secureframe

# SOC 2® Type 2 Report Example

Report on [Company Name]'s Description of the [System Name] and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to [TRUST SERVICES CRITERIA] Throughout the Period [Start Date] to [End Date]

*Note: This example is based on the Illustrative SOC 2® Type 2 Report provided by the AICPA as well as a report template created by one of our trusted audit partners.*

*Like the AICPA's example, this is nonauthoritative and provided only for informational purposes to show how a service organization may organize and present the information required by DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022).*

*For brevity's sake, this example does not include all information that might be described in an actual report. For instance, you will only see four sections in this example. Some SOC 2 Type 2 reports may include a fifth section if the service organization wishes to include additional information, such as future plans for new systems, qualitative information such as marketing claims, or responses from management to deviations identified by the service auditor. Section III also does not include everything that might be described in the description of a service organization's system for brevity's sake.*

# Table of Contents

# Section I: Independent Service Auditor's Report

To the Management of [Company Name],

## Scope

We have examined [Company Name]'s accompanying description of its [System Name] titled "[Company Name] Description of Its [System Name]" throughout the period [Start Date] to [End Date], based on the criteria for a description of a service organization's system in DC Section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period [Start Date] to [End Date], to provide reasonable assurance that [Company Name]'s service commitments and system requirements were achieved based on the trust services criteria relevant to [applicable trust services criteria] set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

[Company Name] uses the [Subservice Organization] described in the [Subservice Organization] subsection of Section III. The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at [Company Name], to achieve [Company Name]'s service commitments and system requirements based on the applicable trust services criteria. The description presents [Company Name]'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of [Company Name] controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

## Service Organization's Responsibilities

[Company Name] is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that [Company Name]'s service commitments and system requirements were achieved. [Company Name] has provided the accompanying assertion titled "[Company Name] Management Assertion" (assertion) about the description and the suitability of design and operating effectiveness of controls described therein. [Company Name] is also responsible for:

- Preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion;
- Providing the services covered by the description;

- Selecting the applicable trust services criteria and stating the related controls in the description; and
- Identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

## Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

## Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

## Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in Section IV.

## Opinion

In our opinion, in all material respects—

a. The description presents [Company Name]'s [System Name] that was designed and implemented throughout the period [Start Date] to [End Date], in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period [Start Date] to [End Date] to provide reasonable assurance that [Company Name]'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the [Subservice Organization] and user entities applied the complementary controls assumed in the design of [Company Name] controls throughout that period.
c. The controls stated in the description operated effectively throughout the period [Start Date] to [End Date] to provide reasonable assurance that [Company Name]'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of [Company Name] controls operated effectively throughout that period.

## Restricted Use

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of [Company Name], user entities of [Company Name]'s [System Name] during some or all of the period [Start Date] to [End Date], business partners of [Company Name] subject to risks arising from interactions with the [System Name], practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

[Service auditor's signature]
[City and state where the report is issued]
[Date of the service auditor's report]

# Section II: [Company Name]’s Management Assertion

[Company Name’s Letterhead]
Date: [Report Date]

We have prepared the accompanying description titled “[Company Name]’s Description of the [System Name]” for the period [Start Date] to [End Date], based on the criteria set forth in DC Section 200, 2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report, in AICPA Description Criteria (description criteria). This description is intended to provide report users with relevant information about [Company Name]’s [System Name], particularly concerning system controls designed, implemented, and operated to provide reasonable assurance that [Company Name]’s service commitments and system requirements were achieved in line with the trust services criteria related to [applicable trust services criteria] as outlined in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

[Company Name] uses a subservice organization to [describe subservice's role in the system]. The description outlines the complementary subservice organization controls that are suitably designed and operating effectively. These are necessary alongside the controls at [Company Name] to meet service commitments and system requirements in line with the relevant trust services criteria. However, the description does not disclose the subservice organization’s controls.

To the best of our knowledge and belief, we confirm that:

- The description presents [Company Name]’s [System Name] as it was designed and implemented throughout the period [Start Date] to [End Date], in accordance with the description criteria.
- The controls stated in the description were suitably designed throughout the period [Start Date] to [End Date], to provide reasonable assurance that [Company Name]’s service commitments and system requirements were achieved based on the applicable trust services criteria, provided that the controls operated effectively, and the complementary subservice organization controls worked as assumed in the design.
- The controls stated in the description operated effectively throughout the period [Start Date] to [End Date], providing reasonable assurance that [Company Name]’s service commitments and system requirements were met based on the applicable trust services criteria, if the complementary subservice organization controls assumed in the design of [Company Name]’s controls operated effectively during the same period.

