Risk Assessment and Management

SOC 1 Type II Document

esm_logo.jpg

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

**10/16/2021**

# Document Information

The following table shows the details for document creation, review, approval, and effective date.

| **Category** | **Information** |
| --- | --- |
| Work Product: | Risk Assessment and Management - SOC 1 Type II Document |
| Project Name: | Security Manual |
| Function Name: | SOC 1 Type II Document |
| Version: | 1.0 |
| Status: | Draft |
| Author(s): | Tauseef Shahzad |
| Reviewer(s): | Asim Jameel |
| Approver(s): | Imran Rahman |
| Control Status: | CONTROLLED, PROTECTED |
| Disclaimer: | This document contains confidential information. Do not distribute this document without prior approval from Nexelus. |

# Revision History

The following table is used for revision details of this document.

| **Author(s)** | **Date** | **Version** | **Description of Change** |
| --- | --- | --- | --- |
| Tauseef Shahzad | October 10, 2021 | 0.1 | Initial Draft |
| Tauseef Shahzad | October 17, 2021 | 1.0 | Formatting and layout changes |
| Imran Rahman | August 29, 2022 | 1.1 | Review and few minor updates |

# Table of Contents

Contents

[Document Information ii](#_Toc112766617)

[Revision History iii](#_Toc112766618)

[Table of Contents i](#_Toc112766619)

[Scope 1](#_Toc112766620)

[Terms and Definitions 2](#_Toc112766621)

[Nexelus Security System (NSS) 2](#_Toc112766622)

[Security Domains 2](#_Toc112766623)

[Nexelus Staff 2](#_Toc112766624)

[Network Services 2](#_Toc112766625)

[Risk Management 4](#_Toc112766626)

[Policy 5](#_Toc112766627)

[Procedure for Risk Assessment 6](#_Toc112766628)

[Risk Identifying Procedure 6](#_Toc112766629)

[Identification of Risk Assessment Team 7](#_Toc112766630)

[Frequency of Risk Assessment 8](#_Toc112766631)

[Risk of disclosure/other risks not identified in the asset risk assessment sheet 8](#_Toc112766632)

[Identification of Risk Assessment Team 8](#_Toc112766633)

[Frequency of Risk Assessment 9](#_Toc112766634)

[Nexelus Objectives for Risk Management 10](#_Toc112766635)

[Risk Treatment Plan 11](#_Toc112766636)

[Goals of Risk Management at Nexelus 11](#_Toc112766637)

[What Benefits Will a Risk Management Plan provide? 11](#_Toc112766638)

[Risk Management Structure and Responsibilities 12](#_Toc112766639)

[Implementation 12](#_Toc112766640)

[Timeframe 13](#_Toc112766641)

[Monitoring and Review 13](#_Toc112766642)

# Scope

At Nexelus, security and privacy of your data is one of our key focus points. Data protection is a foundational building block in gaining and maintaining your trust.

Nexelus implements a robust security program spanning from secure system architecture through training and teaching employees security and privacy best practices. We believe in creating a culture of security awareness and understanding that security doesn’t have to be difficult.

**Reference**

SSAE-18 SOC 1 Type II – Requirements

# Terms and Definitions

Other than terms and definitions given in SSAE 18 – SOC 1 Type II, following terms and definitions are used in Nexelus Security System (NSS) implementation:

### Nexelus Security System (NSS)

All security procedures and policies as defined under Security and Compliance Initiative, and/or other security procedures and policies as defined and implemented at Nexelus.

### Security Domains

The security domain is a discrete logical and / or physical area that is subject to security controls to protect it from all entities outside the domain. For the SOC 1 Type II System the security domain is limited to Nexelus premises.

The location is defined as follows:

* The space within the physical structure bound by, and including, walls, ceiling, floor, doors, and windows.
* All equipment within the physical domain detail mentioned in Asset Identification and Classification Document.

Reference(s):

* Network Security and Access Control Procedure
* Capacity and change Management Procedure

### Nexelus Staff

All personnel employed / contractual engaged by Nexelus are required to follow the policies and procedures as defined in Nexelus Security Manual by management in line with strategic security needs.

