Shared Assessments CTPRP Practice Test

Shared by Ruiz on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

When evaluating compliance artifacts for change management, a robust process should include the following attributes:

Options:

A- Approval, validation, auditable.
B- Logging, approvals, validation, back-out and exception procedures
C- Logging, approval, back-out.
D- Communications, approval, auditable.

Answer:

B

Explanation:

Change management is the process of controlling and documenting any changes to the scope, objectives, requirements, deliverables, or resources of a project or a program. Change management ensures that the impact of any change is assessed and communicated to all stakeholders, and that the changes are implemented in a controlled and coordinated manner. Compliance artifacts are the documents, records, or reports that demonstrate the adherence to the change management process and the regulatory or industry standards.

A robust change management process should include the following attributes:

Logging: This means that any change request or proposal is recorded in a change log or a change register, along with the details of the change initiator, the change description, the change category, the change priority, the change status, and the change history. Logging helps to track and monitor the progress and outcome of each change, and to provide an audit trail for compliance purposes.

Approvals: This means that any change request or proposal is reviewed and approved by the appropriate authority or stakeholder, such as the project manager, the sponsor, the customer, the steering committee, or the regulatory body. Approvals help to ensure that the change is justified, feasible, aligned with the project or program objectives, and acceptable to the affected parties.

Validation: This means that any change request or proposal is verified and tested to ensure that it meets the quality standards, the functional and non-functional requirements, and the expected benefits and outcomes. Validation helps to ensure that the change is implemented correctly,

effectively, and efficiently, and that it does not introduce any errors, defects, or risks.

Back-out and exception procedures: This means that any change request or proposal has a contingency plan or a rollback plan in case the change fails, causes problems, or is rejected. Back-out and exception procedures help to minimize the negative impact of the change, and to restore the original state or the baseline of the project or program. They also help to handle any deviations or issues that may arise during the change implementation or the change review.

CTPRP Job Guide

An Agile Approach to Change Management

CM Overview

Management Artifacts and its Types

Achieving Regulatory and Industry Standards Compliance with the Scaled Agile Framework

8 Steps for an Effective Change Management Process

Question 2

Question Type: MultipleChoice

Which statement is FALSE regarding the methods of measuring third party risk?

Options:

A- Risk can be measured both qualitatively and quantitatively
B- Risk can be quantified by calculating the severity of impact and likelihood of occurrence
C- Assessing risk impact requires an analysis of prior events, frequency of occurrence, and external trends to analyze and predict the potential of a particular event happening
D- Risk likelihood or probability is a critical element in quantifying inherent or residual risk

Answer:

C

Explanation:

This statement is false because assessing risk impact does not require an analysis of prior events, frequency of occurrence, and external trends. These factors are relevant for assessing risk likelihood or probability, not impact. Risk impact is the potential consequence or damage

that a risk event may cause to the organization or its stakeholders. Risk impact can be measured qualitatively (e.g., high, medium, low) or quantitatively (e.g., monetary value, percentage of revenue, number of customers affected). To assess risk impact, the organization needs to consider the nature and scope of the risk, the potential harm or loss, and the sensitivity or tolerance of the organization or its stakeholders to the risk.Reference:

How to Manage and Measure Third-Party Risk, OneTrust Blog

Third-party risk, Deloitte

Assessing Risks in Third Parties, ERM - Enterprise Risk Management Initiative

Question 3

Question Type: MultipleChoice

Which cloud deployment model is focused on the management of hardware equipment?

Options:

A- Function as a service
B- Platform as a service
C- Software as a service
D- Infrastructure as a service

Answer:

D

Explanation:

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.Reference:

Cloud Infrastructure: 4 Key Components and Deployment Models

Cloud Deployment Models - GeeksforGeeks

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

Question 4

Question Type: MultipleChoice

When updating TPRM vendor classification requirements with a focus on availability, which risk rating factors provide the greatest impact to the analysis?

Options:

A- Type of data by classification; volume of records included in data processing
B- Financial viability of the vendor; ability to meet performance metrics
C- Network connectivity; remote access to applications
D- impact on operations and end users; impact on revenue; impact on regulatory compliance

Answer:

D

Explanation:

TPRM vendor classification is the process of categorizing vendors based on their criticality, risk level, and service type. Vendor classification helps to prioritize and allocate resources for vendor assessment, monitoring, and remediation. Vendor classification should be updated periodically to reflect changes in the business environment, vendor performance, and regulatory requirements.

When updating TPRM vendor classification requirements with a focus on availability, the risk rating factors that provide the greatest impact to the analysis are the impact on operations and end users, the impact on revenue, and the impact on regulatory compliance. This is because:

Availability is the degree to which a system or service is accessible and functional when required by authorized users. Availability is a key component of information security and business continuity, as it ensures that the business can operate normally and deliver value to its customers and stakeholders.

Impact on operations and end users measures the extent to which a vendor's service disruption or failure affects the business processes, functions, and activities that depend on the vendor's service. A high impact on operations and end users means that the vendor's service is essential

for the business to perform its core functions and meet its objectives, and that any downtime or degradation of the service would cause significant operational delays, inefficiencies, or losses.