# Section III: [Company Name]’s Description of the System

## Overview of the [Company Name] and Types of Services Provided

[At least one paragraph providing a high-level company overview]

This description details the [System Name] and the related policies, procedures, and control activities for the [System Name]. This description does not include any other services or policies, procedures, and control activities at any subservice organizations.

## Principal Service Commitments and System Requirements

[Company Name] designs its processes and procedures related to the [System Name] to meet its objectives for its [Types of Services]. Those objectives are based on the service commitments that [Company Name] makes to its customers, business partners, vendors, and subservice organizations and the operational and compliance requirements that [Company Name] has established for the services. Service commitments are declarations made by management to its customers regarding the performance of the [System Name]. Service commitments are set forth in standardized contracts, service level agreements, and in the description of the service offering provided online and include the following:

- [Bullet points detailing service commitments]

[Company Name] has established system requirements, which are communicated via service agreements and consist of the following:

- [Bullet points detailing system requirements]

## Components of the System Used to Provide the Services

The system described herein is bounded by the specific aspects of [Company Name]’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers and the data that is processed by the system.

The components that directly support the services provided to user entities are as follows:

### Infrastructure

The [System Name] is comprised of the following components:

| Component | Description | Location |
|---|---|---|
| Firewall | Firewall systems are in place to filter unauthorized inbound network traffic from the internet. | US |
| | | |

## Software

The software component consists of the applications, programs, and other software that support the system. The list of software and ancillary software used to build, support, secure, maintain, and monitor the system are as follows:

| Software Name | Function |
|---|---|
| Developer platform | Source code repository, version control system, and build software |
| | |

## Data

Data consists of transaction streams, files, databases, tables, and output utilized or processed by the system.

All data that is managed, processed and stored as a part of the [System Name] is classified as per the Data Classification Policy which establishes a framework for categorizing data based on its sensitivity, value, and criticality to achieving the objectives of the organization.

Further, all customer data is treated as confidential. The availability of this data is also limited by job function. All customer data storage and transmission follow industry-standard encryption. The data is also regularly backed up as documented in the Data Backup Policy.

## People

The following functional key areas/groups are responsible for planning, directing, and controlling operations:

[Organizational chart, table, or list outlining key areas of authority and responsibility]

## Policies

[Company Name] has implemented the following policies, which serve as the basis for Company procedures. These are made accessible to all relevant employees and contractors, and are reviewed annually:

- [Bullet points listing policies with a brief description]

# Applicable Trust Services Criteria and the Related Controls

## Control Environment

### Management Philosophy and Tone at the Top

The control environment of [Company Name] reflects the philosophy and commitment of senior management to maintaining a secure, confidential, and available system that meets the company's service commitments and trust services criteria. Executive leadership and the Security Steering Committee oversee security initiatives, meeting at least quarterly and reporting to the board annually. This committee establishes security policies and controls to protect confidential information and ensure compliance, emphasizing the importance of security throughout the organization. Resources and personnel are dedicated to implementing, maintaining, and improving these controls in alignment with [Company Name]'s operational objectives.

### Integrity and Ethical Values

Integrity and ethical values form a foundational part of [Company Name]'s control environment, influencing all aspects of its system design, operations, and oversight. Executive management demonstrates a commitment to these values by setting an example and enforcing behavioral standards through a Code of Conduct. All personnel are required to acknowledge the Code upon hiring and review it annually. This code underscores ethical expectations and behavior standards, providing clear guidelines for integrity and professional conduct. Disciplinary measures are in place for any violations of information security policies, ensuring adherence to established ethical principles.

### Organizational Structure and Roles

[Company Name] has a formalized organizational structure, reflected in an organizational chart that details positions of authority, lines of communication, and reporting responsibilities. This structure ensures accountability in overseeing the design, implementation, and monitoring of system controls. Roles related to information security and other trust services criteria are clearly outlined in job descriptions and further defined in the Information Security Policy, promoting clarity and consistency in personnel responsibilities.

