Question 1 of 2

TPA Services, a third-party employee benefit administrator, engaged Marshall Gray, LLP, a CPA firm, to perform a SOC 1® type 1 examination. TPA Services elects to report all subservice organizations using the carve-out method. A staff associate began to prepare the draft report but has questions about the correct wording based on the relevant professional standards.

Amend the paragraphs of the drafted report below as appropriate. Click on each segment of underlined text below and select the needed correction, if any, from the list provided. If the underlined text is already correct in the context of the document, select *[Original text]*. If the underlined text should not be included in the report, select *[Delete text]*.

Drafted report:

Auditor's Report

> **Available Options for Selection 1:**
>
> 1. *[Original text]* Auditor's Report
> 2. *[Delete Text]*
> 3. Independent Service Auditor's Report
> 4. SOC 1® Report
> 5. SOC 1® Type 1 Report

To: User Entities and User Auditors

> **Available Options for Selection 2:**
>
> 1. *[Original text]* To: User Entities and User Auditors
> 2. *[Delete Text]*
> 3. To: Management of TPA Services
> 4. To: Marshall Gray, LLP

Scope

We have examined TPA Services' ("TPA") description of its system, entitled "TPA Services Description of the System," for processing of user entities' transactions throughout the period October 1, Year 1, to September 30, Year 2

("description"), and the suitability of the design and operating effectiveness of TPA Services' controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "TPA Services Management Assertion". The controls and control objectives included in the description are those that management of TPA Services believe are likely to be relevant to internal controls over financial reporting, and the description does not include those aspects of the processing of transactions for user entities that are not likely to be relevant to internal controls over financial reporting.

> **Available Options for Selection 3:**
>
> 1. *[Original text]* throughout the period October 1, Year 1, to September 30, Year 2
> 2. *[Delete Text]*
> 3. as of September 30, Year 2
> 4. for the year ended September 30, Year 2

> **Available Options for Selection 4:**
>
> 1. *[Original text]* suitability of the design and operating effectiveness
> 2. *[Delete Text]*
> 3. operating effectiveness
> 4. suitability of the design

> **Available Options for Selections 5 and 7:**
>
> 1. *[Original text]* control objectives
> 2. *[Delete Text]*
> 3. service commitments and system requirements
> 4. system objectives

> **Available Options for Selection 6:**
>
> 1. *[Original text]* criteria identified in "TPA Services Management Assertion"

2. *[Delete Text]*
3. criteria set forth in DC Section 200, 2018 Description Criteria for a Description of a Service Organization
4. criteria set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, or Privacy

Available Options for Selections 8 and 9:

1. *[Original text]* internal controls over financial reporting
2. *[Delete Text]*
3. security, availability, and privacy
4. security, availability, processing integrity, confidentiality, or privacy
5. user entities' internal control over financial reporting

TPA Services uses the cloud-based Oracle NetSuite accounting system and Oracle Cloud Storage for creating and storing off-site backups. The description includes the control objectives

and related controls of the subservice organizations.

Available Options for Selection 10:

1. *[Original text]* includes the control objectives
2. *[Delete Text]*
3. includes the service commitments and system requirements
4. includes the system objectives
5. excludes the control objectives
6. excludes the service commitments and system requirements
7. excludes the system objectives

Explanation

Background Information

SOC 1® overview

SOC 1®—type 1 vs. type 2—management's assertion and examination scope		
	Type 1	**Type 2**
	As of specified date	Throughou a period
Management's description of the system	✔	✔
Management's written assertion that description fairly presents system	✔	✔
Management's written assertion that the controls related to the control objectives stated in management's description of the system were suitably designed	✔	✔
Report expressing an opinion on management's description of the system and suitability of the design of controls	✔	✔
Management's written assertion that the controls related to the control objectives stated in management's description of the system operated effectively		✔
Report expressing an opinion on management's description of the system, the suitability of the design of controls, and the operating effectiveness of controls		✔
A description of the auditor's tests of controls and the results thereof		✔

SOC 1® engagements are **assertion-based examinations** performed in accordance with AICPA's attestation standards **AT-C 105, AT-C 205, and AT-C 320**. The final step in a SOC engagement is to prepare the service auditor's report and compile the entire SOC report package.

