bright defense

# SOC 2 Type 2 Report Example

This report presents an independent examination of XYZ Company's description of the [System Name] and an assessment of whether the related controls were suitably designed and operated effectively in accordance with the applicable Trust Services Criteria throughout the period from [Start Date] to [End Date], as specified in the report documentation

# SOC 2 Type 2 Report for XYZ Company

## Outline

# Section I – Independent Service Auditor's Report

## Scope of Examination

The independent service auditor was engaged to evaluate **XYZ Company's** description of its **[System Name]** for the period **[Start Date]** through **[End Date]**. The objective of the examination was to determine whether the description conforms to the *Description Criteria* established in DC Section 200, 2018 **Description Criteria for a Description of a Service Organization's System in a SOC 2® Report** and to assess whether the controls described were suitably designed and operated effectively to meet the Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. The auditor reviewed policies, procedures, and control activities and evaluated whether the system description included all relevant aspects of the environment that support the services provided.

## Service Organization's Responsibilities

XYZ Company's management bears full responsibility for the completeness and accuracy of the system description, for designing, implementing, and operating effective controls, and for achieving service commitments and system requirements. Management must:

1. Prepare the description and the assertion in accordance with the Description Criteria, ensuring that it accurately reflects the system as designed and implemented throughout the period.

2. Provide the services described, including maintaining appropriate infrastructure, software, people, processes, and data management activities necessary to deliver the services.

3. Select the applicable Trust Services Criteria relevant to its operations and state the corresponding controls in the description.

4. Identify risks that threaten the achievement of service commitments and system requirements, and design controls to address those risks.

In short, XYZ Company must ensure the system description is complete and accurate and that the controls described are both suitable and operating effectively.

## Service Auditor's Responsibilities

The service auditor's responsibility is to express an opinion on the fairness of the description and the suitability of the design and operating effectiveness of controls. The auditor performed procedures to obtain reasonable assurance that:

- The description was prepared in conformity with the Description Criteria and presents the system accurately.

- The controls were suitably designed to provide reasonable assurance that the company's service commitments and system requirements would be achieved if the controls operated effectively throughout the period and if complementary controls at subservice organizations and user entities were in place.

- The controls operated effectively during the period to achieve the service commitments and system requirements.

To meet these objectives, the auditor planned and performed tests in accordance with AICPA attestation standards, which require independence, professional judgment, and obtaining sufficient appropriate evidence. Evidence was gathered through inquiry, observation, inspection of documents and reports, and re-performance of control activities.

## Inherent Limitations and Projection to Future Periods

Internal control systems, by their nature, have inherent limitations. Even with effective design and implementation, controls may fail due to human error, purposeful circumvention, or changing circumstances. Additionally, controls that are effective today may become inadequate in the future because of changes in business processes, information technology, or regulatory requirements. Therefore, conclusions about the suitability and operating effectiveness of controls apply only to the specified period and do not guarantee that controls will remain effective beyond that period.

## Description of Tests of Controls

The specific controls tested, along with the nature, timing, and results of the tests, are detailed in Section IV of this report. The auditor selected controls based on their relevance to the Trust Services Criteria and the risks they were designed to address. Tests included reviews of documentation, sample examination of transactions, observation of processes, and re-performance of procedures. The results of those tests support the opinion expressed below.

## Opinion

Based on the evidence obtained, the service auditor concludes that, in all material respects:

1. **Presentation of Description:** The description presents XYZ Company's **[System Name]** as it was designed and implemented throughout the period **[Start Date]** to **[End Date]**, in accordance with the Description Criteria.

2. **Suitability of Design:** The controls described were suitably designed throughout the period to provide reasonable assurance that XYZ Company's service commitments and system requirements would be achieved, assuming complementary user entity and subservice organization controls were in place.

3. **Operating Effectiveness:** The controls described operated effectively throughout the period to provide reasonable assurance that XYZ Company's service commitments and system requirements were met, again assuming that the complementary controls at the subservice organization and user entities

functioned as expected.

## Restricted Use

This report, including the description of tests of controls and results, is intended solely for the information and use of XYZ Company, user entities of the system during the period, business partners subject to risks arising from interactions with the system, practitioners providing services to those users, prospective user entities, and relevant regulators. The report is not intended for use by anyone other than these specified parties. Only users who understand the nature of the services, how the system interacts with user entities and subservice organizations, and the applicable Trust Services Criteria should rely on this report.

# Section II – XYZ Company's Management Assertion

## Management's Statement

On **[Report Date]**, XYZ Company's management prepared the accompanying description titled "XYZ Company's Description of the **[System Name]**" for the period **[Start Date]** to **[End Date]**. The description was prepared using the DC Section 200 Description Criteria. The description provides users with relevant information about the system and its controls designed to provide reasonable assurance that service commitments and system requirements were achieved in accordance with the applicable Trust Services Criteria.

