A blue and black logo

Description automatically generated

FakeCompany, Inc.  
SOC 2 Audit Report (Type 2)

Information Systems  
Conducted in February of 2024

Audit Period: January 1, 2023 - December 31, 2023

**A blue circle with white text

Description automatically generated**

Legal Disclaimer  
*This document is intended solely for self-education purposes and does not constitute an official SOC 2 Type audit report. The findings, conclusions, and recommendations presented herein are based on hypothetical scenarios and academic analysis and should not be interpreted as a formal audit conducted by a certified professional. The Heart Hospital, Baylor Scott & White Health, and any referenced entities are used as part of an academic exercise and not as part of an actual assessment. For official audit and compliance services, please consult a certified public accountant or a qualified audit firm.*

Table of Contents

## Introduction

1.1 Purpose

1.2 Scope

1.3 Trust Service Criteria Overview

## Security Controls

2.1 Network Security

2.2 Access Control

2.3 Physical Security

## Confidentiality Controls

3.1 Data Encryption

3.2 Data Masking and Tokenization

## Availability Controls

4.1 System Redundancy

4.2 Backup and Disaster Recovery

## Processing Integrity Controls

5.1 Transaction Processing

5.2 Error Handling and Logging

## Privacy Controls

6.1 Data Subject Rights

6.2 Data Minimization

## Risk Assessment

7.1 Risk Identification and Analysis

7.2 Risk Mitigation Strategies

## Control Testing and Evidence

8.1 Testing Procedures

8.2 Evidence of Control Effectiveness

## Roles and Responsibilities

9.1 Organizational Structure

9.2 Control Ownership and Accountability

## Conclusion and Continuous Improvement

10.1 Summary of Compliance

10.2 Plans for Continuous Monitoring and Improvement

# 1. Introduction

### 1.1 Purpose

This document serves to provide a comprehensive overview of the internal controls implemented by FakeCompany in alignment with the SOC 2 Trust Service Criteria. The purpose is to ensure that these controls are adequately designed and operating effectively to manage risks related to security, availability, processing integrity, confidentiality, and privacy.

### 1.2 Scope

The scope of this SOC 2 audit includes all systems, processes, and data handling activities that support FakeCompany’s delivery of services to its clients. This encompasses data centers located in New York, San Francisco, and London, as well as cloud environments managed through AWS and Azure platforms.

### 1.3 Trust Service Criteria Overview

The Trust Service Criteria include Security, Availability, Processing Integrity, Confidentiality, and Privacy. Each criterion is addressed through a combination of policies, procedures, and technical controls that are designed to mitigate identified risks.

# 2. Security Controls

### 2.1 Network Security

The organization’s network is protected by a Cisco ASA 5520 firewall configured according to industry best practices, including the implementation of strict access control lists (ACLs) to prevent unauthorized access. Firewall rules are reviewed quarterly by the Network Administrator, Jane Smith, and any necessary adjustments are made based on the latest threat intelligence. The most recent review was completed on July 15, 2024. **Evidence**: Attached ‘Firewall Rule Review Report\_Q3\_2024.pdf.’

Additionally, an Intrusion Detection System (IDS) using Snort rules is deployed to monitor network traffic for signs of malicious activity. This IDS is configured to alert the IT Security Team in real-time when suspicious behavior is detected, such as attempts to access restricted areas of the network. **Evidence**: ‘IDS Configuration and Alert Logs\_July\_2024.pdf.’

### 2.2 Access Control

Access to sensitive systems and data is controlled through a combination of role-based access controls (RBAC) and multi-factor authentication (MFA). All employees are assigned roles based on their job functions, and access rights are granted accordingly. MFA is enforced for all critical systems, with authentication factors including a password and a mobile token generated by an RSA SecurID device.

Access reviews are conducted quarterly to ensure that access rights are appropriate for each user’s current role. The last review was carried out on August 1, 2024, by the IT Security Manager, John Doe. Any discrepancies found during the review are addressed immediately, with access being revoked or adjusted as needed. **Evidence**: See ‘Access Control Review Report\_Q3\_2024.pdf’ and ‘RBAC Matrix\_August\_2024.xlsx.’

### 2.3 Physical Security

Physical security measures are in place at all data centers to protect against unauthorized access and environmental hazards. These measures include biometric access controls, 24/7 CCTV monitoring, and redundant power supplies. Only authorized personnel can access the data centers, and all access is logged and reviewed weekly.