### Network Services

Network services required by our network infrastructure are as follow:

* Internet Connectivity from ISP.
* Host based Protection against malware and Virus.
* Switches
* Host based Application Control
* Active Directory
* E-mail Scanning Services
* Patch management service to update all servers/workstations.
* Application and Database servers.
* Log Management.
* Biometric Access Control
* Office 365

# Risk Management

Nexelus recognizes the need for risk management to feature as a consideration in strategic and operational planning, day-to-day management and decision making at all levels in the organization.

Nexelus is committed to managing and minimizing risk by identifying, analyzing, evaluating, and treating exposures that may impact on the organization achieving its objectives and/or the continued efficiency and effectiveness of its operations. Nexelus incorporates risk management into its institutional planning and decision-making processes. Risk management is included as a consideration in development, and operational planning as a delegated line management responsibility. Nexelus staff must implement risk management according to relevant legislative requirements and appropriate risk management standards.

Risk assessments can be conducted on any entity within Nexelus or any outside entity that has signed a Third-Party Agreement with Nexelus. RAs can be conducted on any information system, to include services, applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

## Policy

The execution, development and implementation of remediation programs by Nexelus Security System (NSS) Team for Nexelus informational assets, quality and services. Employees are expected to cooperate fully with any risk assessment being conducted on all informational assets for which they are held accountable. Employees are further expected to work with the Nexelus Security System (NSS) Team in the development of a remediation plan.

## Procedure for Risk Assessment

The risk assessment procedure of Nexelus is as follows:

### Risk Identifying Procedure

Following is the process of identifying the risk on informational assets of Nexelus.

Identification of Informational Assets:

NSS Team identifies the informational assets owned by Nexelus. These assets are listed in our Nexelus Asset Register. These assets are divided into following categories:

• Information

• Paper

• People

• Software

• Hardware/ Physical

Each asset is evaluated on the basis of CIA (Confidentiality, Integrity and Availability).

Asset Value = C(onfidentiality) \* I(ntegrity) \* A(vailability).

Each of these asset parameters are assigned criticality values as Low, Medium and High.

Low = 1, Medium = 2, High = 3

If Asset Value is greater 18 then the asset score is 3, If Asset Value is greater than 6 and less than 18 then asset score is 2 else it will be one.

Assets having asset score 2 and 3 are critical to Nexelus.

**Reference**: List of Assets Nexelus

#### Asset Risk Assessment

After having a complete asset register we develop Asset Risk Assessment Workbook. Possible risks associated with each asset and its vulnerabilities are identified. The risk is assessed on the basis of risk probability and its impact on the company. The definitions of Threats and Vulnerabilities are as follow at Nexelus:

**Threats**

Damage or loss to information assets

**Vulnerability**

Weak links that could be exploited by the threats

**Asset risk rating = Asset Score \* Probability \* Impact**

Asset score is derived from the List of Asset. Probability can take following values (High = 3, Medium = 2 and Low =1). The impact can also be categorized as (High = 3, Medium = 2 and Low =1).

For the risk treatment we do one or multiple of the following: Reduction, Avoidance, and Transfer.

**Reduction:**

These are the measures to reduce the occurrence of certain risk at Nexelus assets.

**Avoidance:**

These are the measures taken to avoid or minimize the risk impact on the assets, even if the risk occurs as well.

**Transfer:**

This risk treatment method is used to transfer the risk to any third party to minimize the risk impact.

**Reference:** Asset Risk Assessment

#### Risk Reporting

NSS is responsible to analyze the risk of existing and new purchased informational assets. But the risk can be reported or informed by any employee through email or by any means which are quickest to reach NSS.

#### Acceptance

This technique recognizes the risk and its uncontrollability. Acceptance is a “passive” technique that focuses on allowing whatever outcome to occur without trying to prevent that outcome. This technique is normally used for “low” or “very low” risks where a scope efficient means of reducing the risk is not apparent. With the mutual consent of top management and risk owner’s information security risk acceptance level is decided at medium residual risks which is mathematically presented as 2 in numeric form. The residual risk level which is above 2 or high is required contingency plans which are made accordingly with respect to risk.