XYZ Company uses one or more subservice organizations to provide components of the service. The description includes the complementary subservice organization controls (CSOCs) assumed in the design of XYZ Company's controls but does not disclose the details of the subservice organization's controls. XYZ Company management attests to the following assertions:

1. **Completeness of Description:** The description presents the **[System Name]** as it was designed and implemented throughout the period and conforms to the Description Criteria.

2. **Design of Controls:** The controls described were suitably designed as of **[Start Date]** and continued to be suitably designed through **[End Date]** to provide reasonable assurance that service commitments and system requirements would be achieved, provided the controls operated effectively and the complementary subservice organization controls functioned as assumed.

3. **Operating Effectiveness of Controls:** The controls described operated effectively throughout the period to provide reasonable assurance that service commitments and system requirements were achieved, assuming complementary subservice organization controls operated effectively.

Management acknowledges its responsibility for the accuracy and completeness of the description and the design and operation of the controls described. It affirms that the controls were designed and operated to provide reasonable assurance that service commitments and system requirements related to Security, Availability, Processing Integrity, Confidentiality, and Privacy were met.

# Section III – XYZ Company's Description of the System

## Company Overview and Services Provided

XYZ Company is a technology-driven service organization that provides **[Types of Services]** to its customers across various industries. Its mission is to deliver reliable, secure, and scalable solutions that enable clients to manage and process data efficiently. XYZ Company has been in operation for over a decade and has built a reputation for strong internal controls, data protection, and customer service. The primary service offering covered by this report is the **[System Name]**, a platform that manages customer data, processes transactions, and provides analytics and reporting capabilities. The system is hosted in secure data centers and cloud environments, leveraging modern technology stacks and industry best practices for security and compliance.

XYZ Company's service model is subscription-based, with customers accessing the **[System Name]** via secure web interfaces or APIs. The company also offers professional services to assist with implementation, customization, and ongoing support. The scope of this description is limited to the **[System Name]** and does not include other services or products that XYZ Company may offer.

## System Boundaries and Exclusions

The description focuses on the system components, policies, procedures, and control activities that directly support the **[System Name]**. Components or controls managed entirely by subservice organizations are outside the scope, except for the complementary controls that XYZ Company assumes are implemented by those subservice organizations. Controls related to physical facilities, such as data center access managed by colocation providers, are described only to the extent that XYZ

Company relies on them but are not included in testing. The description also excludes any internal processes unrelated to the **[System Name]**.

## Principal Service Commitments and System Requirements

XYZ Company makes specific commitments to its customers, business partners, vendors, and subservice organizations regarding the performance of the **[System Name]**. These commitments are formalized in contracts, service level agreements (SLAs), and publicly available documentation. Service commitments typically include:

- **Availability:** Ensuring that the **[System Name]** is available to users with a guaranteed uptime (e.g., 99.9%) during defined hours of operation. XYZ Company commits to maintaining redundant systems and disaster recovery capabilities to minimize downtime.

- **Security:** Protecting customer data from unauthorized access through the implementation of robust authentication, authorization, and network security controls. XYZ Company pledges to use industry-standard encryption for data in transit and at rest, and to maintain a secure development lifecycle.

- **Processing Integrity:** Processing data completely, accurately, and timely according to client instructions. This includes validation of inputs and outputs, ensuring proper system configuration, and performing regular integrity checks.

- **Confidentiality:** Treating customer data as confidential and limiting access to authorized personnel. XYZ Company commits to implementing access controls, data classification, and data retention policies that safeguard sensitive information.

- **Privacy:** Collecting, using, retaining, and disposing of personal information in accordance with applicable privacy laws and contractual obligations. XYZ Company commits to transparent privacy practices and respects data subject

rights.

To meet these commitments, XYZ Company has established system requirements communicated through service agreements and internal policies. System requirements include:

- Maintaining documented policies and procedures that support security, availability, processing integrity, confidentiality, and privacy.

- Implementing technical controls such as firewalls, intrusion detection/prevention systems, encryption, multi-factor authentication, and secure coding practices.

- Performing regular risk assessments, vulnerability scans, penetration tests, and independent audits to identify and remediate weaknesses.

- Providing training and awareness programs for employees and contractors to ensure they understand their roles and responsibilities related to system security and compliance.

- Establishing incident response, business continuity, and disaster recovery plans to ensure timely detection, containment, and restoration in the event of an incident.

- Engaging subservice organizations with appropriate security and compliance controls and verifying that those controls align with XYZ Company's requirements.

These commitments and requirements guide the design and operation of controls within the **[System Name]**.