The last physical security audit, conducted on June 30, 2024, confirmed that all controls were operating as intended. **Evidence**: See ‘Physical Security Audit Report\_June\_2024.pdf’ and ‘CCTV Access Logs\_June\_2024.pdf.’

# 3. Confidentiality Controls

### 3.1 Data Encryption

To meet the Confidentiality criterion, all data at rest in our databases is encrypted using AES-256 encryption. Encryption keys are managed by AWS KMS (Key Management Service), which ensures that only authorized applications can decrypt data. Key rotations occur every six months, with the last rotation completed on July 31, 2024. **Evidence**: ‘Encryption Implementation Diagram’ and ‘KMS Key Management Policy\_2024.pdf.’

Data in transit is protected using TLS 1.2 or higher, ensuring that data exchanged between clients and servers is encrypted and secure. A review of all TLS certificates was completed on July 10, 2024, to ensure that they are up-to-date and configured correctly. **Evidence**: ‘TLS Certificate Review\_July\_2024.pdf.’

### 3.2 Data Masking and Tokenization

Sensitive data, such as personally identifiable information (PII), is masked or tokenized before storage in non-production environments. This process involves replacing sensitive data with non-sensitive equivalents (tokens) that cannot be reversed without access to the original encryption keys. This ensures that developers and testers do not have access to real customer data, reducing the risk of data breaches.

The data masking process was last verified on August 5, 2024, and no issues were identified. **Evidence**: ‘Data Masking and Tokenization Report\_August\_2024.pdf.’

# 4. Availability Controls

### 4.1 System Redundancy

System redundancy is achieved through the deployment of load-balanced servers across multiple geographic locations. In the event of a failure in one location, traffic is automatically redirected to another, ensuring continuous service availability. All critical systems have a 99.9% uptime guarantee, backed by service-level agreements (SLAs) with our hosting providers.

The redundancy setup was tested on July 20, 2024, by simulating a server failure in the New York data center. The system automatically failed over to the San Francisco data center with zero downtime. **Evidence**: ‘Redundancy Test Report\_July\_2024.pdf.’

### 4.2 Backup and Disaster Recovery

Regular backups are taken of all critical systems, with daily incremental backups and weekly full backups. These backups are stored in an offsite location and are encrypted using AES-256 encryption. The disaster recovery plan is tested quarterly to ensure that data can be restored within 24 hours in the event of a major incident.

The last disaster recovery test was conducted on July 25, 2024, and the system was fully restored in 18 hours. **Evidence**: ‘Disaster Recovery Test Results\_July\_2024.pdf’ and ‘Backup Policy\_2024.pdf.’

# 5. Processing Integrity Controls

### 5.1 Transaction Processing

Transaction integrity is ensured through the use of automated validation checks that verify the accuracy and completeness of transactions before they are processed. These checks include data type validation, range validation, and cross-referencing with existing records.

Anomalies or errors detected during processing are logged and reviewed by the Quality Assurance (QA) team within 24 hours. The most recent transaction integrity audit, conducted on August 10, 2024, found no significant issues. **Evidence**: ‘Transaction Integrity Audit Report\_August\_2024.pdf.’

### 5.2 Error Handling and Logging

All system errors are automatically logged and categorized based on severity. Critical errors trigger immediate alerts to the IT support team, who are required to respond within 30 minutes. The logging system is configured to capture detailed information about each error, including timestamps, affected systems, and user actions.

Error logs are reviewed weekly to identify recurring issues and to implement permanent fixes. The last review, on August 15, 2024, identified a recurring issue with data synchronization, which was resolved with a patch on August 18, 2024. **Evidence**: ‘Error Log Review\_August\_2024.pdf.’

# 6. Privacy Controls

### 6.1 Data Subject Rights

To comply with privacy regulations such as GDPR, FakeCompany has implemented procedures for managing data subject requests. These include the right to access, correct, delete, and restrict the processing of personal data. Data subject requests are tracked in our privacy management system, with a standard response time of 30 days.

The last internal audit of data subject request handling, completed on July 31, 2024, confirmed compliance with regulatory requirements. **Evidence**: ‘Data Subject Request Audit\_July\_2024.pdf.’

#### 6.2 Data Minimization

Data minimization practices are enforced to ensure that only necessary personal data is collected and processed. This includes conducting regular data reviews to identify and delete or anonymize data that is no longer needed.

The most recent data review, conducted on August 10, 2024, led to the deletion of 15,000 records that were no longer required for business purposes. **Evidence**: ‘Data Minimization Review\_August\_2024.pdf.’

