Nexelus Security Manual

SOC 1 Type II Document

esm_logo.jpg

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

**10/08/2021**

Document Details

## Document Information

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

| **Category** | **Information** |
| --- | --- |
| Work Product: | Nexelus Security Manual - SOC 1 Type II Document |
| Project Name: | Security Manual |
| Function Name: | SOC 1 Type II Document |
| Version: | 0.1 |
| 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 |
|  |  |  |  |

# Table of Contents

Contents

[Document Details ii](#_Toc87881244)

[Document Information ii](#_Toc87881245)

[Revision History ii](#_Toc87881246)

[Table of Contents i](#_Toc87881247)

[Scope 1](#_Toc87881248)

[Scope 1](#_Toc87881249)

[Reference 1](#_Toc87881250)

[Terms and Definitions 2](#_Toc87881251)

[Security Domains 2](#_Toc87881252)

[Nexelus Staff 2](#_Toc87881253)

[Network Services 2](#_Toc87881254)

[Control Environment 4](#_Toc87881255)

[Legal Framework for Security Policy 5](#_Toc87881256)

[Data and Information Sensitivity Policy 6](#_Toc87881257)

[Physical Environment Control 7](#_Toc87881258)

[Data Center Security 7](#_Toc87881259)

[Network Security 7](#_Toc87881260)

[Encrypted Data In Transit 7](#_Toc87881261)

[Endpoint Security 7](#_Toc87881262)

[Vulnerability Management 7](#_Toc87881263)

[Remote Access Policy 9](#_Toc87881264)

[Remote Server Access 9](#_Toc87881265)

[Remote Database Servers 9](#_Toc87881266)

[Office 365 Accounts 9](#_Toc87881267)

[Access Controls and Policies 11](#_Toc87881268)

[Marking/Classification of Sensitive Information 11](#_Toc87881269)

[Information Media 11](#_Toc87881270)

[Information Access Policy 12](#_Toc87881271)

[Data Handling Policy 12](#_Toc87881272)

[Data Ownership 12](#_Toc87881273)

[Categories 12](#_Toc87881274)

[Owner Responsibilities 12](#_Toc87881275)

[Custodian Responsibilities 13](#_Toc87881276)

[User Responsibilities 13](#_Toc87881277)

[Clean Desk Policy 13](#_Toc87881278)

[Disposal/Destruction Policy 13](#_Toc87881279)

[Data Access Policy 14](#_Toc87881280)

[Data Backup Policy 15](#_Toc87881281)

[Backup Procedure 15](#_Toc87881282)

[Data Backup & Recovery Procedure 15](#_Toc87881283)

[Project Content Backup 15](#_Toc87881284)

[E-Mail Backup of Leaving Employee 16](#_Toc87881285)

[Project Content Restore 16](#_Toc87881286)

[How to Restore Outlook Emails 16](#_Toc87881287)

[Data Retention Policy 17](#_Toc87881288)

[E-mail Data Retention 17](#_Toc87881289)

[Financial and HR Data Retention 17](#_Toc87881290)

[General Data Retention 17](#_Toc87881291)

[TFS Data Retention 18](#_Toc87881292)

[Source Code Retention 18](#_Toc87881293)

[Security and Awareness Training Policy 19](#_Toc87881294)

[Business Continuity Plan 20](#_Toc87881295)

[Significant Business Disruptions (SBD) 20](#_Toc87881296)

[Internal SBDs 20](#_Toc87881297)

[External SBDs 20](#_Toc87881298)

[Approval and Execution Authority 20](#_Toc87881299)

[Assumptions 20](#_Toc87881300)

[Business Impact Analysis 21](#_Toc87881301)

[Disaster Recovery Plan 22](#_Toc87881302)

[Nexelus Office 22](#_Toc87881303)

[Key Staff 22](#_Toc87881304)

[Recovery Time Objective (RTO) 22](#_Toc87881305)

[Recovery Point Objective (RPO) 22](#_Toc87881306)

[Maximum Tolerable Outage (MTO) 23](#_Toc87881307)

[Critical Business Services 23](#_Toc87881308)

[Business Continuity and Disaster Recovery Management Team 23](#_Toc87881309)

[Plan Maintenance Procedure 24](#_Toc87881310)

[Disaster Recovery Steps 24](#_Toc87881311)

[Restore Servers in Azure 25](#_Toc87881312)

[A. Create new Servers 25](#_Toc87881313)

[B. Recover Databases 25](#_Toc87881314)

[C. Recover Web Application (Web Server): 26](#_Toc87881315)

[Incident Reporting Policy 32](#_Toc87881316)

[Types of Incidents 32](#_Toc87881317)

[Critical Incidents 33](#_Toc87881318)

[Internal Reporting 33](#_Toc87881319)

[External/Client Reporting 33](#_Toc87881320)

[Collection of Evidence 34](#_Toc87881321)

[Problem Management 34](#_Toc87881322)

[Root Cause Analysis 34](#_Toc87881323)

[Knowledge Base 34](#_Toc87881324)

[Communication 35](#_Toc87881325)

[Enforcement 35](#_Toc87881326)

[Internal Audit 36](#_Toc87881327)

[Audit Planning 36](#_Toc87881328)

[Audit Execution 36](#_Toc87881329)

[Audit Reporting 37](#_Toc87881330)

[Follow-up Audit 37](#_Toc87881331)

[Independent Review of SOC Compliance 37](#_Toc87881332)

[Procedure for Control of Nonconforming Products 38](#_Toc87881333)

[Scope 38](#_Toc87881334)

[Roles and Responsibilities 38](#_Toc87881335)

[General Manager and QA Lead 38](#_Toc87881336)

[Network and Security Manager 38](#_Toc87881337)

[Principal Internal Auditor 38](#_Toc87881338)

[Nexelus Employees 39](#_Toc87881339)

[Classification of Observations and Non-Conformity 39](#_Toc87881340)

[Internal Audit Procedure 39](#_Toc87881341)

[Identification of Nonconformities 39](#_Toc87881342)

[Authorization for NCRs Closing 40](#_Toc87881343)

[Maintenance of Records 41](#_Toc87881344)

[Procedure for Corrective and Preventive Actions 42](#_Toc87881345)

[Scope 42](#_Toc87881346)

[Procedure 42](#_Toc87881347)

[Corrective Action 42](#_Toc87881348)

[Preventive Actions 42](#_Toc87881349)

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

## Scope

This manual is applicable to all the activities of SSAE 18 (SOC 1 Type 1) at Nexelus as mentioned in this manual.