## System Components

The system supporting the services provided by XYZ Company consists of multiple components working together to deliver secure and reliable services. The principal components include infrastructure, software, data, and people. A high-level overview of these components is provided below.

| Component | Description | Location |
|---|---|---|
| **Firewalls and Network Security** | Hardware appliances and software configurations that monitor and control incoming and outgoing network traffic based on predetermined security rules. Firewalls filter unauthorized traffic and prevent common attacks such as denial of service and port scanning. Additional network security measures include intrusion detection/prevention systems (IDS/IPS) and secure virtual private networks (VPNs). | Primary and secondary data centers located in the United States and backup locations in other regions |
| **Servers and Virtualization** | Physical servers and virtual machines that host the **[System Name]** application, databases, and supporting services. Servers are configured with secure baselines, and virtualization technology is used to isolate workloads, improve resource utilization, and facilitate redundancy. Automated configuration management tools ensure consistency across environments. | Primary data centers and cloud infrastructure |

| | | |
|---|---|---|
| **Software Applications** | The **[System Name]** application itself, including user interfaces, APIs, and supporting services; development tools such as integrated development environments (IDEs), source code repositories, version control systems, and build automation platforms; monitoring and logging tools; and third-party libraries. Applications are developed following secure coding guidelines and undergo code reviews and security testing. | Cloud hosting and managed services |
| **Data Stores** | Databases, files, and storage systems that hold customer and internal data. All data is classified according to the Data Classification Policy and may be designated as public, internal, confidential, or restricted. Confidential and restricted data are encrypted in transit and at rest. Backup systems and replication ensure data availability and integrity. | Redundant storage across multiple availability zones |
| **People** | Personnel involved in the operation and maintenance of the system, including executive leadership, systems engineers, software developers, security analysts, customer support representatives, and compliance officers. Each role has defined responsibilities, and duties are segregated to reduce the risk of unauthorized actions. | Headquarters and remote offices |

**Additional Components**

In addition to the primary components, the system incorporates:

- **Middleware:** Messaging and integration components that facilitate communication between services. Middleware components are configured for high availability and secure data exchange.

- **Monitoring and Alerting Systems:** Tools that collect logs, metrics, and events from infrastructure and applications. These systems support real-time monitoring and generate alerts based on predefined thresholds or anomalous patterns.

- **Configuration Management Databases (CMDB):** Inventories of hardware, software, and network assets, with relationships and dependencies tracked to facilitate change management, incident response, and root cause analysis.

- **Secure Development Pipelines:** Continuous integration and continuous deployment (CI/CD) pipelines with automated testing, code quality checks, vulnerability scanning, and controlled release processes.

## Organizational Structure and Key Roles

XYZ Company maintains a structured organization to ensure clear lines of authority, accountability, and communication. A simplified representation of key functional areas is provided below:

| Role / Department | Primary Responsibilities |
|---|---|
| **Board of Directors and** | Establishes the company's strategic direction, approves major policies, and oversees risk management. Provides oversight of |

| | |
|---|---|
| **Executive Leadership** | the control environment and compliance with regulatory requirements. |
| **Chief Executive Officer (CEO)** | Overall responsibility for company operations and strategic execution. Works closely with senior management to ensure the company meets its service commitments and system requirements. |
| **Chief Technology Officer (CTO)** | Oversees technology strategy, system architecture, and engineering teams. Ensures that technology investments align with service commitments and support secure and reliable operations. |
| **Chief Information Security Officer (CISO)** | Leads the Information Security Program, develops security policies and procedures, conducts risk assessments, and manages incident response. Chairs the Security Steering Committee. |
| **Chief Risk Officer (CRO)** | Coordinates risk management activities, maintains the risk register, and oversees periodic risk assessments. Reports findings to executive leadership and ensures alignment with the organization's risk appetite. |
| **Security Steering Committee** | Cross-functional group that meets quarterly to review security strategy, incidents, compliance status, and improvements. Includes senior management from IT, security, risk, and compliance. |
| **Engineering Teams** | Develop and maintain the **[System Name]** application and infrastructure. Follow secure coding standards, perform code |

| | |
|---|---|
| | reviews, and collaborate with security on vulnerability remediation. |
| **Operations / DevOps** | Maintain and monitor the production environment. Manage deployments, patching, backup, and recovery procedures. Work with security to implement infrastructure changes securely. |
| **Quality Assurance (QA)** | Conduct functional and security testing of applications. Validate that changes meet requirements and do not introduce defects or vulnerabilities. |
| **Customer Support and Client Services** | Provide support to customers, process service requests, and address concerns. Communicate incidents and maintenance windows to users. |
| **Compliance and Audit** | Monitor adherence to internal policies and regulatory obligations. Coordinate external audits, manage remediation efforts, and track compliance metrics. |

## Policies and Procedures

XYZ Company's policy framework underpins its control environment. Policies are approved by senior management and reviewed annually to ensure they remain relevant and effective. Key policies include:

1. **Code of Conduct:** Establishes expectations for ethical behavior, integrity, and professionalism. All employees acknowledge the Code upon hiring and renew their acknowledgment annually.