#### Risk Sources

Risk sources are interfaces and dependencies of services provided by Nexelus to internal and external stakeholders.

### Identification of Risk Assessment Team

The procedure for risk assessment starts with identification of the team which will analyze the risk levels. Our NSS team has assigned Risk Assessment at Nexelus for its assets in management review meeting to **Network Manager**. Team selection criteria are as follow:

1. Management is also involved in risk management.
2. NSS Lead should fulfill the requirements:
3. More than 5 years if experience in network and infrastructure security.
4. More than 2 years job experience in the company.
5. Must be involved in implementation process of NSS.
6. NSS Member should fulfill the following requirements:
7. Must have completed Implementer in-house training
8. More than 1-2 years job experience in the company or mandated by President, General Manager and/or CEO OR CTO.
9. Must be from Development, Quality Assurance, HR, or Networks Department.
10. Must be involved in implementation process of NSS.
11. Must have experience to deal with compliances for at least 1 year.

### Frequency of Risk Assessment

It is decided by management that risk assessment will be performed once before internal audit to evaluate all risks against existing and new assets.

### Risk of disclosure/other risks not identified in the asset risk assessment sheet

In case of following disclosures of information, disciplinary action will be taken against the non-compliant personnel:

1. HR Records
2. Clients’ Data
3. Projects’ Data
4. Other confidential information

### Identification of Risk Assessment Team

The procedure for risk assessment starts with identification of the team which will analyze the risk levels. NSS Team has assigned the duties for Risk Assessment at Nexelus for its assets to Network/Systems Manager in the management review meeting. Team selection criteria are as follow:

1. Management is also involved in risk management.
2. NSS Lead should fulfill the requirements:

* Must have completed Implementer training
* More than 2 years job experience in the company
* Must be from Dev/ QA/ HR department
* Must be involved in implementation process of ISMS

1. NSS Member should fulfill the following requirements:

* Must have completed Implementer in-house training
* More than 1-2 years job experience in the company or mandated by President, General Manager/CEO OR CTO
* Must be from Development, Quality Assurance, Human Resource or Networks/Systems Department
* Must be involved in implementation process of NSS
* Must have experience to deal with compliances

### Frequency of Risk Assessment

It is decided by management that risk assessment will be performed once before internal audit (once year) to evaluate all risks against existing and new assets.

Risk of disclosure/other risks not identified in the asset risk assessment sheet

In case of following disclosures of information, disciplinary action will be taken against the guilty:

* HR Records
* Clients’ Data
* Projects’ Data
* Other confidential information

## Nexelus Objectives for Risk Management

Nexelus is committed to the management of risk to continue to protect its:

1. Customers, clients and stakeholders
2. Employees, and their skills
3. Environment
4. Quality of service
5. Assets and intellectual property
6. Contractual and statutory obligations
7. Image and reputation

Risk management is a key part of improving our business and services to be a leading Organization. Our aim is to achieve best practice in controlling all the risks to which our business is exposed. To achieve this aim, risk management standards are created, maintained, and will be continually improved. This will involve risk identification and risk evaluation linked to practical and cost-effective risk control measures commensurate with our business.

Risk management is a continuous process demanding awareness and proactive action from all Nexelus employees and outsourced service providers to reduce the possibility and impact of accidents and losses, whether caused by Nexelus or externally. Risk Management is a core responsibility for all managers. Suitable risk management activities are incorporated into our business planning, operations and the management of our contractors and service providers. The scope of these activities encompass:

1. Education and training in risk management for staff
2. Developing risk management standards
3. Helping to prioritize and schedule risk control improvements in each of Nexelus business units
4. Reporting to Nexelus Management on risk improvement and compliance

Our challenge for the future is to infuse risk management into our culture, our everyday business operations and those of our contractors and business partners. Everyone’s involvement and support are critical to an effective result.