## 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 use in ISMS implementation:

### 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 and HiQuSystems 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):

1. 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 laid by management in line with strategic security needs.

* Network services required by the defined network infrastructure.
* Data Access and Retention Policy
* Acceptable Use Policy
* Clean Desk Policy
* Code of Conduct Policy
* Personnel Security Policy
* User identification, Authentication and Authorization Policy
* Training and Onboarding Policy

### Network Services

Network services required by our network infrastructure are as follow:

* Internet Connectivity from ISP.
* Host based Protection against malware and Virus.
* Web filtering.
* 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

# Organization and Management

## Organizational Structure

## Job Role Description

Job role descriptions are maintained separately in Job Role Description Manual document

## Acceptable Use Policy

## Code of Conduct Policy

## Personnel Security Policy

## User Identification, Authentication, and Authorization Policy

## Employee Hiring and Screening Process

## Visitor Log policy

## Confidentiality Policy

## Clean Desk Policy

A clean desk policy is part of an overall company security strategy. It is, as it states, about keeping your work desk clean. In general, a clean desk policy will mandate that at the end of each working day, that employees clear their desk. This means, for example, securely disposing of Post It notes, keeping written notes in a safe place, and ensuring that any removable media isn’t just lying around. Keep sensitive information from view of unauthorized people;

* Erase whiteboards,
* Do not leave any client data printouts in view on tabletop. It should be kept in drawer while not in use.
* Password protected screen saver must be applied on all desktops with 10 minutes timeout
* No document or its link should be placed on computer Desktop
* Add more clauses..

Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

# 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 will incorporate 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.

# Secure Systems Management Policy

## Data and Information Sensitivity Policy

The Information Security Management System exists for various levels of classification. All documentation will be clearly marked for appropriate access control as defined by its classification and handled in accordance with Nexelus Data Classification and Labeling Sheet.

Reference(s):

* Data Handling Policy
* Data Backup Policy
* Data Retention Policy
* Acceptable Encryption and Key Management Policy
* Remote Access Policy
* End User Encryption and Key Management Policy

## Physical Environment Control

### Data Center Security

Nexelus cloud-based services and platforms are hosted on Microsoft Azure. Azure datacenters meet security regulations and standards with industry-leading physical and environmental controls. Nexelus solutions benefit from a datacenter and network architecture built to meet the requirements of the most security-sensitive organizations. Azure is compliant with a wide range of standards, laws and regulations including CIS, CSA, various ISO standards, WCAG, SOC 1, SOC 2 and SOC 3.

References:

<https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-soc-1>

<https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-soc-2>

<https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-soc-3>

## Network Security

Nexelus Management is committed to maintaining and improving the security of its environments. Maintaining secure network environments requires continuous attention. We regularly review the services and information accessible on our servers and their security requirements.

Security controls are implemented within networks using a strict access control policy. Access points into the network are blocked apart from those deemed essential or business critical.

### Encrypted Data In Transit

All transmission of data over the internet is communicated via HTTPS. Our services support Transport Layer Security 1.3 encryption, providing the necessary levels of confidentiality, integrity and non-repudiation.

### Endpoint Security

Malware protection suites are installed and managed from a centralized location including monitoring and logging of events.

### Vulnerability Management

Nexelus performs various security tests and audits for the infrastructure and application. Tests include amongst others:

* Static code analysis
* Dynamic code analysis
* Network vulnerability assessment
* Network penetration testing
* Application vulnerability assessment
* Penetration testing of multiple environments and solutions

### Remote Access Policy

The purpose of this policy is to define the activities associated with the provision of access security for employees and authorized nonemployees working remotely to protect Nexelus Information System, information systems, networks, data, databases, and other information assets from cybersecurity events that may occur while in use by remote workers. Additional policies governing data protection activities will be addressed separately.

The scope of this remote access security policy is all IT systems, software, databases, applications, and network resources needed by the Company to conduct its business, and the access security controls needed to protect those assets when being accessed remotely. The policy is applicable to all Company employees, contractors, and other authorized third-party organizations.

### Remote Server Access

All users will access remote servers by their individual accounts for logging and tracking purpose. Minimum Access policy will be applied and users will be provided with RDC access to relevant servers only. All remote server access will be performed using official desktop and laptops only. The communication will be secured using VPN. Two-factor access will be applied on remote desktop access.

No shared passwords will be used to access remote servers.

### Remote Database Servers

All relevant employees will have limited Database access through their individual database user login credentials. Remote Desktop access will be provided to Database Manager and general Manager only. Remote Desktop and Database access will be available through VPN. Two-factor access will be applied on remote desktop access.

### Office 365 Accounts

All office 365 accounts will be secured using strong password and two-factor authentication using SMS or Microsoft authenticator as secondary authentication method.

## Data Backup Policy

Nexelus keeps backup of all the electronic data which will be ready to use in case of any disaster or at time of need. Electronic data includes software & application source code and employee emails.

### Backup Procedure

All Nexelus production, test, and release servers are maintained on Microsoft Azure. Backup for servers is maintained on Microsoft Azure Cloud for last 15 days. This backup is taken automatically by Azure on daily basis and maintained on cloud. The servers can be reconstructed on-the-fly from these backups.

Local Development server backups are maintained on external hard drives by Network Administrator. Data backup log sheet will be updated after each back up by the Senior Network Engineer and verified by the General Manager.

There is one set of our backup media (i.e. hard disk) which is then transferred safely at our offsite data backup location. This data backup site is at sufficient distance away to escape any damage due to any disaster at our main site.

