**UniQuE**

Information Security Audit Procedure

(Engagement Name and Id)

(Client)

**Document History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Changes |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Review And Approval**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Company | Role | Name | Date | Signature |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Distribution**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Company | Name | Number | Media | Action |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Storage**

|  |  |  |
| --- | --- | --- |
| Location | Access | Administrator |
|  |  |  |
|  |  |  |

Company Confidential - Copyright © 2017 Capgemini - All rights reserved

Template Version Number: Group Reference v1.0**Table Of Contents**

[1. Introduction 4](#_Toc480977319)

[2. Audit Scope And Objectives 5](#_Toc480977320)

[3. Roles And Responsibilities 6](#_Toc480977321)

[4. Information Security Audit Process 7](#_Toc480977322)

[4.1. General 7](#_Toc480977323)

[4.2. Process 7](#_Toc480977324)

[4.2.1. Initial Preparation 7](#_Toc480977325)

[4.2.2. Opening Meeting 7](#_Toc480977326)

[4.2.3. Audit Execution 7](#_Toc480977327)

[4.2.4. Audit Reporting 7](#_Toc480977328)

[4.2.5. Closing Meeting 7](#_Toc480977329)

[4.2.6. Audit Follow-Up And Closure 7](#_Toc480977330)

[5. Information Security Audit Schedules 8](#_Toc480977331)

# Introduction

<< This section must introduce the procedure for information security audit in an engagement >>

# Audit Scope And Objectives

<<Mention here the overall scope and objective of the information security audit for an engagement. >>

# Roles And Responsibilities

<<Detail out the roles and responsibilities for the entire information security audit program. >>

# Information Security Audit Process

## General

<< Eg:

* An ISMS audit programme shall be created that contains all scheduled and potential audits for the whole calendar year. This shall include schedule of internal audits, audits of suppliers, audits to be performed by clients and third-party audits, as appropriate
* Internal audits shall be scheduled twice a year or as the need arises.
* Only competent personnel who are truly independent of the subject area shall perform audits.
* The Lead Auditor shall supervise the activity of the Audit Team.
* An Audit Notification is sent to the department/section to be audited at least three working days in advance of the audit.

>>

## Process

<<This section should detail out the audit workflow to be followed. >>

### Initial Preparation

<< Mention here the pre-requisites required for the information security audit. >>

### Opening Meeting

<<Mention here the details for the opening meeting. This would typically include audit introduction, schedule, audience, scope and agenda, etc. >>

### Audit Execution

<< Explain here the procedure to be followed while conducting the information security audit. >>

### Audit Reporting

<< Detail out the reporting mechanism to be followed for the information security audit. >>

### Closing Meeting

<<Mention here the details for the closing meeting. This would typically include audit findings, recommendations, and gaps, by the auditor. >>

### Audit Follow-Up And Closure

<<This section will detail out the procedure to be followed for the NCs raised, corrections to be done and the CAPA execution >>

# Information Security Audit Schedules

<< This section should include the detailed schedule of the information security audit for an engagement. >>