Service Organization Control (SOC) 2

Compliance Process

esm_logo.jpg

Nexelus USA  
New York, NEW YORK (NY)  
646-558-1950 ext.128

**9/28/2021**

Contents

[What is SOC 2 Compliance 1](#_Toc83734528)

[SOC 2 compliance Requirements 2](#_Toc83734529)

[Other SOC 2 Compliance Requirements 4](#_Toc83734530)

[1. Availability 4](#_Toc83734531)

[Deliverables 4](#_Toc83734532)

[2. Processing integrity 4](#_Toc83734533)

[Deliverables 5](#_Toc83734534)

[3. Confidentiality 5](#_Toc83734535)

[Deliverables 5](#_Toc83734536)

[4. Privacy 5](#_Toc83734537)

[Privacy Principles 5](#_Toc83734538)

[Information Categories Covered in Privacy Protections 6](#_Toc83734539)

[Deliverables 7](#_Toc83734540)

# What is SOC 2 Compliance

Service Organization Control (SOC) 2 is a set of compliance requirements and research procedures aimed at third-party service providers. It is designed to help companies determine if their business partners and vendors can safely manage data and protect the interests and privacy of their customers.

SOC 2 was developed by the American Institute of Certified Public Accountants (AICPA). Within its processes, there are two types of SOC 2 reports:

**SOC 2 Type 1** details about the systems and controls you have for security compliance. Auditors check the evidence and verify that you are meeting the appropriate standards of trust. Think of it as a time point confirmation of controls.

**SOC 2 Type 2** evaluates how your processes work in providing the desired level of security and data management over a period of time.

# SOC 2 compliance Requirements

The compliance of SOC 2 is based on a specific customer data management system, which consists of five sections of Trust Services:

* Security
* Availability
* Considering Integrity
* Confidentiality
* Privacy

**Security** is the basis of SOC 2 compliance, which contains a wide range of methods common to all five categories of trust service.

The safety policy focuses on protecting assets and service data in accordance with SOC 2 compliance with unauthorized use. You may use access controls to prevent malicious attacks or unauthorized deletion of data, misuse of company software, unauthorized modification, or disclosure of company information.

When it comes to security, the basic Checklist for SOC 2 is provided in Annexure 1 of this document.

SOC 2 Compliance covers these controls:

1. **Logical and physical access controls**—How you restrict and manage logical and physical access, to prevent any unauthorized access
2. **System Operations**—How you manage your system operations to detect and mitigate deviations from set procedures
3. **Change Management**—How you implement a controlled change management process and prevent unauthorized changes
4. **Risk Mitigation**—How you identify and develop risk mitigation activities when dealing with business disruptions and the use of any vendor services

Some SOC 2 criteria are very broad and more policy-driven, whereas some are technical—but even the technical criteria won't tell you exactly what you need to do. As such, SOC 2 criteria are somewhat open to interpretation. It is up to each company to achieve the goal of each criterion by implementing various controls. The Trust Services Criteria document includes various “points of focus” to guide you.

For example, to meet the criteria for Logical and Physical Access Controls, one company may implement new onboarding processes, two-factor authentication, and systems to prevent the downloading of customer data when performing support, while another may restrict access to data centers, conduct quarterly reviews of permissions, and strictly audit what is done on production systems. No combination is perfect, or even specifically required. What is required is to achieve the end state desired by the criteria.

When you address the common criteria, you cover the security principles, which is the minimum requirement to become SOC 2 compliant.

# Other SOC 2 Compliance Requirements

With security covered, you should be able to attract business. However, if you operate in the finance or banking sector—or any industry where privacy and confidentiality is paramount—then you need to achieve a higher standard of compliance. Many companies look for vendors that are fully compliant, as it instills trust and demonstrates a commitment to minimizing risk.

You can go beyond the basic security principles to gain compliance for additional criteria in the other trust services categories below.

## 1. Availability

Availability is certainly a key service provided by Nexelus, because if the data center goes down, the client’s business will be impacted. Clients of the Nexelus expect assurance of high availability of the data center.

The availability principle focuses on the accessibility of your system, in that you monitor and maintain your infrastructure, software, and data to ensure you have the processing capacity and system components needed to meet your business objectives.

SOC 2 compliance requirements in this category include:

This could include controls such as

**Measures Current Usage**—Measurement of use of system components is performed to establish a baseline for capacity management and to refer to when evaluating the risk of lack of availability due to capacity constraints.

**Forecasts Capacity**—A forecast and comparison of expected average and high use of system components to system capacity and tolerances is performed. Considerations include capacity in the event there is a system failure.

**Identifies Environmental Threats**—Management identifies environmental threats as part of the risk assessment that could impair the availability of the system. These could include threats resulting from weather, failure of environmental control systems, electrical discharge, fire, and flood/water.

**Designs Detection Measures**—Measures are implemented for detecting anomalies that could result from environmental threat events.

**Implements and Maintains Environmental Protection Mechanisms**— Environment protection mechanisms are implemented by Management to prevent and mitigate against environmental events.

**Responds to Environmental Threat Events**—Procedures have been developed and put in place for responding to environmental threats and for evaluating the effectiveness of those policies and procedures on an ongoing or periodic basis. This includes, but is not limited to, automatic mitigation systems (i.e., UPS and generator back-up subsystem).