DR Recovery Site Requirements will be asked in case of data backup

### Data Backup & Recovery Procedure

All electronic backups must conform to the following procedures:

* All data, source code files must be adequately and systematically backed up as per our policy.
* One set of backups is made.
* The backup is precisely labeled (folder); we use the date label on which the backup is taken (e.g., [Label]- yyyymmdd).
* The data(s) are kept in order depending on the date of backup taken.
* This will be stored safely at the backup site.
* With every backup taken, Senior Network Engineer updates the backup log.

Reference(s)

* Backup Log

*Log sheet is signed by issuance and receiving authorities.*

### Project Content Backup

It is the responsibility of the Senior Network Engineer to ensure that they have suitable backups of all the projects. The following should be backed up:

* All projects’ data on TFS
* All SOC related data on TFS

### E-Mail Backup of Leaving Employee

Senior Network Engineer is responsible to take immediate backup of e-mails of employee leaving the organization. He will keep that backup/ archive data with other records and maintain ex-employee data on network storage. The information of ex-employee is not available to all employees working in the organization. It can be used with prior permission of General Manager by others in terms of requirements and then Senior Network Engineer will provide this data to them.

### Project Content Restore

In cases where a non-catastrophic issue requires a data restore, the Senior Network Engineer is responsible for performing the restore using backups. Senior Network Engineer will manually restore repository to a prior state if provided a viable backup of project repository.

### How to Restore Outlook Emails

Restoration of email accounts requires a .PST file to be backed up, to restore emails, contacts, and other data from a backup copy of an Outlook PST file:

1. Select File, then Import and Export from the menu in Outlook.
2. Select Import from another program or file.
3. Click Next.
4. Highlight Personal Folder File (PST).
5. Click next again.
6. Now use the Browse button to select the backup copy of the PST file you want to recover from your backup location.
7. Make sure Replace duplicates with items imported is selected.
8. Click Next.
9. Finish the import process with Finish.

## Legal Framework for Security Policy

Nexelus acknowledges the complexity of legal requirements found in the global networking environment created by the Internet. NEXELUS Security System was drafted to meet, and in some instances exceed the protections found in existing laws and regulations. If any Nexelus Security System component conflicts with existing laws or regulations, this observation must be promptly reported to the management for taking corrective actions.

Reference(s):

* Procedure for Compliances and SLA Review

## Data Retention Policy

Nexelus Data Retention Policy is intended to define what data should be retained and for how long. The data covered in these guidelines includes, but is not limited to, Administrative, Fiscal, E-mail, General, Temporary, Database Backups, TFS, Source Code, Test Data, Log Files etc.

All employees should familiarize themselves with the data retention policy relevant to them.

There are two broader categories of data (Paper Data and Electronic Data). All paper data will be retained by Admin Office & SOC Team with the approval of General Manager. Network Administrator will ensure all electronic data backup according to data retention policy and hand over the archives to Admin Office & SOC Team for retention on site and off site.

### E-mail Data Retention

Nexelus emails data of all ex-employees are backed up in DVDs and these are kept in storeroom for a period of three years. Current employees’ data email data is resided in Microsoft Office 365 Server.

### Financial and HR Data Retention

Nexelus Financial and HR Record is all information related to revenue and expense for the company. All paper record will have retained by Admin Office for the period of three years. To ensure Financial data secrecy, it is retained by General Manager. A table below explains that which type of data needs to be retained.

|  |  |  |
| --- | --- | --- |
| Item. | Record Types | Retention Period |
| 1 | Financial Data | ? |
| 2 | HR Data | ? |
| 8 | Inventory Records | ? |
| 9 | Invoices to customers | ? |
| 11 | Purchase Records | ? |
| 12 | Employee Personal Files | ? |
| 13 | Manuals, User Guides | ? |

### General Data Retention

Nexelus general record/correspondence covers information that relates to customer interaction and the operational decisions of the business. Admin officer will retain paper data of this category. The individual employee is responsible for electronic data retention of General Correspondence.

### TFS Data Retention

All Data on TFS will be retained from the day it is started.

### Source Code Retention

Source Code data will never be deleted.

## Data Breach Policy

A data breach response plan, also known as a security breach response plan or a cyber incident response plan, helps businesses appropriately respond to a cybersecurity attack by providing the necessary steps to respond in a straightforward, documented manner. This policy relates to all personal and special categories (sensitive) data held by the organization regardless of format. This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents across the organization.

### Types of breach

For the purpose of this policy, data security breaches include both confirmed and suspected incidents.

An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately, and has caused or has the potential to cause damage to the University’s information assets and / or reputation

An incident includes but is not restricted to, the following:

* loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad / tablet device, or paper record);
* equipment theft or failure.
* system failure.
* Unauthorized use of, access to or modification of data or information systems;
* Attempts (failed or successful) to gain unauthorized access to information or IT system(s);
* unauthorized disclosure of sensitive / confidential data;
* website defacement.
* hacking attack.
* unforeseen circumstances such as a fire or flood;
* human error.
* ‘blagging’ offences where information is obtained by deceiving the organization who holds it.

### Reporting an incident

Any individual who accesses, uses or manages the University’s information is responsible for reporting data breach and information security incidents immediately to Network Administrator and GM. If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. The incident is reported as per Incident Reporting Policy.

# Information and Communication

Access Controls and Policies is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of the company without proper authorization. The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Nexelus confidential information, this policy also set forth the standards for data labeling.

## Marking/Classification of Sensitive Information

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Confidential" may be written or designated in a conspicuous place on or in the information in question. Even if no marking is present, Nexelus information is presumed to be "Confidential" unless expressly determined to be Nexelus Public information by an Nexelus employee with authority to do so.

### Information Media

#### Hard Copies

1. Hard copies should be marked to identify the data classification.
2. The Document Classification Sheet contains the Classification information, which can have any of the Classification categories.
3. Any document left unmarked, will be considered as non-sensitive.

#### Documents Of External Origin

Documents of External Origin / Customer Property are not marked physically but have been accounted for in the Data Classification sheet.

#### Soft Copies of Data, Software, and/or Other Information Systems

Soft copies of client requirements, project documentation, Application Code, Database Schema are not marked physically but have been accounted for in the Data Classification sheet.

