practice: risk analysis should account for the service arrangement, access model, data handled, and effectiveness of

compensating controls. NIST's telework and endpoint guidance emphasizes protecting devices, data, and remote access through centrally managed security controls; see NIST SP 800-46 Rev. 2. Shared Assessments' program resources likewise emphasize assessing third-party control environments and associated risks: Shared Assessments.

QUESTION NO: 7

Which of the following factors is MOST important when assessing the risk of shadow IT in organizational security?

A. The organization maintains adequate policies and procedures that communicate required controls for security functions

B. The organization requires security training and certification for security personnel

C. The organization defines staffing levels to address impact of any turnover in security roles

D. The organization ' s resources and investment are sufficient to meet security requirements

ANSWER: A

Explanation:

The organization maintains adequate policies and procedures that communicate required controls for security functions is the most important factor because governance establishes the organization's baseline expectations for authorized technology use, data handling, access, procurement, risk acceptance, and exception management. Shadow IT commonly emerges when technology is acquired or used outside established approval and oversight processes. Clear, current, and communicated policies define those processes and make it possible to identify when an application, service, device, or data flow has bypassed required security review. They also assign accountability, require appropriate due diligence and monitoring, and establish a consistent mechanism for reporting and remediating unauthorized technology use. In a third-party risk context, these controls help ensure that externally sourced services are evaluated for security, privacy, resilience, and contractual requirements before organizational data or systems are exposed. This governance foundation supports effective awareness, detection, and response activities by defining what "approved," "required," and "noncompliant" mean in practice. Shared Assessments emphasizes the use of standardized tools and practices to assess third-party risk and promote consistent control expectations across the vendor lifecycle. See Shared Assessments and the NIST Privacy Framework and Cybersecurity Framework relationship for governance-oriented risk-management context.

QUESTION NO: 8

A vendor inventory lists a provider as low risk because it does not process personal information. A new integration will allow the provider to use an account to administer the organization's identity platform. What is the MOST appropriate classification action?

A. Reassess inherent risk and classification before privileged access is enabled

B. Retain the low-risk classification because the provider does not process personal information

C. Require only a data-processing addendum before enabling the integration

D. Defer classification review until the next scheduled reassessment

ANSWER: A

Explanation:

The organization should reassess the provider's inherent risk and classification before enabling the integration because privileged administrative access can create significant security and operational exposure independent of personal-data processing. The reassessment should consider the scope and persistence of access, affected systems, authentication methods, monitoring, and the impact of compromise or misuse.

Keeping the existing classification because no personal information is processed would omit a material risk factor. A data-processing addendum may not be relevant to the relationship, and waiting for a future reassessment would allow the risk profile to change without appropriate due diligence.

QUESTION NO: 9

A visual representation of locations, users, systems and transfer of personal information between outsourcers and third parties is defined as:

A. Configuration standard

B. Audit log report

C. Network diagram

D. Data flow diagram

ANSWER: D

Explanation:

Data flow diagram is correct because it graphically documents how personal information moves through an organization's environment and across external relationships. In third-party risk management, this diagram can identify the locations where information is collected, processed, stored, accessed, transmitted, or otherwise handled; the users and systems involved; and the transfers between the outsourcer and its third parties. Mapping these flows gives the organization a practical foundation for understanding its data-processing ecosystem, defining the scope of an assessment, and identifying where privacy, security, contractual, and regulatory controls should apply. It is especially useful for assessing whether sensitive or personal information crosses organizational, geographic, system, or service-provider boundaries and for establishing accountability at each handoff. Shared Assessments materials emphasize the importance of understanding data flows when evaluating third-party services and their associated risks. The U.S. National Institute of Standards and Technology similarly describes data-flow mapping as a means to understand how personally identifiable information is processed throughout a system and its lifecycle. See Shared Assessments and NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.

QUESTION NO: 10

A critical service provider has completed due diligence. The assessment identifies a significant access-review deficiency, but the provider has implemented a compensating control and submitted a remediation plan. Which action is MOST appropriate before the relationship is approved?

A. Calculate the residual risk and obtain risk acceptance or escalation as required by policy

B. Approve the relationship because a remediation plan has been submitted

C. Reject the relationship because any significant finding exceeds inherent risk tolerance

D. Close the finding once the provider documents a compensating control

ANSWER: A

Explanation:

The organization should determine the residual risk after considering the compensating control and remediation plan, then obtain approval at the authority level defined by policy if that residual risk is within tolerance. Inherent risk reflects the exposure created by the service before controls are considered; it does not alone determine whether the relationship can proceed.

Accepting the provider solely because it submitted a plan would not establish whether the remaining exposure is acceptable. Conversely, automatically rejecting the provider or treating the finding as closed would ignore the organization's defined risk-treatment and approval processes. The finding should remain tracked until remediation is validated.

QUESTION NO: 11

Which statement is FALSE when describing the third party risk assessors' role when conducting a controls evaluation using an industry framework?