# 7. Risk Assessment

### 7.1 Risk Identification and Analysis

A formal risk assessment was conducted on June 30, 2024, identifying potential threats to data confidentiality, such as unauthorized access to cloud storage and vulnerabilities in third-party software. Each risk was evaluated based on its potential impact and likelihood, and controls were implemented to mitigate these risks.

For example, the risk of unauthorized access to cloud storage was mitigated by implementing MFA for all cloud accounts and encrypting sensitive files. **Evidence**: ‘Risk Assessment Report\_June\_2024.pdf’ and ‘Cloud Security Policy\_2024.pdf.’

### 7.2 Risk Mitigation Strategies

Mitigation strategies are developed for each identified risk, with specific controls assigned to mitigate the risk. For example, to address the risk of phishing attacks, a company-wide phishing awareness program was implemented, along with technical controls such as email filtering and real-time phishing detection tools.

The effectiveness of these strategies is reviewed quarterly, with the last review conducted on August 1, 2024. **Evidence**: ‘Risk Mitigation Review\_August\_2024.pdf’ and ‘Phishing Awareness Training Materials\_2024.pdf.’

# 8. Control Testing and Evidence

### 8.1 Testing Procedures

Control testing is conducted regularly to ensure that all controls are operating effectively. Testing procedures include simulated attacks, penetration testing, and control reviews. For example, penetration testing was conducted on July 15, 2024, to assess the security of external-facing systems. The test identified a vulnerability in the web application firewall (WAF), which was patched immediately.

All testing activities are documented, and results are reviewed by the IT Security Manager, who ensures that any issues are promptly addressed. **Evidence**: ‘Penetration Test Report\_July\_2024.pdf’ and ‘Vulnerability Management Policy\_2024.pdf.’

### 8.2 Evidence of Control Effectiveness

Evidence of control effectiveness is collected and maintained for each control, including logs, reports, and audit trails. For example, the effectiveness of access controls is evidenced by access logs, which show that only authorized users accessed the system during the audit period.

The evidence collected is stored in a secure document repository and is reviewed during internal audits to ensure that it is complete and accurate. **Evidence**: ‘Access Logs\_Q3\_2024.pdf’ and ‘Internal Audit Report\_August\_2024.pdf.’

# 9. Roles and Responsibilities

### 9.1 Organizational Structure

FakeCompany’s organizational structure supports the effective implementation and monitoring of internal controls. The IT Security team is responsible for implementing technical controls, while the Compliance team oversees policy adherence and regulatory compliance.

A detailed roles and responsibilities matrix is maintained, outlining each team’s responsibilities. For example, the IT Security Manager, John Doe, is responsible for quarterly access reviews, while the Compliance Officer, Jane Smith, is responsible for managing data subject requests. **Evidence**: ‘Roles and Responsibilities Matrix\_2024.pdf.’

### 9.2 Control Ownership and Accountability

Each control has an assigned owner who is responsible for its implementation, monitoring, and documentation. Control ownership is documented in the roles and responsibilities matrix and is reviewed annually to ensure that responsibilities align with current roles.

For example, the owner of the data encryption control is the Chief Information Security Officer (CISO), who is responsible for ensuring that encryption policies are followed and that encryption keys are managed securely. **Evidence**: ‘Encryption Policy\_2024.pdf’ and ‘Key Management Review\_July\_2024.pdf.’

# 10. Conclusion and Continuous Improvement

### 10.1 Summary of Compliance

FakeCompany has implemented a robust set of controls that align with the SOC 2 Trust Service Criteria. Through regular testing, continuous monitoring, and a commitment to improvement, the organization ensures that these controls remain effective in mitigating identified risks.

The SOC 2 audit confirmed that controls were operating effectively during the audit period, with no significant deficiencies identified. **Evidence**: ‘SOC 2 Audit Report\_2024.pdf.’

### 10.2 Plans for Continuous Monitoring and Improvement

To maintain compliance and adapt to evolving threats, FakeCompany has established a continuous monitoring program that includes regular reviews of all controls, real-time monitoring of critical systems, and annual risk assessments.

Future improvements include upgrading the IDS to incorporate machine learning for better threat detection and implementing a new data loss prevention (DLP) system. These initiatives are scheduled for completion by December 2024. **Evidence**: ‘Continuous Improvement Plan\_2024.pdf.’

For further demonstrations of my SOC 2 auditing experience, including additional SOC 2 audit samples, security assessment tools, and compliance resources, please visit my GitHub repository: <https://github.com/Cameron-K03/Security-Auditing>

[A qr code on a white background

Description automatically generated](https://github.com/Cameron-K03/Security-Auditing)