## Information Access Policy

#### Access

Nexelus employees, contractors, people with a business need to know.

#### Distribution within Nexelus

Standard interoffice mail approved electronic mail and electronic file transmission methods.

#### Distribution outside of Nexelus internal mail

This kind of outbound information will only be sent through Nexelus mail server only. If the data is large, then we will use approved electronic file transmission methods [VPN, sftp, more].

#### Electronic distribution

No restrictions except that it be sent to only approved recipients.

## Data Handling Policy

Data is one of the potentially most valuable and most damage prone assets owned by Nexelus. It is also one of the most intangible assets of ours. Protection of the Confidentiality, Integrity, and Availability of data in all forms and through all life cycles is a cornerstone to a successful Information Security process.

### Data Ownership

Customer Data, and information which has been entrusted to Nexelus, must be protected in a manner commensurate with its data classification label. Security measures must be employed regardless of the media on which information is stored (paper, overhead transparency, computer bits, etc.), the systems that process it (personal computers, firewalls, voice mail systems, etc.), or the methods by which it is moved (electronic mail, face-to-face conversation, etc.). Information must also be consistently protected no matter what its stage in the life cycle from origination to destruction.

### Categories

Nexelus has established three categories, at least one of which applies to each worker. These categories are Owner, Custodian, and User. These categories define general responsibilities with respect to data security.

### Owner Responsibilities

Information Owners are the Department Managers, Top Management, or their delegates within Nexelus who bear responsibility for the acquisition, development, and maintenance of production applications which both process customer information and defining the Nexelus infrastructure. All production application system information has a designated Owner. For each type of information, Owners designate the relevant classification level, define which users will be granted access, as well as approve requests for various ways in which the information will be utilized.

### Custodian Responsibilities

Custodians are in physical or logical possession of either Nexelus information or information that has been entrusted to Nexelus. While Support department and Information Technology Department staff members clearly are custodians, local system administrators are also Custodians. Whenever information is maintained only on a personal computer, the user is necessarily present along with the custodian. Each type of production application system information must have one or more designated Custodians. Custodians are responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and making back-ups so that critical information will not be lost. Custodians are also required to implement, operate, and maintain the security measures defined by information owners.

### User Responsibilities

Users are responsible for familiarizing themselves with and complying with all Nexelus policies, procedures, and standards dealing with information security. Questions about the appropriate handling of a specific type of information should be directed to either the Custodian or the Owner of the involved information. Users are increasingly placed in a position where they must handle information security matters that they did not handle in days gone past. The new security concerned environment forces users to play security roles that they had not previous had to play.

## Disposal/Destruction Policy

Deposit outdated paper information to Admin manager who will properly destroy it with paper shredder; electronic data should be expunged/ cleared. Reliably erase or physically destroy media.

## Data Access Policy

Access to data is controlled and provided to teams and members with specific business needs. Regular permission review is performed to prevent permission overlap, permission creep or conflict of interests. All data access breaches and loopholes discovered during normal operations, monitoring controls, internal and external audits are escalated and resolved through incident reporting, escalation, and resolution procedure.

Data Access Register is maintained for data access classification and assignment to resources.

# Training Policies

## Onboarding of New Employees

## Security and Awareness Training Policy

Nexelus perform various activities to improve the awareness around security and privacy. Some of these include annual awareness training sessions for both security and privacy.

# Business Continuity and Disaster Recovery

## Business Continuity Plan

Nexelus Business Continuity Policy is to respond to significant business disruptions by safeguarding employees’ lives and company property, quickly recovering, and resuming its operations by restoring its critical business services, protecting all the company’s information and records, and allowing our customers to transact business.

If we determine we are unable to continue our business, we will assure customers prompt access to their information held with Nexelus.

### Significant Business Disruptions (SBD)

Nexelus Business Continuity Plan anticipates two kinds of SBDs, internal and external.

#### Internal SBDs

These internal disruptions affect only our company’s ability to communicate and do business, such as a fire in our building, hardware or software failure or sudden death of an employee.

#### External SBDs

These prevent the overall operation of the markets or several companies to operate and continue their operations. Examples include terrorist attack, a city flood, a wide-scale earthquake, or a regional disruption (civil unrest or War). Our response to an external SBD relies more heavily on other organizations and systems such as Law Enforcement Agencies (Police, FIA), Fire brigade, Rescue 1122 or National Disaster Response Unit.

#### Approval and Execution Authority

General Manager is responsible for approving and executing this plan. He/she is also responsible for conducting the annual review during annual review meeting for SOC Compliance. This approval and execution authority personnel can be changed in case the existing person leaves the company or as Per Top Management decisions in annuals review meetings.

### Assumptions

The Business Continuity Plan is predicted on the validity of the following four assumptions:

* The situation that causes the disaster is localized to the data processing facility of operations and system in the building or space housing the functional area; or to the communication systems and networks that support the functional area. It is not a general disaster, such as an earthquake or flood affecting a major portion of Islamabad Pakistan.
* It should be noted that the plan would still be functional and effective, if third party restores relevant services, for example, electricity services, water and building management etc.
* The plan is based on the availability of the hot sites or the backup resources. The accessibility of these or equivalent backup resources, is a vital requirement.
* The plan is a document that reflects the changing environment and requirements of the Nexelus. Therefore, the plan requires the continued allocation of resources to maintain and to keep it in a constant state of readiness.

The Business Continuity Plan also provides its objectives, gains Senior Management support, and allocates the necessary time and resources to develop, exercise and maintain the plan. The following are the main objectives of the plan.

* Minimizing interruptions to business/service operations.
* Resuming critical operations within a specified time after a disaster.
* Assuring clients/customers that their interests and business are protected, to gain their confidence.
* Limiting the severity of the disruption.
* Expediting the restoration of services.
* Establishing awareness, so that management and staff understand the implications of a disaster upon services.
* A brief study of Business Impact Analysis, regarding Nexelus operations, and corporate customers businesses.