A. The Assessor ' s role is to conduct discovery with subject matter experts to understand the control environment

B. The Assessor ' s role is to conduct discovery and validate responses from the risk assessment questionnaire by testing or validating controls

C. The Assessor ' s role is to provide an opinion on the effectiveness of controls conducted over a period of time in their report

D. The Assessor ' s role is to review compliance artifacts and identify potential control gaps based on evaluation of the presence of control attributes

ANSWER: C

Explanation:

The Assessor's role is to provide an opinion on the effectiveness of controls conducted over a period of time in their report is the false statement. In a third-party controls evaluation, the assessor performs a structured assessment against defined control criteria drawn from an applicable framework, such as NIST, ISO, COBIT, or COSO. The assessor gathers evidence through discovery discussions, examines relevant artifacts, and validates whether the expected control attributes are present and operating as represented. The resulting report should communicate factual assessment results, evidence-based observations, and identified gaps in an objective manner. It is not an assurance opinion comparable to an independent audit opinion on the effectiveness of controls over a defined period. Maintaining this distinction preserves the assessment's scope, methodology, and independence, while giving the organization useful information for risk decisions and remediation planning. This approach is consistent with NIST's assessment model, which focuses on assessing implemented controls and documenting assessment results, as described in NIST SP 800-53A. Shared Assessments also describes its third-party risk management resources and assessment tools as mechanisms for evaluating third-party controls and risks; see Shared Assessments Resources.

QUESTION NO: 12

Which statement is TRUE regarding a vendor ' s approach to Environmental, Social, and Governance (ESG) programs?

A. ESG expectations are driven by a company ' s executive team for internal commitments end not external entities

B. ESG requirements and programs may be directed by regulatory obligations or in response to company commitments

C. ESG commitments can only be measured qualitatively so it cannot be included in vendor due diligence standards

D. ESG obligations only apply to a company with publicly traded stocks

ANSWER: B

Explanation:

"ESG requirements and programs may be directed by regulatory obligations or in response to company commitments" is correct because a vendor's ESG program can arise from both mandatory external requirements and voluntary organizational priorities. Regulatory developments increasingly require organizations to assess, report, manage, or exercise due diligence over environmental and social impacts in their operations and value chains. These obligations can flow through procurement and third-party relationships when a company needs vendors to provide relevant information, meet contractual standards, or support compliance activities.

At the same time, a company may establish ESG commitments independently of a particular legal mandate. For example, an organization may adopt emissions-reduction goals, supplier conduct standards, human-rights expectations, diversity objectives, or governance principles as part of its corporate strategy, stakeholder commitments, or risk-management framework. It can then incorporate those commitments into vendor selection, due diligence, contracting, monitoring, and remediation processes. This approach reflects the practical connection between ESG and third-party risk management: the vendor's practices may affect the customer's regulatory exposure, reputation, operational resilience, and stated sustainability commitments. The European Commission's overview of corporate sustainability due diligence illustrates the regulatory

dimension of value-chain expectations, while the GRI Standards demonstrate how organizations use structured ESG reporting frameworks: European Commission and GRI Standards.

QUESTION NO: 13

The following statements reflect user obligations defined in end-user device policies

EXCEPT:

A. A statement specifying the owner of data on the end-user device

B. A statement that defines the process to remove all organizational data, settings and accounts at offboarding

C. A statement detailing user responsibility in ensuring the security of the end-user device

D. A statement that specifies the ability to synchronize mobile device data with enterprise systems

ANSWER: D

Explanation:

A statement that specifies the ability to synchronize mobile device data with enterprise systems is the exception because it describes a technical capability or an organization-controlled configuration decision, rather than an action or accountability assigned to an end user. End-user device policies establish the conditions under which devices may access organizational resources and the responsibilities users accept when using those devices. Synchronization with enterprise services is typically enabled, restricted, or managed through mobile-device-management, endpoint-management, access-control, and data-protection configurations. Whether synchronization is allowed can depend on device enrollment, compliance status, operating-system version, encryption, authentication strength, application controls, and the sensitivity of the data involved. Users may be required to comply with synchronization controls, but the mere ability to synchronize is not itself a user obligation. Shared Assessments' third-party risk resources emphasize assessing controls that protect information and systems, including governance and technical safeguards, while endpoint-management guidance distinguishes configuration and compliance settings from end-user responsibilities. See Shared Assessments' Standardized Information Gathering Questionnaire and Microsoft Learn's device-compliance policy guidance.

QUESTION NO: 14

Which statement is FALSE regarding the risk factors an organization may include when defining TPRM compliance requirements?

A. Organizations include TPRM compliance requirements within vendor contracts, and periodically review and update mandatory contract provisions

B. Organizations rely solely on regulatory mandates to define and structure TPRM compliance requirements

C. Organizations incorporate the use of external standards and frameworks to align and map TPRM compliance requirements to industry practice

D. Organizations define TPRM policies based on the company's risk appetite to shape requirements based on the services being outsourced

ANSWER: B

Explanation:

Organizations rely solely on regulatory mandates to define and structure TPRM compliance requirements is false because a sound third-party risk management program uses regulatory obligations as an important input, rather than its only design basis. Compliance requirements must be proportionate to the organization's own risk appetite, business model, outsourced services, information and asset sensitivity, threat environment, contractual commitments, and stakeholder expectations. Regulatory requirements also commonly establish a baseline that must be interpreted and operationalized in the organization's specific environment. A mature TPRM program therefore translates applicable legal and regulatory duties into

risk-based controls, due-diligence activities, contracting requirements, monitoring practices, and escalation processes that address the actual services and relationships in scope. This approach allows requirements to remain effective when a relationship presents material operational, cybersecurity, privacy, resilience, or concentration risk beyond a minimum regulatory obligation. It also supports consistent governance across multiple jurisdictions and evolving third-party arrangements. NIST's supply-chain risk guidance emphasizes integrating risk management practices throughout the organization and its supplier relationships, while Shared Assessments promotes a risk-based, standardized approach to assessing third parties. See NIST SP 800-161 Rev. 1 and Shared Assessments.