A SOC report package includes separate sections for the service auditor's report, management's assertion, management's description of the system, criteria and controls, and optional information that management wants to include. The contents of a SOC 1® report package depend on the following factors:

- Type of report (type 1, type 2)
- Method used to report subservice organizations (inclusive, carve-out)
- Need to report complementary subservice organization controls (CSOCs)
- Need to report complementary user entity controls (CUECs)

The service auditor's report **must be in writing** and **be signed by a licensed CPA**, such as the engagement partner. Report distribution is restricted to user entities and their auditors (ie, user auditors). In a SOC 1® engagement, the service auditor's report **must also contain specific report elements** as prescribed by AT-C 320.

Response 1: Report Title

Auditor's Report

Correct response: Independent Service Auditor's Report

AT-C §320.41 outlines the elements that must be included in a SOC 1® type 1 service auditor's report. **AT-C §320.41a** requires that the **report title include the word *independent***. AT-C §105.26, the general attestation standard, states, "The practitioner must be independent when performing an attestation engagement in accordance with the attestation standards unless the practitioner is required by law or regulation to accept the engagement."

Service auditors **must be independent of the service organization and any subservice organizations reported using the inclusive method**. Independence is not required for user entities or for any subservice organizations reported using the carve-out method.

To be independent, a service auditor must be free from conflicts of interest, neutral, and fair.

Response 2: Addressee

To: User Entities and User Auditors

Correct response: To: Management of TPA Services

AT-C §320.41b states that a service auditor's report must include "an appropriate addressee as required by the circumstances of the engagement." Typically, the **most appropriate addressee is the engaging party**. In this scenario, the service organization is both the engaging party (ie, the party that hired the CPA) and the responsible party (ie, the party under examination). In other scenarios, the **engaging and responsible parties may differ** (eg, a user entity [engaging party] hires a CPA to perform a SOC examination on a service organization [responsible party]).

"User entities and user auditors" would not be an appropriate addressee unless both groups are engaging parties. Likewise, a CPA firm would not address a service auditor's report to itself.

Response 3: Examination Time Frame

throughout the period October 1, Year 1, to September 30, Year 2

Correct response: as of September 30, Year 2

A SOC 1® engagement can be type 1 or type 2. In a **type 1** engagement, the service auditor examines only management's **description of the service organization's system and the suitability of the design of controls as of a specified date** (eg, as of September 30, Year 2).

Type 2 examinations are performed *throughout a period*, and the service auditor must also test the operating effectiveness of controls. In this scenario, the engaging party has requested a type 1 report, and thus the service auditor's examination includes only the system description and the suitability of the design of controls that existed as of a particular day. The service auditor would not perform tests or express an opinion on the operating effectiveness of controls.

Response 4: Scope of Examination

suitability of the design and operating effectiveness

Correct response: suitability of the design

A SOC 1® engagement can be type 1 or type 2. In a **type 1** engagement, the service auditor examines only management's **description of the service organization's system and the suitability of the design of controls as of a specified date** (eg, as of September 30, Year 2).

Type 2 examinations are performed *throughout a period*, and the service auditor must also test the operating effectiveness of controls. In this scenario, the engaging party has requested a type 1 report, and thus the service auditor's examination includes only the system description and the suitability of the design of controls that existed as of a particular day. The service auditor would not perform tests or express an opinion on the operating effectiveness of controls.

Responses 5 and 7: Service Organization's Objectives

control objectives

Correct response: control objectives

According to the COSO Internal Control—Integrated Framework, **objectives are the aim of management activities** (ie, management's goals). Risks threaten the achievement of objectives, and controls should be designed to mitigate risks.

Management is responsible for specifying objectives in every SOC examination. Because each type of SOC examination evaluates a different subject matter, these objectives are known by different terms. For example, in a **SOC 1®** examination, the correct term is ***control objectives***. The objectives in a SOC 2® examination are called *service commitments and system requirements*. In SOC for Cybersecurity, the objectives are known as *cybersecurity objectives*, and in a SOC for Supply Chain, the objectives are termed *system objectives*.

Thus, in a SOC 1®, the service auditor evaluates whether the controls included in management's system description were suitably designed to achieve the service organization's *control objectives*.

Response 6: Suitable Criteria

criteria identified in "TPA Services Management Assertion"

Correct response: criteria identified in "TPA Services Management Assertion"

Every SOC for Service Organizations (eg, SOC 1®, SOC 2®, SOC 3®) engagement involves measuring or evaluating the subject matter (ie, management's description of the service organization's system and the related controls). Both management and the service auditor **measure or evaluate the subject matter against suitable criteria**.