### Business Impact Analysis

[Blurbs]

## Disaster Recovery Plan

Nexelus Disaster Recovery (DR) plan is in place with the following objectives:

* In case of any significant business disruption, we will resume our critical business services within 48 hours from the decision to invoke disaster recovery.
* Nexelus recovery point objective is to restore our last period-end data, that is our last weekly backup.

A disaster is defined as an incident which results in the loss of computer processing at the Nexelus site to the extent that relocation to the alternate office location must be considered. A disaster can be a result from several accidental, malicious, or environmental events such as fire, flood, terrorist attack, human error, and software or hardware failures.

The primary objective of this Disaster recovery Plan is to ensure the continued operation of identified business critical systems in the event of a disaster. Since Development, QA and Production environments are hosted in Microsoft Azure, which is SOC compliant, there is no need to procure and deploy new servers for alternate location. This ensures that client operations will remain operational in case of a disaster. However, for back-office operations and development, following goals have been set:

### Nexelus Office

* To be operational at the alternate office location within six working days after the incident.
* To operate at the alternate office location for up to one month.
* To reinstate Nexelus facilities in the main Nexelus premises within the maximum working standby period.
* To minimize the disruption to Nexelus business.

### Key Staff

* Key staff is identified, and provided appropriate equipment to operate from home
* Appropriate security policies are in place for selected staff to work from home.

### Recovery Time Objective (RTO)

The Recovery Time Objective (RTO) is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption), to avoid unacceptable consequences associated with a break in business continuity.

### Recovery Point Objective (RPO)

The Recovery Point Objective (RPO) refers to the amount of data at risk. It is determined by the amount of time between data protection events and reflects the amount of data that potentially could be lost during a disaster recovery

### Maximum Tolerable Outage (MTO)

Additionally, there is an additional measure; the Maximum Tolerable Outage (MTO). The MTO is the maximum time that our business will survive from the disruption or interruption in critical business services.

Nexelus can survive without its critical business services for a maximum of one business day. In case of any incident BCDR (Business Continuity and Disaster Recovery) Team will conduct the impact analysis to evaluate the recovery time. If this recovery time is more than our MTO time, we will initiate our Disaster Recovery Plan.

### Critical Business Services

Nexelus manages client applications in cloud using Microsoft Azure Services. [blurbs]

It is also involved in software development and software support services. Both of these are our critical services and reason for offshore office. For this purpose, we need the following assets, data (source code) infrastructure, development and OS software and personnel to carry on and continue our business. These critical requirements of our business are as follows:

* Access to TFS (Server deployed in cloud).
* At least one Server Machine.
* At least one Internet connection.
* One telephone line.
* Wired and/or Wireless Local area Network infrastructure.
* xxx computers with installed OS and Visual Studio.

As part of our BCP and disaster recovery plan we will designate a backup site ready to use in case of any SBD (significant business disruption).

### Business Continuity and Disaster Recovery Management Team

Nexelus Security Team also acts as Nexelus Business Continuity Management Team consists of following personnel:

* CEO
* General Manager
* General Manager (Development)
* Senior System Architect
* Senior Network Engineer
* QA Lead

Nexelus Security Team will have an electronic copy of this plan stored on their respective Microsoft OneDrive account, so that in case of emergency they can use it for guidance.

### Plan Maintenance Procedure

Ensuring that the plan reflects ongoing changes to the resources is crucial. This task includes updating the plan and revising this document to reflect updates; testing the updated plan; and training the personnel. The Business Continuity Management members are responsible for this comprehensive maintenance task. The Nexelus Security Team members will make sure that the plan undergoes a more formal review every Six months to confirm the incorporation of all changes since the previous quarter. Annually, the Nexelus Security Team members initiate a complete review of the plan, which could result in major revisions to this document. These revisions will be updated and distributed to all Nexelus Security Team members. The BCP plan is a live document and requires updates as soon as there are changes and will include a mechanism for induction of new services.

### Disaster Recovery Steps

[blurbs]

|  |  |  |
| --- | --- | --- |
| Info | Description | Details |
| Access to Azure Portal | You will need Azure portal access to spin up new servers |  |
| Access to Backup server images |  |  |
| DB Back Source Folder | Folder path with Database backups. |  |
| DB Destination Folder | Folder path on new DB server where we will copy the backup. This folder should be accessible by SQL server where we are restoring backups. |  |
| Application Files Source Folder | Folder path where Application / Document files are backed up. |  |
| Application Files Destination Folder | Folder path where application files will be copied to restore. |  |
| DB Server IP Address | IP Address of new DB server. This will be required when updating Database connection settings for Web Application. |  |
| Web Server IP Address | This will be required when creating shared folder for GP files. |  |
| SFTP Details | Make sure you have access to SFTP setup details. |  |
| SQL Script to create Databases. | Will be referenced as nexelus\_dr\_recovery\_create\_all\_databases in this document. |  |
| SQL Script to restore database. | Will be referenced as nexelus\_dr\_recovery\_restore\_databases in this document. | This SP should take one parameter as below. 1- Backup path: This SP will get backups for all databases from this path and will restore all databases. |
| Update Script to update Server name, uid/pwd for all databases. | This Script will update DB server name, user id and password for all databases. Question is, do we need to use separate users for all clients the same way we are doing, or we can use “sa” for all users for disaster recover. in any case, we must create this script to do this automatically, rather than doing it manually. For now, let’s assume we will use “sa” for all clients. nexelus\_dr\_recovery\_update\_database\_credentials will be referenced in this document. | This SP will take 2 parameters. user ID and password. |

## Restore Servers in Azure

[blurbs]

### A. Create new Servers

Login to Azure Portal.

1. Spin up new Servers.
2. Restore Server Images:
   1. Restore Database server Image.
   2. Restore Web Server Image.
3. Copy source Files**.**
   1. Copy files from source folder to Destination Folders.