2. **Information Security Policy:** Defines overarching security objectives, roles, and responsibilities. It covers areas such as access control, data protection, vulnerability management, physical security, and incident

response.

3. **Data Classification and Handling Policy:** Outlines classifications for data (e.g., public, internal, confidential, restricted) and specifies handling requirements, including storage, transmission, access, and retention.

4. **Access Control Policy:** Describes the process for granting, modifying, and revoking access to systems and data. It enforces least privilege, multi-factor authentication, and periodic access reviews.

5. **Change Management Policy:** Governs the planning, approval, testing, and implementation of changes to systems, applications, and infrastructure. It ensures that changes are documented, authorized by appropriate personnel, and communicated to stakeholders.

6. **Vulnerability Management Policy:** Defines the process for identifying, prioritizing, and remediating vulnerabilities. It includes requirements for vulnerability scanning, patch management, penetration testing, and reporting.

7. **Incident Response Plan (IRP):** Provides guidance on detecting, investigating, responding to, and recovering from security incidents. The IRP includes communication protocols, escalation procedures, and post-incident analysis.

8. **Business Continuity and Disaster Recovery (BC/DR) Policy:** Specifies procedures to maintain operations during disruptions and to recover systems and data in the event of a disaster. It covers backup frequency, offsite storage, alternate work locations, and recovery objectives.

9. **Acceptable Use Policy:** Specifies permissible use of company assets and networks. It prohibits unauthorized software installation, data exfiltration, and inappropriate use of resources.

10. **Privacy Policy:** Describes how personal information is collected, used, shared, stored, and destroyed in compliance with applicable privacy laws and contractual requirements. It outlines data subject rights, consent mechanisms, and retention schedules.

Each policy is supplemented by procedures that describe how to implement the policy, identify responsible parties, and include forms and templates as needed. Policies are communicated through the intranet, new hire training, and annual refreshers. Changes to policies follow a documented approval process.

## Control Environment

XYZ Company fosters a control environment that emphasizes security, integrity, and accountability. Management establishes clear expectations and provides resources to implement controls effectively. The following elements illustrate the control environment:

- **Management Philosophy and Tone at the Top:** Senior management actively promotes a culture of security and ethical behavior. The Security Steering Committee meets at least quarterly to oversee security initiatives and allocate necessary resources. Executive leaders communicate the importance of compliance and model desired behaviors.

- **Commitment to Integrity and Ethical Values:** The Code of Conduct sets expectations for ethical conduct, and employees are required to acknowledge it during onboarding and annually thereafter. The Code includes provisions on confidentiality, conflicts of interest, anti-bribery, and reporting mechanisms.

- **Organizational Structure and Assignment of Authority:** Responsibilities for designing, implementing, and monitoring controls are clearly delineated in organizational charts and job descriptions. Lines of reporting ensure accountability and independence where necessary.

- **Competence and Personnel Development:** XYZ Company screens candidates through background checks and requires confidentiality agreements. New hires receive comprehensive orientation and training on policies, security practices, and specific job functions. Ongoing training ensures that employees remain competent and aware of evolving threats and regulatory changes.

- **Policy Violation and Escalation Procedures:** An open reporting culture encourages employees to report suspected policy violations or control deficiencies without fear of retaliation. Reports can be made to supervisors, the Security Officer, or through anonymous hotlines. Incidents are logged, investigated, and resolved, with outcomes tracked to ensure follow-up actions.

## Information and Communication

Effective information and communication processes are crucial to ensuring that individuals receive the information they need to fulfill their responsibilities. XYZ Company communicates internally through:

- **Intranet Portal:** Central repository for policies, procedures, forms, and announcements. Employees can access resources, training materials, and system documentation. Updates to policies or procedures are communicated via notifications and highlighted on the portal.

- **Email and Collaboration Tools:** Official communications, incident notifications, and general announcements are distributed via email. Collaboration tools such as chat platforms and shared workspaces enable teamwork and knowledge sharing.

- **All-Hands Meetings and Departmental Meetings:** Management regularly communicates strategic priorities, security updates, and compliance requirements. Department meetings discuss operational metrics, upcoming changes, and improvement initiatives.

- **External Communications:** Customers are informed of maintenance windows, changes to service features, and incident notifications through the customer portal or email. Documentation is available on the company's website and includes service descriptions, data protection measures, and privacy practices.