### New Personnel and Ongoing Training

To foster a culture of security awareness, [Company Name] requires new hires to complete background checks, sign confidentiality agreements, and acknowledge their obligations under the Code of Conduct. Personnel also undergo training upon hiring and receive annual refreshers on topics critical to maintaining information security. This training includes the appropriate use of system resources, handling of confidential data, and responding to security incidents. Additionally, training records are maintained to track compliance and reinforce [Company Name]'s commitment to a secure and compliant environment.

### Policy Violations and Escalation Procedures

[Company Name] has established procedures for reporting and addressing policy violations. Workforce members are encouraged to report any noncompliance issues to designated supervisors or the Security Officer, with protections against retaliation for reports made in good faith. Reported incidents are investigated thoroughly, and if a violation is confirmed, corrective disciplinary actions are applied. This proactive stance reinforces the organization’s dedication to upholding security policies and maintaining the integrity of its control environment.

## Information and Communication

Effective information and communication are foundational to [Company Name]'s control system, ensuring timely and relevant information is captured, processed, and communicated across the organization. This process supports [Company Name]'s key operations by capturing essential data from transactions, security systems, and interactions with clients, employees, and external stakeholders.

[Company Name] provides detailed information on its systems and services via internal documentation and its public website, ensuring transparency for internal and external stakeholders. Communication channels include [Tool Name], which allows personnel and users to report concerns related to [applicable trust services criteria]. Any reported issues are addressed per the Security Incident Response Plan. Policies like the Change Management Policy and Security Incident Response Plan outline communication protocols for significant events, such as system updates, incidents, or unauthorized disclosures.

## Risk Management

The risk management framework at [Company Name] identifies, assesses, and addresses risks relevant to the organization’s operational and security objectives. The Chief Risk Officer (CRO) oversees risk management activities and ensures alignment with the organization’s risk appetite and strategic goals. Regular risk assessments are conducted across all departments to evaluate the evolving risk landscape and identify areas for improvement. Risks identified in assessments are addressed through policies, controls, or process modifications to prevent potential incidents, data loss, or system unavailability.

Risk monitoring is supported by documented policies that provide guidance for high-priority areas, including data protection, user access, and incident response. These policies are reviewed periodically to ensure they remain relevant and effective in mitigating risks.

## Monitoring Activities

Monitoring controls are embedded within [Company Name]'s processes to verify that all operational and security controls are functioning as designed. The responsibility for monitoring lies with both line management and the Internal Control group, which reports to the CRO. Monitoring activities include:

- Periodic review of key control metrics that are tracked and reported automatically where feasible.
- Regular staff and departmental meetings to review operational and control metrics and identify areas for corrective action.
- Quarterly control self-assessments by functional departments to evaluate control effectiveness and address any deficiencies.

The Internal Control group consolidates monitoring outcomes, and the CRO presents them quarterly to the Management Committee. Independent evaluations by the internal audit team supplement these activities, assessing the adequacy of controls, testing their effectiveness, and providing recommendations for improvements.

## Control Activities

Control activities within [Company Name] are implemented to ensure that objectives regarding system security, data confidentiality, and operational availability are achieved. These activities include policies, procedures, and mechanisms to support access control, change management, vulnerability management, and incident response.

### Access Control

Access control measures at [Company Name] safeguard information systems from unauthorized access. All system access is governed by an Access Control Policy, which outlines user authentication, authorization, and privilege management procedures. Role-based access is enforced, limiting system access based on job responsibilities. New hires and internal transfers are required to have their access rights reviewed to confirm alignment with their roles, and access is removed promptly upon employee termination or role change.

Quarterly access reviews are conducted by managers to verify that access permissions remain consistent with employee responsibilities, and any necessary changes are addressed. User access is continuously monitored for unusual activity through automated security information and event management (SIEM) alerts.

### Change Management

The Change Management Policy at [Company Name] governs the process for implementing changes to systems and applications. This policy ensures that changes are documented, tested, reviewed, and approved before being deployed. Any change that could impact system security or operations must go through a formal review process, including risk assessment, to prevent disruptions or unintended consequences.