### B. Recover Databases

* 1. RDC to new DB Server.
  2. Open Microsoft SQL Server Management Studio (MSMS) and step c. to k. for each company database.
  3. **Create New** Databases for All company using steps below
     1. Click on “New Query” in MSMS
     2. Copy SQL Script from “nexelus\_dr\_recovery\_create\_all\_databases “ in New Query Window.
     3. Run the script by pressing F5.
        1. This will create databases for All clients.
  4. **Restore Full Backup.**
     1. Clear Query Window
     2. Copy SQL Script from “nexelus\_dr\_recovery\_restore\_databases“ in New Query Window.
     3. Provide Backup folder path as parameter.
     4. Run the script by pressing F5.
        1. This will restore databases for All clients based on backup.
  5. **Restore partial backup**
  6. **Update Database credentials:**
     1. Clear Query Window
     2. Copy SQL Script from “nexelus\_dr\_recovery\_update\_database\_credentials“ in New Query Window.
     3. Provide user ID and password as parameters.
     4. Run the script by pressing F5.
        1. This Script will update user id and password for all client enterprise databases in pdm\_company\_site table.
  7. Share Folder for Format and GP posting.

C. Recover Web Application (Web Server):  
Restoring web server image will restore all applications and required configurations. However, we will have to perform following tasks once Web Server Image is restored.

1. **Update Application’s Web.Config.  
   Please note:** You need to perform this step for all client applications.  
   * 1. Open IIS Manager.
     2. Click on Server name to expand the node.
     3. Click on “Site” nodes to expand it.
     4. Click on client application node you are working with to expand it.
     5. Right click on Web folder and select Explore.
        1. Graphical user interface, text, application

           Description automatically generated
        2. Graphical user interface, application

           Description automatically generated
     6. This will open windows explorer.
     7. Search for Web.Config in opened folder.
     8. Open web.config in notepad.
     9. Search for “databaseserver\_esment” in web.config and update existing values with new database server, user Id and password.
     10. Text, letter

         Description automatically generated
     11. Search for “connectionStrings” in web.config.
     12. Replace old database name, user/pwd with new DB server, UID and password.
         1. Graphical user interface, text, application

            Description automatically generated
2. **Update Report Server Web.Config.**You need to perform this step for every report server for every client.  
   We can also write a small application/ Script to update these values automatically. Will discuss this later.
   * 1. Right Click on reportServer Application in IIS and click Explore
     2. Graphical user interface, text, application

        Description automatically generated
     3. This will open windows explorer where report server files are stored.
     4. Search for Web.Config in notepad.
     5. Update highlighted values with new values for database server, userid /pwd.
        1. Text, letter

           Description automatically generated
3. Update File folder Credentials in App pool (If needed) [Asif Azim to fill]
5. **Verification Process.**
   1. Open application for any Client.
   2. Login Into application using default user credentials.
   3. Navigate through different User Interfaces.
   4. Pint few reports to verify report server is working.
   5. For Media clients only.
      1. Open Client Profile.
      2. Load Any client.
      3. Go to integrations Section.
      4. Open Look up for Google Ads account.
      5. Press refresh button.
         1. System should prompt those accounts has been refreshed.
   6. Go to database server.
   7. Open query manager.
   8. Go to link Servers and Expand “172.16.8.224” Node to make sure Hstar Connection is working.
      1. Graphical user interface, text, application, chat or text message

         Description automatically generated

Open GP for Hy and Login into GP to make sure GP is working.

# Monitoring

Nexelus evaluates whether each of each of the defined internal control components, and the principles within each component, are present and functioning as per SOC 1 compliance. The process may be achieved through separate evaluations or ongoing activities. Monitoring also includes initiating appropriate corrective actions.

## Procedure for Control of Nonconforming Products

This procedure provides a system for:

1. Evaluating the root cause of defects and eliminate the nonconformity
2. Evaluating projects, policies, procedures and other related documents and processes
3. Creating/suggesting a permanent solution that prevents recurrence of problems in procedure, applies to the review and subsequent disposition of non-conforming product.

### Scope

This procedure applies to all activities related to identifying and eliminating non-conformities in products, projects, policies, processes, equipment’s etc.

## Incident Reporting Policy

All incidents, accidents and hazards are reported to designated authorities as defined in the procedure. By doing this Nexelus will keep the record for all the reported incidents, accidents, and hazards. Moreover, we will also learn from these events as to avoid such scenarios in future.

Diagram

Description automatically generated

1. Incident Management Process

### Types of Incidents

There are number of incidents which can be predicted or anticipated of while operating in software development industry. Some of them are standard and common with other industries. Some of the incidents’ categories are given below.

* Infrastructure failure
* Data loss
* Data theft
* Fire
* Civil unrest (strike, riots, fight, sabotage, and other forms of crime)
* Terrorist activity (bomb blast, bomb alert)
* Physical security breach
* Building damage issues
* Utility failure (Power & Water)
* Service Interruption

### Critical Incidents

Few of the critical incidents and their responsible personnel are as under:

|  |  |  |  |
| --- | --- | --- | --- |
| Item | Incident | Owner (Pakistan) | Owner (USA) |
|  | Network | Shafiq Ahmad | Peter Plakowski |
|  | Infrastructure | Arshad Sadal | Imran Rahman |
|  | Network Hacking | Shafiq Ahmad | Peter Plakowski |
|  | Software Hacking | Tauseef Shahzad | Asim Jameel |
|  | Application Crash | Support ([support@nexelus.net](mailto:support@nexelus.net)) | |
|  |  |  | |

### Internal Reporting

All the internal incidents, accidents, or hazards at Nexelus are reported on Internal Service Desk on Jira portal. HR, Admin, Accounts, Senior Network Engineer and/or Administrator and General Manager are involved in the Incident Management Team. General Manager is the head of Incident Management Team. All the decisions will be taken after his approval.

* For every incident, the incident is reported on Jira portal, and its related actions and root cause is mentioned over there. However, in case of emergency issues are also fixed on verbal communication and are then logged on Jira later. For more details Change Management Procedure is available.
* It is the duty of the person who witnesses any incident to report it on Jira center.
* It is the responsibility of the incident management team to take appropriate actions against all incidents.
* Admin Manager checks all issues and assigns to concerned individual. Email is sent automatically to the concerned individual, and he/she is then responsible to resolve the issue.
* Though not necessary but a ‘Lesson Learnt Report’ should be prepared.