## Risk Treatment Plan

### Goals of Risk Management at Nexelus

The goals behind introducing Risk Management into Nexelus are three fold:

* To provide an assurance that Nexelus has identified its highest-risk exposures and has taken steps to properly manage these.
* To ensure that Nexelus business planning processes include a focus on areas where risk management is needed.
* To establish a process across Nexelus that will integrate the various risk control measures that Nexelus already has.

### What Benefits Will a Risk Management Plan provide?

Risk Management will assist us to achieve the Nexelus’ corporate objectives by:

* Integrating the various risk control measures that the Nexelus currently uses into one holistic view of what the Nexelus is doing to minimize its risk exposures. This single view will show priorities and any gaps that need to be addressed.
* Implementing a visible, formalized and consistent process for managing the Nexelus’ exposures to risk, thereby supporting continuous improvement in the Nexelus programs and providing an assurance of more effective outcomes.
* Incorporating identified risk management solutions into planning and administrative processes resulting in more structured, accountable and effective business planning and project management.
* Building on existing risk management strategies such as our administrative, engineering, contractual, safety and quality management controls; and
* Encouraging staff and managers to think about risk, and risk management, in their day-to-day work; in program, contractor and project management; and in forward planning activities.

Risk Management is applied to all the Nexelus activities, including those delivered on the Nexelus behalf by external service providers and project contractors. This helps us to:

* Ensure that the quality and reliability of services and other program outputs are of a very high standard.
* Ensure services meet requirements and are delivered within cost and schedule.
* Protect employees, property, information and all other assets.
* Comply with all legal requirements relative to areas of risk.

## Risk Management Structure and Responsibilities

Management, NSS team and department managers are responsible for managing risk within their span of control, for promoting the application of risk management by contractors, and assisting with the identification of global or broadly based risks that could impact on the Nexelus as a whole.

Management appoints NSS Risk Assessment Team to act as a focal point for communication and coordination of risk assessment, awareness training and risk management assurance.

A team has been established by the Nexelus management and is responsible for:

1. Co-coordinating the regular formal updating of Risk Assessment Workbook and Risk Treatment Plans and compiling a master set.
2. Maintaining corporate risk and risk control information.
3. Ensuring that all relevant risk areas are considered including those emanating from the services of external providers and contractors.
4. Analysis and reporting to the Nexelus Management via meetings or emails.

The identification and review of critical risk areas within the Nexelus and the implementation of the Nexelus Risk Management Plan will also be the subject of internal audit protocols, to be applied by Internal Audit with the oversight and approval of the management.

### Implementation

Nexelus achieves the above requirements by developing suitable analysis and documentation of risks in corporate activities,

1. Identify risks in the immediate work area and of wider impact.
2. Assess the probability of the risk eventuating.
3. Assess the likely impact on the work area and/or organization if the risk occurs.
4. Determine an overall risk rating based on probability and impact.
5. Record any existing controls or strategies which aim to reduce the risk.
6. Determine if the risk exposure is acceptable or not.
7. Determine further action plans and contingency plans to manage the risk where appropriate.
8. Monitoring and reviewing risk in external services, and where appropriate, providing input to contractors’ risk management processes,
9. Periodically reviewing and updating the Risk Assessment Workbook to account for changes in risks and related issues.

Satisfactory risk management is achieved when training has been completed by all relevant personnel, when risk assessment of all critical programs and risk exposures has been concluded.

### Timeframe

All team members have recently received a copy of this Risk treatment Plan containing the Nexelus Policy on Risk Management, guidelines on Risk Management implementation and Nexelus initial Risk Assessment Workbook.

Managers are requested to take the time to discuss the Risk Treatment Plan with their staff to ensure that they are aware of Nexelus Risk Management Policy and their role in implementation of the Risk Management Process.

The timeframe for further development and implementation of risk management within 6 months of initiation of the process.

### Monitoring and Review

The monitoring, review and updating of Risk Registers, Mitigation and Contingency Plans will be coordinated by the NSS Team, in conjunction with Internal Audit, in line with their responsibilities under this Plan.