Communication is two-way; employees and users can report concerns or anomalies. XYZ Company uses a designated channel (e.g., a ticketing system or issue reporting portal) to submit questions or report incidents. Reported issues are triaged according to the Security Incident Response Plan and escalated as needed.

## Risk Management

A formal risk management program identifies, assesses, and addresses risks related to the company's strategic objectives, operations, and compliance obligations. The program includes the following components:

1. **Risk Governance:** The Chief Risk Officer leads the risk management program and ensures coordination across departments. The CRO reports to the Board and executive leadership, providing quarterly updates on risk exposure and mitigation efforts.

2. **Risk Assessment Process:** Periodic risk assessments are conducted to identify threats and vulnerabilities that could impact security, availability, processing integrity, confidentiality, or privacy. Assessments evaluate potential impacts and likelihood, resulting in risk ratings and prioritization for treatment.

3. **Risk Treatment:** Based on the assessment, XYZ Company selects appropriate responses, including mitigating, transferring, accepting, or avoiding risks. Control activities are designed or enhanced to reduce residual risk.

4. **Risk Register:** Identified risks, their owners, treatment plans, and status are documented in a risk register. The register is reviewed regularly to track progress and update actions.

5. **Risk Monitoring and Reporting:** Risks are monitored through metrics, audits, and performance indicators. Significant risks or changes in risk exposure are reported to the Security Steering Committee and executive leadership for review and decision-making.

6. **Compliance Monitoring:** The risk management process includes monitoring changes in laws and regulations (e.g., data protection laws, industry standards) and ensuring that policies and controls remain aligned with these requirements.

## Monitoring Activities

XYZ Company employs a comprehensive monitoring program to ensure that controls function as intended and to detect deviations promptly. Monitoring activities include:

- **Continuous Monitoring:** Automated tools collect data from systems, applications, and networks to track uptime, performance, and security events. Dashboards display key metrics such as login attempts, access logs, system capacity, and error rates.

- **Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs):** Management defines KPIs and KRIs to measure the effectiveness of controls and processes. Examples include patch deployment timeliness, incident response times, and user access review completion rates.

- **Regular Meetings:** Operational teams meet weekly or biweekly to review metrics, discuss anomalies, and plan corrective actions. Quarterly meetings with the Internal Control group provide a forum to discuss control

effectiveness across departments and address systemic issues.

- **Control Self-Assessments:** Departments conduct quarterly self-assessments of their controls, documenting evidence of operation and identifying areas for improvement. Findings are consolidated by the Internal Control group and presented to the CRO.

- **Internal Audits:** The internal audit function performs independent evaluations of controls, focusing on high-risk areas. Audits assess compliance with policies, evaluate design and operating effectiveness, and issue recommendations. Audit results are reported to the Audit Committee and management.

- **External Audits:** In addition to the SOC 2 examination, XYZ Company undergoes other external assessments (e.g., ISO 27001, PCI DSS as applicable) to validate adherence to industry standards.

## Control Activities

Control activities are the policies, procedures, and mechanisms put in place to achieve the company's objectives related to security, availability, processing integrity, confidentiality, and privacy. These activities are embedded throughout the organization and include preventive, detective, and corrective measures.

#### Access Control

Access control safeguards prevent unauthorized access to systems and data. Key aspects include:

- **User Provisioning and De-Provisioning:** Access rights are granted based on job responsibilities and least privilege principles. Access requests are documented, approved by managers, and implemented by system administrators. Access changes (e.g., transfers, promotions) trigger reviews to ensure alignment with duties. Access is terminated promptly upon employee

separation.

- **Authentication and Authorization Mechanisms:** The system employs multi-factor authentication for administrative and privileged accounts. Role-based access controls (RBAC) enforce segregation of duties, ensuring that no individual can unilaterally perform critical tasks. Authorization rules are regularly reviewed and updated as roles evolve..

- **Periodic Access Reviews:** Managers perform quarterly reviews of access rights to confirm that access remains appropriate for each user. Results are documented, and access is adjusted as necessary.

- **Monitoring and Alerting:** Automated monitoring tools (e.g., SIEM systems) track login attempts, privileged account usage, and anomalous access patterns. Alerts are generated for suspicious activity and investigated by the security team.

- **Physical Access Controls:** Data centers are secured with multi-factor physical access mechanisms such as biometric readers, badges, and mantraps. Visitor access is logged and escorted, and equipment rooms are monitored by surveillance cameras. Physical access is granted on a need-to-have basis and reviewed periodically.

**Change Management**

Changes to systems and applications must follow a structured process to prevent unauthorized modifications and to maintain stability. The Change Management process includes:

1. **Change Request Submission:** Changes are proposed by authorized personnel and documented in a ticketing system. The request includes description, rationale, risk assessment, and proposed implementation plan.