In case of any legal breach, Incident Management Team will report using information on following:

### External/Client Reporting

For external/client reporting following are used:

* Support center (Jira)
* Emails
* Phone Calls
* Microsoft Teams

External issues include client complaints, suggestions, enhancements, data beach, and/or incidents relating to Nexelus Application and customer Services etc.

Reference(s):

* Support Center (Jira)

### Collection of Evidence

This activity depends upon the place of occurrence of an incident. If it is in the premises of Nexelus then it is the responsibility of Nexelus Security Team to collect the evidence and maintain records for it. If the incident occurs in the building, then it is the duty of Manager Admin to keep the records of incident evidence. Moreover, in case of a major disaster, Nexelus Security Team can make joint effort with Manager Admin to collect and save the evidence.

### Problem Management

Every incident has a root cause. Root cause is basically the problem. For problem management that root cause is analyzed and entered in the history of every issue. The root cause is also mentioned in the knowledge base.

### Root Cause Analysis

Following tools can be used for the root cause analysis (RCA) of problems:

* Brainstorming
* FTA (Fault Tree Analysis)

### Knowledge Base

Report is generated for all the issues which are reported on service desk. This report becomes the knowledge base for the period for which report is generated. Currently, it is planned twice a year. It is the responsibility of Network Administrator and/or Admin Manager to write root cause and solution in the knowledge base. If the issue is repeated and is of the sort that it can be then it is promoted to the status of problem. For each problem permanent fix is recommended and implemented by the concerned department. The effectiveness of the fix is checked and then it is marked closed in the knowledge based. Those problems which are accepted by management as a normal problem are also marked in the knowledge base.

An incident has a root cause that root cause is analyzed and entered on service desk and is present in knowledge base as well.

### Communication

Communication with stake holders is conducted by using communication channels as mentioned in communication procedure.

### Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## Internal Audit

Nexelus maintains a team of auditors to conduct the Internal Audit on regular basis. The Internal Auditors are selected from different organizational functions based on their experience and professional skills. They are then trained on auditing skills by conducting internal training sessions.

Principal Internal Auditor as appointed by company maintains the List of Internal Auditors. The training plan for the auditors is included in the training schedule of Nexelus.

Sometimes Internal Audit is conducted by Nexelus Audit team in the form of a gap analysis.

### Audit Planning

The process for planning an Internal Audit is as follows:

The Principal Internal Auditor discusses Annual Audit Plan in management review meeting and prepares audit schedule, which covers all processes of the SOC in all areas where it is implemented.

The Principal Internal Auditor ensures that all the applicable clauses are audited at least once in a year by trained auditors, chosen from the Nexelus employees.

Principal Internal Auditor assigns qualified auditors that are independent of the activities being audited. The auditors are also assigned different areas to audit periodically to ensure that they do not become too familiar with the activities of a department and a fresh approach is ensured.

### Audit Execution

The process of audit execution is as follows

1. Approximately a week prior to the planned audit, Principal Internal Auditor distributes the audit schedule to all relevant Managers to ensure their availability on the date of the scheduled audit. Moreover, this schedule is communicated through all the relevant Managers in the SOC Compliance meeting.
2. Principal Internal Auditor informs the auditee about the timings of audit in advance. If any changes in timings are desired, auditors make adjustment on the day of the audit in the brief opening meeting with auditee.
3. The auditors conduct audit on sample basis, which is informed to auditee in the brief opening meeting.
4. During the audit, the auditor only asks questions from the persons performing the tasks and uses suitable language for auditee.
5. During the audit, the auditors can use their own designed checklist. Checklist consists of leading questions, which ensure no area of the department is left out.
6. The auditor uses the audit checklist as a reference document and notes down all the observations on it. Audit findings/observations may be noted on a single paper.
7. The auditors also use the Checklist to identify non-conformances observed during the audit and transfer these on the Non-Compliance Report (NCR), which is presented to the auditee by the auditor.
8. To see whether relevant records of operations and inspections conform to standard and specifications, results of the process/operation activity are selected, and their record is traced backwards.
9. NCR remains with the auditee and/or departmental representative until the closing of non-conformance(s) raised during the audit. After closing of all non-conformances NCR are submitted to MR for record.
10. The NCR must be signed by the lead auditor and the auditee.
11. Principal Internal Auditor maintains Internal Audit Logbook to efficiently monitor the progress and follow up of Internal SOC Compliance Audit results.

Independent audit will be conducted by the consulting team (if available) with6 month intervals as required by SOC standard.

### Audit Reporting

After the completion of audit, the auditors submit their findings (observations, NCRs) to Principal Internal Auditor, who compiles all these findings and prepares the Internal Audit Report. It includes the summary of the audit, audit non-conformities and observations observed.

### Follow-up Audit

A follow-up audit is conducted to check the effective implementation of the corrective action proposed during the actual audit. This audit is conducted on or after the date agreed upon during the original audit. During this process due consideration will be given to the corrective actions suggested during the initial audit. For the follow-up audit, corrective and preventive actions are used as a reference which is also part of NCR.

### Independent Review of SOC Compliance

QA team has been designated to perform Internal Audits independently and objectively as required by checklist of Internal Audit. This audit will be performed as per audit plan on regular intervals as required by SOC and other security standards in place at Nexelus.

### Roles and Responsibilities

### General Manager and QA Lead

The CEO, General Manager, and QA Lead will be informed about the NCRs by the Principal Internal Auditor. They will provide appropriate suggestions for resolutions and assist in root cause analysis and preventive and corrective actions.

The Development Manager will also make sure that customer complaints are appropriately handled and resolved as logged in Support Center to deals with client-side issues.

A separate JIRA repository for Internal Support is being setup to manage and track internal issues, complaints, suggestions, and incidents.

The Network and Security Manager will also make sure that all security, quality, and service-related complaints are properly handled and resolved.

### Network and Security Manager

The Network and Security Manager will review and resolve the network, hardware, and application software non-conformities.

### Principal Internal Auditor

• The Principal Internal Auditor shall maintain the record of NCRs and close the NCRs after verification of the appropriate action taken. The Principal Internal Auditor shall also ensure that all NCRs are properly handled and resolved.