Changes are tested in a controlled environment to evaluate their effectiveness and potential impact on system stability. Once approved, changes are communicated to relevant stakeholders, and any necessary training or documentation updates are provided to affected personnel. A post-change review is conducted to confirm successful implementation and identify any follow-up actions.

### Vulnerability Management

[Company Name] implements a proactive vulnerability management program that includes regular scanning, patch management, and periodic penetration testing. The vulnerability management process follows these steps:

- **Scanning**: Automated vulnerability scans are run weekly to identify potential weaknesses in the system.
- **Patch Management**: Patches are prioritized and applied based on risk level, with critical patches implemented as soon as possible.
- **Penetration Testing**: External experts conduct penetration tests at least annually to identify and address security gaps.
- **Reporting and Remediation**: Results from scans and tests are documented, and remediation activities are tracked until resolved.

Quarterly reports are generated to track the status of vulnerability remediation, and findings are presented to the CRO and senior management for review.

### Incident Response

[Company Name] maintains a robust Incident Response Plan (IRP) to ensure that any security incidents are promptly identified, contained, and resolved. The IRP outlines procedures for the detection, documentation, escalation, and resolution of incidents. Incident response activities include:

#### Identification

The identification phase involves promptly detecting potential security incidents to mitigate impact and begin the response process.[Company Name] uses automated monitoring systems, such as a Security Information and Event Management (SIEM) solution, which generates alerts for any suspicious activity, anomalies, or potential threats within the

environment. Additionally, employees and third parties can report incidents through established communication channels.

During this phase, security analysts at[Company Name] assess the alerts and reports to determine if an incident has occurred. Once confirmed, the incident is categorized by severity, type, and potential impact to prioritize response efforts. Incident identification logs are documented and reviewed by the incident response team, who initiate further actions according to the IRP.

### Containment

Containment aims to limit the impact of the incident and prevent its spread while maintaining system stability.[Company Name] employs two levels of containment:

- Short-term Containment: Immediate actions are taken to isolate affected systems, restrict access to compromised accounts, and prevent further damage. Short-term containment measures may include disconnecting impacted devices from the network, revoking credentials, and enabling firewall rules to block malicious traffic.
- Long-term Containment: After short-term containment, long-term actions are implemented to create a stable environment for incident investigation and remediation. This may include setting up temporary environments or using secure backups to maintain business operations while resolving the incident.

Containment efforts are continuously monitored, with logs documenting all actions taken, and the incident is escalated if necessary.[Company Name] management is updated regularly on containment status.

### Eradication

In the eradication phase, the root cause of the incident is identified and addressed to prevent recurrence. Security analysts at[Company Name] analyze compromised systems, investigate vulnerabilities exploited by attackers, and remove any malicious code or artifacts from the environment. Common eradication measures include:

Patching known vulnerabilities or applying configuration changes.
Removing malware, rogue accounts, and unauthorized software from the systems.
Enhancing security settings to prevent similar incidents in the future.
All eradication activities are logged, and affected personnel are informed about any operational or policy adjustments resulting from the incident.

### Recovery

In the recovery phase, [Company Name] implements measures to restore systems and data to normal operations following the containment and eradication of the incident. This phase is

designed to ensure that all affected assets are returned to a secure state, and business processes can resume without additional risk of compromise.

Key steps in the recovery process include:

1. **System Restoration**: After verifying that the threat has been fully eradicated, impacted systems are restored from clean, trusted backups. Recovery processes are executed in alignment with the organization's Business Continuity and Disaster Recovery (BCDR) plans to ensure minimal downtime and data integrity.
2. **System Validation**: After restoration, [Company Name] conducts comprehensive testing and validation of restored systems to confirm that all security controls are functioning as expected. This includes verifying patches, configurations, and updates applied during the eradication phase.
3. **User Access Restoration**: Access to systems, applications, or data that was restricted during containment is re-enabled for authorized users following successful validation of the system's security posture.
4. **Post-Incident Monitoring**: Enhanced monitoring of the affected systems and networks is conducted for a defined period to detect any signs of recurring issues or vulnerabilities related to the initial incident. Monitoring helps verify that systems remain secure post-recovery.
5. **Documentation and Review**: Recovery activities, findings, and lessons learned are documented to improve future incident response efforts. The incident response team conducts a post-recovery analysis to assess what worked effectively and what needs improvement, feeding these insights into future response and recovery planning.