2. **Impact and Risk Assessment:** A change advisory board (CAB) reviews proposed changes, evaluates potential impacts on security, availability, and compliance, and determines whether additional testing is needed. High-risk changes may require additional approvals.

3. **Testing:** Changes are tested in pre-production environments to ensure functionality and to identify unintended consequences. Functional and security tests (e.g., unit tests, integration tests, regression tests, vulnerability scans) are performed.

4. **Approval:** Once testing is successful, the change is formally approved by authorized individuals (e.g., project managers, security managers, product owners). Emergency changes follow an expedited approval process and are reviewed retrospectively.

5. **Implementation:** Approved changes are deployed according to the implementation plan. Deployments are often automated to reduce human error and to ensure consistency across environments.

6. **Communication:** Affected stakeholders (e.g., users, support teams) are notified of the change schedule and potential impacts. Release notes and documentation are updated accordingly.

7. **Post-Implementation Review:** After deployment, changes are monitored to ensure they function as intended. Any issues discovered are addressed promptly, and the CAB reviews outcomes to improve future change management.

**Vulnerability Management**

XYZ Company's vulnerability management program proactively identifies and addresses weaknesses in systems. The program includes:

- **Regular Scanning:** Automated vulnerability scans are conducted weekly on infrastructure, applications, and network components. Scans are configured to detect missing patches, insecure configurations, and known vulnerabilities.

- **Patch Management:** Identified vulnerabilities are prioritized based on severity and exploitability. Critical patches are applied as soon as possible (within defined timeframes), while medium and low-risk patches follow scheduled maintenance cycles. Patching progress is tracked and reported.

- **Penetration Testing:** External security experts perform penetration tests at least annually to simulate real-world attacks and identify vulnerabilities that may not be detected by automated scanners. Findings are documented, and remediation steps are tracked until resolved.

- **Configuration Management:** Hardening guidelines are applied to servers, network devices, and applications. Baseline configurations are documented, and continuous configuration monitoring detects deviations from expected baselines.

- **Reporting and Metrics:** Vulnerability management metrics (e.g., number of open vulnerabilities, average time to remediate) are reviewed regularly by the CRO and senior management.

**Incident Response**

The Incident Response Plan (IRP) outlines procedures to detect, analyze, respond to, and recover from security incidents. Its objectives are to minimize impacts, restore normal operations, and prevent recurrence. The IRP covers:

1. **Preparation:** Defining roles and responsibilities, training incident responders, and maintaining tools and resources (e.g., SIEM, forensics tools). The IRP includes contact lists, communication templates, and escalation criteria.

2. **Identification:** Monitoring systems generate alerts for suspicious activity such as unusual network traffic, failed login attempts, or abnormal system behavior. Employees and third parties can report incidents through designated channels. Security analysts assess and confirm incidents based on the severity and impact.

3. **Containment:** Actions are taken to limit the scope and impact of an incident. Short-term containment may involve isolating affected systems, revoking compromised credentials, and blocking malicious traffic. Long-term containment aims to provide a stable environment for investigation and remediation, such as establishing clean environments or restoring from backups.

4. **Eradication:** The root cause is identified, and remediation steps are taken to remove malware, close vulnerabilities, or strengthen controls. This may include applying security patches, reconfiguring systems, or enhancing monitoring.

5. **Recovery:** Systems are restored to normal operation using validated backups and recovery procedures. Recovery includes verifying system configurations, re-enabling user access, and monitoring for recurrence. Business Continuity and Disaster Recovery plans are followed to minimize downtime.

6. **Post-Incident Analysis:** After an incident is resolved, the response team conducts a debrief to capture lessons learned and update the IRP. Findings may lead to changes in policies, controls, or training.

7. **Testing and Training:** The IRP is tested semi-annually through tabletop exercises and simulated incidents. Results inform improvements, and employees receive training to recognize and report incidents.

## Complementary User Entity Controls (CUECs)

Certain controls must be implemented by user entities (customers) to fully meet the service commitments and system requirements. These complementary user entity controls (CUECs) include:

| User Entity Control | Purpose | Relevant Criteria |
|---|---|---|
| Customers must report material changes to their own control environments that could affect the service provided by XYZ Company | Ensures XYZ Company can assess impacts and adjust controls or support accordingly | CC2.1 |
| Customers are responsible for managing user accounts within their organizations, including setting strong passwords and enforcing multi-factor authentication for access to the **[System Name]** | Supports access control and reduces the risk of unauthorized access | CC6.1 |
| Customers must ensure that devices used to access the **[System Name]** are protected by up-to-date anti-malware software and secure configurations | Reduces the likelihood of compromised endpoints affecting the service | CC5.2 |
| Customers must establish their own incident response processes to address potential security events impacting data processed by the **[System Name]** | Enables coordinated response between the customer and XYZ Company in the event of an incident | CC7.1 |
| Customers should review service reports and monitoring information provided by XYZ | Enhances transparency and accountability | CC3.2 |

| | | |
|---|---|---|
| Company (e.g., access logs, audit trails) and raise any concerns promptly | | |