Impact on revenue measures the extent to which a vendor's service disruption or failure affects the business's income, profitability, and market share. A high impact on revenue means that the vendor's service is directly or indirectly linked to the business's revenue generation, and that any downtime or degradation of the service would cause substantial financial losses, reduced customer satisfaction, or competitive disadvantage.

Impact on regulatory compliance measures the extent to which a vendor's service disruption or failure affects the business's adherence to the laws, regulations, standards, and contractual obligations that govern its industry, sector, or jurisdiction. A high impact on regulatory compliance means that the vendor's service is subject to strict regulatory requirements, and that any downtime or degradation of the service would cause serious legal penalties, fines, sanctions, or reputational damage.

Therefore, these three factors are the most important to consider when updating TPRM vendor classification requirements with a focus on availability, as they reflect the potential consequences and risks of vendor unavailability for the business.

CTPRP Job Guide

Criticality and Risk Rating Vendors 101

The Third-Party Vendor Risk Management Lifecycle

What Is Third-Party Risk Management (TPRM)? 2024 Guide

Third-Party Risk Management and ISO Requirements for 2022

Question 5

Question Type: MultipleChoice

Which TPRM risk assessment component would typically NOT be maintained in a Risk Register?

Options:

A- An assessment of the impact and likelihood the risk will occur and the possible seriousness
B- Vendor inventory of all suppliers, vendors, and service providers prioritized by contract value
C- An outline of proposed mitigation actions and assignment of risk owner
D- A grading of each risk according to a risk assessment table or hierarchy

Answer:

B

Explanation:

A risk register is a tool that records and tracks the identified risks, their probability, impact, status, and mitigation actions throughout the life cycle of a third-party relationship1.A risk register typically includes the following components2:

A unique identifier for each risk

A description of the risk and its source

A rating or grading of the risk according to a risk assessment table or hierarchy

An assessment of the impact and likelihood the risk will occur and the possible seriousness

An outline of proposed mitigation actions and assignment of risk owner

A status update on the risk and the progress of the mitigation actions

A target date for resolving the risk or closing the action A vendor inventory is a list of all the third parties that a banking organization engages with, along with relevant information such as the type, scope, and nature of the services provided, the contract terms and conditions, the performance indicators, and the risk ratings3. A vendor inventory is not a component of a risk register, but rather a separate document that supports the planning and due diligence phases of the third-party relationship life cycle. A vendor inventory may be prioritized by contract value, but also by other criteria such as the criticality of the service, the risk level of the vendor, and the strategic importance of the relationship.Reference:

1: Third-Party Risk Management (TPRM): Final Interagency Guidance, KPMG, June 2023

2: What Is Third-Party Risk Management (TPRM)? 2024 Guide, UpGuard, January 2024

3: Third-Party Risk Management Guidance, OCC Bulletin 2023-29, October 2023

[4]: Certified Third Party Risk Professional (CTPRP) Study Guide, Shared Assessments, 2023

[5]: Best Practices Guidance for Third-Party Risk, GARP, February 2023

Question 6

Question Type: MultipleChoice

Which statement BEST represents the roles and responsibilities for managing corrective actions

upon completion of an onsite or virtual assessment?

Options:

A- All findings and remediation plans should be reviewed with internal audit prior to issuing the assessment report
B- All findings and remediation plans should be reviewed with the vendor prior to sharing results with the line of business
C- All findings and need for remediation should be reviewed with the line of business for risk acceptance prior to sharing the remediation plan with the vendor
D- All findings should be shared with the vendor as quickly as possible so that remediation steps can be taken as quickly as possible

Answer:

C

Explanation:

According to the Certified Third Party Risk Professional (CTPRP) Job Guide, one of the key tasks of a third party risk professional is to ''manage the corrective action process for identified issues and ensure timely resolution'' (p. 10). This task involves the following steps:

Document the findings and recommendations from the assessment and communicate them to the appropriate stakeholders

Review the findings and recommendations with the line of business (LOB) and obtain their risk acceptance or rejection

If the LOB accepts the risk, document the rationale and approval in the risk register

If the LOB rejects the risk, work with the vendor to develop a remediation plan that addresses the root cause and mitigates the risk

Monitor the progress and completion of the remediation plan and verify the effectiveness of the corrective actions

Update the risk register and the vendor profile with the results of the remediation

Therefore, the statement that best represents the roles and responsibilities for managing corrective actions is C, as it reflects the need to review the findings and need for remediation with the LOB for risk acceptance before sharing the remediation plan with the vendor. This ensures that the LOB is aware of the risks and their impact, and that the vendor is committed to resolving the issues in a timely and satisfactory manner.

CTPRP Job Guide, Shared Assessments, 2020

Best Practices Guidance for Third Party Risk, Global Association of Risk Professionals (GARP), 2019

Simple Guide for Corrective and Preventative Action (CAPA), Qualcy eQMS, 2020

[The Three Key Parts of an EHS Corrective Action Plan], EHS Daily Advisor, 2021