By following these recovery steps, [Company Name] ensures resilient operations and builds stronger defenses to mitigate the impact of potential future incidents.
Testing

The IRP is tested semi-annually to ensure its effectiveness, with adjustments made based on test results to continuously improve incident response capabilities.

## Complementary User Entity Controls

The following user entity controls are assumed to be implemented by user entities and are necessary for the service organization's service commitments and system requirements to be achieved.

| User Entity Control | Relevant Criteria |
|---|---|
| User entities have policies and procedures that require reporting any material changes to their control environment that may adversely affect the ability of ABC to deliver service. | CC2.1 |
| | |

## [Subservice Organization]

The services provided by XYZ Cloud Hosting, a subservice organization, are outside the scope of this report. However, [Company Name] management assumes that complementary subservice organization controls (CSOCs) are implemented effectively. These are detailed in the table below.

| [Subservice Organization] | Services Provided | Complementary User Entity Controls |
|---|---|---|
| ABC Company | [Description] | The subservice organization performs periodic vulnerability assessments (CC 3.2). |
| | | |

## System Incidents

During the reporting period from [Start Date] to [End Date], no significant system incidents were identified that affected the effectiveness of the controls in place or resulted in the failure to achieve service commitments.

## Significant Changes to the [System Name]

There were no changes during the reporting period that would likely affect users' understanding of the system's operational effectiveness or service delivery from [Start Date] to [End Date].

# Section IV: Trust Services Criteria, Related Controls, and Tests of Controls

## Trust Services Criteria and Related Controls for Systems and Applications

[Company Name] has designed and implemented controls to ensure that its service commitments and system requirements are consistently met. These controls are presented below and are integral to the description of the [System Name] throughout the period from [Start Date] to [End Date]. Controls are mapped to each applicable Trust Services Criteria and organized by criteria area, with unique control numbers assigned to align with the relevant criteria.

## Procedures for Assessing Completeness and Accuracy of Information Provided by the Entity (IPE)

For tests of controls requiring the use of IPE (e.g., controls requiring system-generated populations for sample-based testing), [Auditor Name] performed a combination of the following procedures where possible based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

- inspect the source of the IPE,
- inspect the query, script, or parameters used to generate the IPE,
- mapping data between the IPE and the source, and/or
- inspect the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

In addition to the above procedures, for tests of controls and system controls based on Trust Services Criteria requiring management's use of IPE in the execution of the controls (e.g., periodic reviews of user access listings), [Auditor Name] inspected management's procedures to assess the validity of the IPE source and the completeness, accuracy, and integrity of the source data or inputs.

## Testing Methods

The following methods were employed in testing the operating effectiveness of the controls:

- **Inquiry**: The service auditor conducted interviews with management, operations, administrative and other relevant personnel who are responsible for developing, ensuring adherence to and applying controls
- **Observation**: The service auditor observed the application of control activities by the service organization's personnel to validate implementation.
- **Inspection**: The service auditor inspected source documents, reports, system configurations, and other items as necessary to confirm the performance of specified control activities.
- **Re-performance**: The service auditor independently executed procedures or controls originally performed by the service organization to validate their effectiveness.

## Controls without an Occurrence in the Examination Period

Certain controls within [Company Name]'s control set are performed on an as-needed basis and are triggered by specific events. If the underlying event did not occur during the examination period, the service auditor indicated procedures performed to validate that the underlying event did not occur.

## [Company Name]'s Controls

In the following table, the [applicable trust services criteria] criteria and the related control activities have been specified by, and are the responsibility of [Company Name]:

| Criteria Area | Reference # | Supporting Control Activity | Criteria Description |
|---|---|---|---|
| CC1.0 | CC1.1 | Entity establishes behavioral standards which are defined in the Code of Business Conduct and makes it available to all staff members on the company intranet | COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. |
| | | | |

## Tests of Controls and Results

The following table outlines the tests of controls and the results thereof in relation to the control activities specified above.

| Control Number | Control Activity | Criteria Mapping | Service Auditor's Tests | Results of Tests |
|---|---|---|---|---|
| CC3.3.1 | Entity considers the potential for fraud when assessing risks. This is an entry in the risk matrix. | COSO Principle 8 | Observed the risk matrix records. | No exceptions noted. |
| | | | | |