## Complementary Subservice Organization Controls (CSOCs)

XYZ Company uses subservice organizations, such as **XYZ Cloud Hosting**, to provide infrastructure hosting and related services. While the subservice organization's controls are outside the scope of this report, XYZ Company assumes that the subservice organization implements complementary controls necessary to meet service commitments. Examples include:

| Subservice Organization | Services Provided | Expected Complementary Controls |
|---|---|---|
| **XYZ Cloud Hosting** | Infrastructure hosting, data center management | Performs periodic vulnerability assessments, applies security patches promptly, restricts physical access to data centers, maintains environmental controls (power, cooling, fire suppression), and monitors network security |
| **Third-Party Monitoring Provider** | Real-time monitoring and alerting | Maintains robust detection mechanisms, escalates critical alerts to XYZ Company, ensures continuity of monitoring services |
| **Identity Verification Service** | Identity proofing and authentication services | Implements secure identity verification processes, protects personal data, and maintains high availability |

| | | |
|---|---|---|
| **Payment Processing Service** | Handles customer payments and sensitive financial data | Complies with PCI DSS requirements, encrypts payment data, and segregates payment systems from other infrastructure |

XYZ Company regularly evaluates subservice organizations through due diligence, contract requirements, and review of third-party attestation reports (e.g., SOC 2 Type 2, ISO 27001) to ensure that their controls align with XYZ Company's expectations.

## System Incidents and Significant Changes

During the reporting period from **[Start Date]** to **[End Date]**, no significant incidents occurred that affected the effectiveness of the controls or resulted in failure to meet service commitments. Any minor incidents were handled through the incident response process without impact on service commitments.

There were no significant changes to the **[System Name]** or its control environment during the period that would impact users' understanding of the system's operations or service delivery. Routine enhancements and maintenance activities followed the Change Management Policy and were communicated to stakeholders.

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

## Overview of Trust Services Criteria

XYZ Company designed and implemented controls to meet the applicable Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy. Each criterion focuses on a different aspect of service reliability and data protection:

1. **Security:** The system is protected against unauthorized access, both physical and logical.

2. **Availability:** The system is available for operation and use as committed or agreed.

3. **Processing Integrity:** System processing is complete, valid, accurate, timely, and authorized.

4. **Confidentiality:** Information designated as confidential is protected according to policy or agreement.

5. **Privacy:** Personal information is collected, used, retained, disclosed, and disposed of according to the entity's privacy notice and criteria.

Controls are mapped to the criteria and organized by criteria area. Each control is assigned a unique identifier to facilitate testing and reporting.

## Procedures for Assessing Information Provided by the Entity (IPE)

Some controls rely on system-generated information (IPE) to evaluate operating effectiveness. To ensure accuracy and completeness of this information, the service auditor performed procedures such as:

- Inspecting the source of the IPE (e.g., logs, databases, reports) to verify its reliability.

- Reviewing queries, scripts, or parameters used to generate the information to confirm that they selected the intended data.

- Comparing data in the IPE to source systems (e.g., reconciling user lists, transaction counts) to ensure completeness and accuracy.

- Inspecting the IPE for anomalies such as missing sequences, gaps in timing, or irregular patterns.

- Evaluating management's procedures for validating IPE in the execution of controls (e.g., verifying that user access listings used in quarterly reviews are complete and accurate).

## Testing Methods

The service auditor employed several methods to test the operating effectiveness of controls:

- **Inquiry:** Interviews with management, operations, and administrative personnel responsible for designing and performing controls, to understand processes and evaluate whether controls were executed as described.

- **Observation:** Witnessing the application of control activities, such as observing an engineer implement a change, a manager conduct an access review, or a security analyst respond to an incident. Observation verifies that controls were performed and that procedures align with documentation.

- **Inspection:** Examining source documents, reports, system configurations, logs, screenshots, and other evidence to confirm that control activities occurred. For example, inspecting change tickets, access review approvals, vulnerability scan reports, or incident tickets.

- **Re-performance:** Independently executing control procedures to validate results. For example, the auditor might re-perform a sample of backup restorations, user provisioning steps, or review logs to ensure that the control is functioning correctly.

These methods provide reasonable assurance that controls operated effectively during the examination period.

## Controls Without an Occurrence

Some controls are triggered only when specific events occur, such as emergency changes, major incidents, or disaster recovery tests. If such events did not occur during the examination period, the auditor verified that the triggering events did not take place and documented the rationale for not testing those controls.