• The Principal Internal Auditor will conduct the root cause analysis on the NCR in collaboration with relevant personnel and fill the details on the NCR.

### Nexelus Employees

This procedure applies to all the employees of Nexelus shall report all non-conformities whenever they encounter any. NCRS can be defined as follows:

### Classification of Observations and Non-Conformity

#### Major Nonconformity

Fails to satisfy the requirements of Soc Compliance or Systematic failures to carry out an activity.

#### Minor Nonconformity

Satisfies the requirements of SOC Compliance but fails to satisfy the Organization’s own internal Standards, Procedures, Policies, Manuals, or Non-Systematic failures.

#### Observation

An area of weakness that could be improved or be given any suggestions for improvement.

### Internal Audit Procedure

### Identification of Nonconformities

In software development, non-conforming items are identified at the following stages:

1. At receiving inspection stage of hardware items.
2. During an audit activity (Internal Audit).
3. Management Review
4. By general observation of any employee of Nexelus.

#### Purchased Products

Three types of non-conformances are normally found in purchase items received in the company

1. Totally rejected (all types of hardware & software)
2. Re-workable by supplier
3. Acceptable with some concession- depending upon the nature of the purchased or acquired product.

In all the above cases the receiver fills the Defect Advice Note and sends it to Administration Manager, who subsequently fills in the rest of the portion of the same note for onward dispatch to the concerned supplier. A copy of all filled Defect Advice Notes is also kept for reference and record. Further details may be found in Procurement Procedure.

#### Software Products

In the disposition of the non-conformities of software products developed in the company, attention is paid to the following aspects

1. Any discovered problems are recorded using the Internal Support Center.
2. Areas impacted by any modifications are identified & retested. The record of the testing is logged in the Internal Support Center.
3. Sometimes changes are required to be made to the software product for improvement in design or due to prevention of potential bugs. These changes are recorded in the Change Request Form.

#### Audit Non-Conformity

1. Any nonconformity uncovered during the audit activity is regarded as the Audit Nonconformity. Audit nonconformities are logged and reported using the NCR. Corrective and preventive actions taken on the NCRs are logged. The NCRs are closed after verification and analysis of the appropriate actions taken. The NCRs are closed and maintained by the Principal Internal Auditor.

#### Network/Equipment Nonconformity

1. Users can submit requests for their problems on the service desk on Internal Support Center. The Network and Security Manager responds to user’s requests or complaint in timely manner and adds history for the problem.

#### SOC Compliance Nonconformity

1. Any activity not according to the documented procedures of the SOC Standard will be considered as nonconformity and an NCR will be generated against it. Corrective or Preventive actions will be taken accordingly and logged on the NCR respectively. Internal Support Center will be responsible to keep the record of NCR.

#### Information Security Management System Nonconformity

1. Any activity not according to the documented policies and procedures of the ISMS will be considered as nonconformity and an NCR will be generated against it. Corrective or Preventive actions will be taken accordingly and logged on the NCR respectively. Principal Internal Auditor will be responsible to keep the record of NCR.

#### Service Management System Nonconformity

1. Any activity that is not in accord to the documented policies and procedures of the Nexelus Security Policy will be considered as nonconformity and an NCR will be generated against it. Corrective or Preventive actions will be taken accordingly and logged on the NCR respectively. Principal Internal Auditor will be responsible to keep the record of NCR.

### Authorization for NCRs Closing

All closed NCRs are submitted to Principal Internal Audit for record and closure.

### Maintenance of Records

Records related to Non-Conformance activities will be maintained

## Procedure for Corrective and Preventive Actions

This procedure provides system and instructions to assign responsibilities for initiating, requesting, implementing, and checking the effectiveness of corrective and preventive actions.

### Scope

This procedure applies to preventing and correcting nonconformities related to components, finished products, and the Quality Assurance, Service Management, and Information Security Management Systems. This procedure affects all other departments and functions in the company.

### Procedure

Procedures for corrective and preventive actions are given below:

#### Corrective Action

Corrective actions will be taken to correct existing problems (problems that have occurred). These may include problems involving the product, process, or equipment.

1. Principal Internal Auditor and Support Departments will send details of the nonconformities including customer complaint to concerned person for resolution. The concerned person will conduct the relevant corrective actions to ensure that all nonconformities are removed. Details of these actions will be recorded in the Corrective and Preventive Action (CPA) columns of the NC log.
2. The performed actions will be audited/ reviewed by Principal Internal Auditor and/or other assigned personnel to assess the effectiveness of the corrective actions.
3. In case the action was effective, the NC will be closed. Otherwise, the details will be entered in the CPA including “Reasons for Ineffectiveness” and “Next Target Action”. Till the corrective/preventive actions are declared as effective, the audit/review will be continuously conducted. Once the corrective/preventive actions are considered as effective, the NC will be closed.
4. This action can be implemented for all types of nonconformities that occur before and after the internal audit.

#### Preventive Actions

Preventive actions will be taken to prevent potential problems or to avoid from reoccurrence of any issue. These may include potential problems in the product, process, or equipment.

1. Any existing and potential problems may be identified in purchased products, unreleased/released software products, network, equipment, SOC Compliance, Service Management System, and Information Security Management System.
2. These problems may be identified through general observation, inspection, audits, management reviews and customer feedback.
3. Root cause analysis of the existing problem will be recorded on the NC log.
4. A follow-up audit may be conducted after which the relevant details will be entered in the NC log and appropriate action will be taken.
5. The performed actions will be audited/reviewed by Principal Internal Auditor and/or other assigned personnel to assess the effectiveness of the preventive actions.
6. In case the action was effective, the NC will be closed, otherwise the details will be entered in the CPA columns of the NC log including “Follow up”. Till the corrective/preventive actions are declared as effective, the audit/review will be continuously conducted. Once the preventive actions are considered as effective, the NC will be closed.
7. This action can be implemented for all types of nonconformities that occur before and after the internal audit.
8. CPA columns of the NC log will be filled against major problems which required protecting future issues. It is not necessary that all IRF or NCs must have CPAs.