In a **SOC 1®** examination, the subject matter is measured or evaluated against the **criteria listed in management's assertion**. AT-C 320 provides detailed standards for assessing the suitability of criteria in a SOC 1®. The general standard found in AT-C 105 states that suitable criteria must be *relevant, objective, measurable, and complete*. The **CPA must determine whether such criteria are suitable.**

All SOC examinations other than SOC 1® measure or evaluate the subject matter against description criteria (eg, the AICPA's DC 100, DC 200, DC 300) and control criteria (eg, the AICPA's Trust Services Criteria).

Responses 8 and 9: Report Relevance

internal controls over financial reporting

Correct response: user entities' internal control over financial reporting

SOC 1® reports provide assurance about the service organization's system and controls **relevant to user entities' internal control over financial reporting (ICFR)**. Most SOC 1® examinations are performed on service organizations that process transactions (eg, payroll, payments, claims, loans, investments) on behalf of user entities, as well as on cloud service providers (eg, SaaS). It is important to understand that SOC 1® examinations do not evaluate the controls over the service organization's financial reporting but rather over the *user entities'* financial reporting. The report language must make this clear.

All SOC reports except SOC 1® are relevant to security, availability, processing integrity, confidentiality, or privacy to some degree and may benchmark controls against the Trust Services Criteria (TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, or Privacy*).

Response 10: Subservice Organizations

includes the control objectives

Correct response: excludes the control objectives

As part of its responsibilities in a SOC 1® type 1 examination, management must choose whether to report subservice organizations under the inclusive method or the carve-out method. In this scenario, the service organization elects to use only the carve-out method. In the **carve-out method**, the nature of the subservice organization's services is included in management's system description. However, the description **excludes the subservice organization's objectives and related controls**.

The carved-out subservice organization's controls that are necessary to achieve the service organization's objectives are **listed in a separate section of the report as complementary subservice organization controls (CSOCs)**. The service auditor does not perform any tests on CSOCs and therefore is not required to be independent of carved-out subservice organizations.

Question 2 of 2

Exhibits: "Testing Summary.pdf"

A service auditor is performing a SOC 2®, type 2 examination of a data center's system and controls throughout the period of October 1, 20X1, to September 30, 20X2. Consider the following:

- The engagement team performed tests of controls related to the common and supplemental trust services criteria and submitted testing workpapers to the engagement manager for review.
- While reviewing the team's workpapers, the engagement manager prepared a summary of the tests of controls and results. This summary is in the exhibits above.
- The engagement manager then drafted the table below to describe the service organization's controls, the service auditor's tests of controls, and the results of the service auditor's tests in section 4 of the SOC 2® report.

As the engagement partner reviewing the draft report, consider whether the information disclosed in columns A, B, and C provides sufficient detail to enable report users to understand how the data center's controls affect their own risk assessment. In column D, select the most appropriate review note the engagement partner would write after evaluating the draft report. Each option may be used once, more than once, or not at all.

	A	*B*	*C*	*D*
1	**Service Organization Control**	**Service Auditor Tests of Controls**	**Results of Service Auditor's Tests**	**Engagement Partner Review Notes**
2	CE-2: As part of the new hire process, background checks are performed for new hires.	For a sample of new hires during the audit period, inspected supporting records to determine that a background check was performed as part of the hiring process.	No exceptions noted.	

3	CA-1: On a quarterly basis, management performs external network vulnerability scans. Results are reviewed and, if applicable, remediation is tracked.	For a sample of quarters, determined that management performed quarterly external network vulnerability scans, reviewed the results, and, if needed, tracked remediation tasks.	No exceptions noted.	
4	LA-1: New user access to in-scope systems and data requires management approval prior to provisioning.	For a sample of new users, inspected help-desk tickets to determine that the access request was documented and authorized by management prior to provisioning.	No exceptions noted.	
5	LA-3: Management performs a quarterly review of users with administrative access to the in-scope application to validate that their access is appropriate.	Inspected documentation of management reviews to determine whether management performed the reviews on a quarterly basis and followed up on action items.	No exceptions noted.	
6	CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Inspected a sample of application and system change tickets to determine that the changes were documented, tested, and approved.	Exceptions noted. Four of the 25 sample changes were deployed without approval.	
7	CM-2: In-scope applications have dedicated environments for development, testing, and production.	Observed the existence and use of separate development, testing, and production environments for each in-scope application.	Exceptions noted.	

> **Available Options for 'Engagement Partner Review Notes' (Column D):**
>
> 1. No adjustment necessary because the information is sufficient.