## XYZ Company Controls and Mapping to Trust Services Criteria

The following table presents examples of XYZ Company's control activities mapped to the Trust Services Criteria and COSO principles. The list is illustrative and not exhaustive.

| Criteria Area | Reference # | Control Activity | Criteria Description |
|---|---|---|---|
| Security – Control Environment | **CC1.1** | The organization establishes and communicates a Code of Conduct outlining acceptable behavior, | COSO Principle 1 – The entity demonstrates a commitment to integrity and ethical values. |

| | | | |
|---|---|---|---|
| | | integrity, and confidentiality expectations. The Code is published on the intranet, and employees acknowledge receipt upon hire and annually thereafter. | |
| Security – Risk Assessment | **CC3.3** | Management considers the potential for fraud when identifying and assessing risks, and includes fraud risk factors in the risk assessment matrix. | COSO Principle 8 – The entity considers the potential for fraud in assessing risks. |
| Security – Control Activities | **CC6.2** | Access to production systems is restricted based on least privilege. User access is reviewed quarterly by managers, and deviations are corrected promptly. | COSO Principle 10 – The entity selects and develops control activities that contribute to the mitigation of risks. |
| Availability – Change Management | **CC9.2** | Changes to systems are subject to documented approval, testing, and change implementation procedures. Emergency | Trust Services Criterion for Change Management – Controls provide reasonable assurance that system changes do not adversely affect system availability. |

| | | | |
|---|---|---|---|
| | | changes are reviewed retrospectively. | |
| Processing Integrity – Input Controls | **PI1.1** | Validation checks ensure that data input to the system is complete and accurate; erroneous entries generate error messages and are corrected before processing continues. | Trust Services Criterion for Processing Integrity – Controls provide reasonable assurance that processing is complete, valid, accurate, and timely. |
| Confidentiality – Data Transmission | **C1.2** | Confidential data transmitted over public networks is encrypted using industry-standard protocols (e.g., TLS). Keys are managed securely, and transmission logs are reviewed. | Trust Services Criterion for Confidentiality – Controls provide reasonable assurance that confidential information is protected during transmission. |
| Privacy – Notice and Consent | **P1.1** | A privacy notice informs data subjects about collection, use, and sharing of personal information. Consent is obtained where required by law, and mechanisms are in | Trust Services Criterion for Privacy – Controls address notice, choice, consent, and data subject rights. |

| | | | |
|---|---|---|---|
| | | place to handle data subject requests. | |

### Tests of Controls and Results

The auditor tested the controls listed above and other controls to determine whether they operated effectively. The table below provides illustrative examples of tests performed and the results:

| Control Number | Control Activity | Criteria Mapping | Service Auditor's Tests | Results |
|---|---|---|---|---|
| **CC3.3.1** | Management considers the potential for fraud when assessing risks, and this consideration is documented in the risk matrix. | COSO Principle 8 | Reviewed the risk assessment documentation and risk matrix for evidence of fraud considerations; interviewed the CRO about risk assessment procedures. | No exceptions noted; fraud risks were documented and considered. |
| **CC6.2.1** | User access to the **[System Name]** is reviewed quarterly by the system owner and approved by management. | COSO Principle 10, CC6.2 | Selected a sample of users; inspected quarterly access review records for completeness and evidence of management approval; verified | No exceptions noted; reviews were completed and documented; inappropriate access was removed timely. |

| | | | | |
|---|---|---|---|---|
| | | | that access changes were made where necessary. | |
| **CC9.2.2** | Changes to production systems are approved, tested, and documented before deployment. | Change Management Criterion | Selected a sample of change tickets; inspected documentation for approvals, testing evidence, and deployment results; observed change deployment for one change. | No exceptions noted; all sampled changes followed the policy. |
| **PI1.1.1** | Input validation checks prevent incomplete or incorrect data entry into the system. | Processing Integrity Criterion | For a sample of transactions, inspected system logs and input validation rules; re-performed input of invalid data to verify rejection; interviewed developers about validation logic. | No exceptions noted; validation rules functioned correctly. |

| | | | | |
|---|---|---|---|---|
| **C1.2.1** | Data transmitted over external networks is encrypted using TLS 1.2 or higher. | Confidentiality Criterion | Inspected configuration files and encryption settings; observed network traffic using packet capture; verified certificates and encryption protocols. | No exceptions noted; encryption protocols were appropriately configured. |
| **P1.1.1** | A privacy notice is provided to users, and data subject requests are processed within statutory timeframes. | Privacy Criterion | Reviewed the privacy notice; inspected records of data subject requests and responses; interviewed privacy officer about consent management. | No exceptions noted; privacy notice was comprehensive, and data subject requests were handled within required timeframes. |

These examples illustrate the depth of testing performed. The full listing of controls tested and results is available to authorized parties upon request.