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

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.