2. Information is insufficient because it does not disclose the control tested.
3. Information is insufficient because it does not disclose whether the test was performed on the full population or a sample.
4. Information is insufficient because it does not disclose the nature of the tests performed.
5. Information is insufficient because it does not disclose the number of items tested.
6. Information is insufficient because it does not disclose the number and nature of deviations.
7. Information is insufficient because it does not disclose the root cause for exceptions.
8. Information is insufficient because it does not disclose who performed the test.

Explanation

Background Information

Service auditor's tests of controls – required disclosures

Information to be described	No deviations identified	Deviations identified
Controls tested	Yes	Yes
Tests performed on the full population or sample	Yes	Yes
Nature of tests performed	Yes	Yes
Number of items tested	No	Yes
Number and nature of deviations	N/A	Yes
Causative factors	N/A	Optional
Test performed by service organization internal audit function and service auditor's work	Optional	Optional

The last step in the SOC engagement process is to prepare the service auditor's report and compile the entire SOC report package. **Section 4** of a **SOC 2® type 2** report package includes a **detailed list of the service organization's controls, as well as the service auditor's tests of controls and the results**, describing any exceptions with sufficient detail.

The description of the service auditor's tests and results provides report users with information necessary to **assess whether the service organization's controls operated effectively** throughout the period. Service auditors should describe the tests and results with **sufficient detail to enable report users to understand how the service organization's controls affect their own risk assessment**. These details should support the service auditor's opinion.

The AICPA's SOC 2® Guide lists the items service auditors must include when describing tests of controls and results. When **deviations** (ie, exceptions) are found, the service auditor must provide **additional information** such as the number of items tested and the number and nature of deviations. The service auditor must **describe all deviations because materialitydoes not apply** to disclosing testing exceptions.

Service auditors may describe causative factors and disclose any work performed by the service organization's internal audit function, but such disclosure is optional.

Control CE-2: New Hire Background Checks

Service Organization Control	Service Auditor Tests of Controls	Results of Service Auditor's Tests	Engagement Partner Review Notes
CE-2: As part of the new hire process, background checks are performed for new hires.	For a sample of new hires during the audit period, inspected supporting records to determine that a background check was performed as part of the hiring process.	No exceptions noted.	**No adjustment necessary because the information is sufficient.**

Based on the testing summary in the exhibit, the service auditor inspected background check records for a sample of new hires. The tests on control CE-2 did not identify any deviations. The draft report appropriately **discloses** the following items **required** when the service auditor does not find any deviations:

Disclosure when no deviations are identified	**Information included in the draft report**

Controls tested	CE-2: Background checks are performed on new hires
Tests performed on the full population or sample	Sample of new hires during the period
Nature of tests performed	Inspected supporting records to determine whether a background check was performed for new hires

Therefore, the description of the service organization's controls, the service auditor's tests of controls, and results is **sufficient**. No other information is required because the service auditor did not identify any deviations.

Control CA-1: Vulnerability Scans

Service Organization Control	Service Auditor Tests of Controls	Results of Service Auditor's Tests	Engagement Partner Review Notes
CA-1: On a quarterly basis, management performs external network vulnerability scans. Results are reviewed and, if applicable, remediation is tracked.	For a sample of quarters, determined that management performed quarterly external network vulnerability scans, reviews the results, and, if needed, tracks remediation tasks.	No exceptions noted.	**Information is insufficient because it does not disclose the nature of the tests performed.**

Based on the testing summary in the exhibit, the service auditor inspected a sample of vulnerability scan results, management reviews, and remediation trackers. The service auditor concluded there were no deviations in the test of control CA-1. However, the draft report is **insufficient** because it **does not describe the nature of the tests performed**, a **required disclosure** when describing controls with no deviations. The following disclosures are required:

Disclosure when no deviations are	Information included in the draft report

identified	
Controls tested	CA-1: External network scans are performed on a quarterly basis; results are reviewed and, if applicable, remediation is tracked
Tests performed on the full population or sample	Sample of vulnerability scans, reviews, and remediation trackers
Nature of tests performed	**Omitted**

To **correct the description**, the service auditor should include the nature of the tests performed (eg, "For a sample of quarters, inspected vulnerability scanning results, management's reviews, and remediation trackers to determine that external network vulnerability scans were performed quarterly, the results were reviewed by management, and remediation tasks were tracked").