**Implements Business Continuity Plan Testing**—Business continuity plan testing is performed on at least an annual basis. The testing includes (1) developing testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from the entire entity that can impact availability; (3) scenarios that consider the potential for lack of availability of key personnel; and (4) updating continuity plans and systems based on test results.

**Tests Integrity and Completeness of Back-Up Data**—The integrity and completeness of back-up information is tested on at least an annual basis.

### Deliverables

1. Asset Register
2. Access Control Process and Register
3. Backup Process and Log
4. Recovery Infrastructure (Fault Tolerance, etc)
5. Recovery Plan and Test Records
6. Capacity and Availability Management Strategy
7. Risk Register
8. Corrective and Preventive Action Log

## 2. Processing integrity

The processing integrity principle focuses on delivering the right data at the right price at the right time. Data processing should not only be timely and accurate, but it should also be valid and authorized.

SOC 2 compliance requirements in this category include:

* Create and maintain records of system inputs—Compile accurate records of system input activities.
* Defines processing activities—Define processing activities to ensure products or services meet specifications.

### Deliverables

1. Development Process
2. QA Process
3. Deployment Process
4. Risk Mitigation Plan

## 3. Confidentiality

The confidentiality principle focuses on restricting access and disclosure of private data so that only specific people or organizations can view it. Confidential data may include sensitive financial information, business plans, customer data in general, or intellectual property.

SOC 2 compliance requirements in this category include:

* Identify confidential information—Implement procedures to identify confidential information when it is received or created, and determine how long it should be retained.
* Destroy confidential information—Implement procedures to erase confidential information after it is identified for destruction.

### Deliverables

1. Firewall
2. Infrastructure Security Policies (Firewall, Database, Application Access)
3. SLA for employees with confidentiality compliance clauses

## 4. Privacy

The privacy principle focuses on the system's adherence to the client's privacy policies and the generally accepted privacy principles (GAPP) from the AICPA. This category of SOC considers methods used to collect, use, and retain personal information, as well as the process for disclosure and disposal of data.

SOC 2 compliance requirements in this category include:

* Use clear and conspicuous language—The language in the company's privacy notice is clear and coherent, leaving no room for misinterpretation.
* Collect information from reliable sources—The company confirms third-party data sources are reliable and operates its data collection process fairly and legally.

### Privacy Principles

The GAPP consists of ten privacy principles. The privacy principles are listed and summarized below:

1. Management. The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. Notice. The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. Choice and consent. The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. Collection. The entity collects personal information only for the purposes identified in the notice.
5. Use, retention, and disposal. The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6. Access. The entity provides individuals with access to their personal information for review and update.
7. Disclosure to third parties. The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. Security for privacy. The entity protects personal information against unauthorized access (both physical and logical).
9. Quality. The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. Monitoring and enforcement. The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

### Information Categories Covered in Privacy Protections

Organizations have a responsibility to keep a variety of data collected secure and private. A few of the most common types of data requiring protection are personally identifiable information (PII) and protected heath information (PHI).

PII is broadly defined as any information that can be used to identify, contact, or locate a specific person. The National Institute of Standards and Technology further specifies that PII is “any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.”

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient’s consent or knowledge.

HIPAA defines PHI as data or documentation including the following 18 identifiers:

1. Names
2. Geographic identifiers (more specific than State)
3. Dates specific to an individual (other than year only)
4. Phone numbers
5. Email addresses
6. Fax numbers
7. Social Security numbers
8. Medical record numbers
9. Health insurance beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers (e.g., license plate or vehicle numbers)
13. Device serial numbers
14. Web URLs
15. IP address numbers
16. Biometric identifiers (such as finger, retinal, and voice prints)
17. Full face images
18. Any other number, characteristic, or code unique to an individual

PHI that is created, received, stored, or transferred in an electronic form is often referred to as ePHI. The same privacy protections needed for PHI are required for ePHI.

### Deliverables

1. Privacy Policy
2. Vulnerability Assessment for Control Environment
3. Penetration Test Audit Report

# Security

The security principle refers to protection of system resources against unauthorized access. Access controls help prevent potential system abuse, theft or unauthorized removal of data, misuse of software, and improper alteration or disclosure of information.

Security for Nexelus is implemented in following areas:

## IT Security

Nexelus application is deployed in Microsoft Azure environment. Microsoft Azure is Microsoft's public cloud computing platform. It provides a range of cloud services, including compute, analytics, storage, and networking. Users can pick and choose from these services to develop and scale new applications or run existing applications in the public cloud.

With a 99.99% System Availability target, Microsoft Azure is based on a high availability architecture. With a broad set of international certifications and industry-specific compliance standards, Azure Cloud strictly adheres to global compliance standards. Certifications include ISO 27001, FedRAMP, SAS70, SOC 1, and SOC 2. To further ensure data security, all data and log files are backed up on a regular basis with tapes stored off-site. Please refer to the following link for more information regarding hosting compliance:

<http://azure.microsoft.com/en-gb/support/trust-center/compliance/>

## Application Security

Annexure 1  
Checklist for SOC 2

[To be done]

Annexure 2

Availability Control Mapping