Control LA-1: New User Access

Service Organization Control	Service Auditor Tests of Controls	Results of Service Auditor's Tests	Engagement Partner Review Notes
LA-1: New user access to in-scope systems and data requires management approval prior to provisioning.	For a sample of new users, inspected help-desk tickets to determine that the access request was documented and authorized by management prior to provisioning.	No exceptions noted.	**No adjustment necessary because the information is sufficient.**

Based on the testing summary in the exhibit, the service auditor inspected a sample of help-desk tickets and did not identify any deviations in their test of control LA-1. The draft report appropriately **discloses** the following **items required** for controls with no deviations:

Disclosure when no deviations are identified	**Information included in the draft report**

Controls tested	LA-1: New user access requires management approval prior to provisioning
Tests performed on the full population or sample	Sample of new user access
Nature of tests performed	Inspected help-desk tickets for management approval of new users

Service auditors **need only to provide information that is required and applicable**. For example, although second-level managers also approved of some access requests, such information is not required to be disclosed because it is not a part of the control. Therefore, **no adjustment is necessary** because the description of the service auditor's tests of controls and results is **sufficient**.

Control LA-3: Administrator Roles

Service Organization Control	Service Auditor Tests of Controls	Results of Service Auditor's Tests	Engagement Partner Review Notes
LA-3: Management performs a quarterly review of users with administrative access to the in-scope application to validate that their access is appropriate.	Inspected documentation of management reviews to determine whether management performed the reviews on a quarterly basis and followed up on action items.	No exceptions noted.	**Information is insufficient because it does not disclose whether the test was performed on the full population or a sample.**

Based on the testing summary in the exhibit, the service auditor inspected documentation of management reviews of administrator user access and did not identify any deviations in their test of control LA-3. However, the draft report **does not indicate whether the tests were performed on the full population or a sample**, a required disclosure for controls with no deviations. The following disclosures are required:

Disclosure when no deviations are identified	Information included in the draft report
Controls tested	LA-3: Management performs a quarterly review of users with administrative access
Tests performed on the full population or sample	**Omitted**
Nature of tests performed	Inspection documentation of quarterly administrator access reviews

Therefore, **the information included is insufficient**. To correct the description, the service auditor must indicate whether the tests were performed on the full population or a sample (eg, "For a sample of quarters, inspected documentation of management reviews of administrator access to determine whether management performed the reviews on a quarterly basis and followed up on action items").

Control CM-1: Change Approvals

Service Organization Control	Service Auditor Tests of Controls	Results of Service Auditor's Tests	Engagement Partner Review Notes
CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Inspected a sample of application and system change tickets to determine that the changes were documented, tested, and approved.	Exceptions noted. Four of the 25 sample changes were deployed without approval.	**Information is insufficient because it does not disclose the control tested.**

Based on the testing summary in the exhibit, the service auditor identified deviations in 4 of 25 sample change tickets inspected. However, the **draft report described the applicable criteria rather than the control tested** by the service auditor, a required disclosure. The following disclosures are required when a service auditor identifies a deviation:

Disclosure when deviations are identified	Information included in the draft report
Controls tested	**Omitted**
Tests performed on the full population or sample	Sample of changes
Nature of tests performed	Inspected application and system change tickets
Number of items tested	25 out of a population of 400
Number and nature of deviations	4 of the sampled changes were deployed without approval

Therefore, the information on the table is **insufficient** because the **service organization control is not disclosed**. The corrected description of the control tested would be "CM-1: Application and system changes are documented, tested, and approved."

Control CM-2: IT Environments

Service Organization Control	Service Auditor Tests of Controls	Results of Service Auditor's Tests	Engagement Partner Review Notes
CM-2: In-scope applications have dedicated environments for development, testing, and production.	Observed the existence and use of separate development, testing, and production environments for each in-scope application.	Exceptions noted.	**Information is insufficient because it does not disclose the number and nature of deviations.**

Based on the testing summary in the exhibit, the service auditor identified deviations in 2 of the 5 in-house applications The draft report does not describe **the number and nature of deviations**, a **required disclosure** for controls with deviations. The draft description included the following:

Disclosure when no deviations are identified	Information included in the draft report
Controls tested	CM-2: Applications use different change environments (D8580)

Tests performed on the full population or sample	Full population
Nature of tests performed	Observed the existence and use of separate development, testing, and production environments
Number of items tested	5 out of 5
Number and nature of deviations	**Omitted**

Therefore, the information is **insufficient** because the number and nature of deviations are not disclosed. **To correct the description**, the table should state "Exceptions noted. A testing environment was not available for 2 of the 5 in-house applications."