

**Cyber security Audit and compliance**

Manual

Circle T Industries

Table of Contents

[2 Scope of this Document 3](#_Toc189495875)

[3 Ownership of this Document 3](#_Toc189495876)

[3.1 Document Properties 3](#_Toc189495877)

[4 Guidelines 4](#_Toc189495878)

[4.1 Design 4](#_Toc189495879)

[4.2 Capture 5](#_Toc189495880)

[4.3 Analyse 6](#_Toc189495881)

[4.4 Respond 7](#_Toc189495882)

[5 Managing Director Sign-off 8](#_Toc189495883)

# 

# Scope of this Document

|  |  |
| --- | --- |
| Role | Details |
| Staff | Acknowledge |
| Guests | Aware |
| Public | Share on approval from the document owner |

# Ownership of this Document

If any questions exist as to the nature or content of this procedure, they should be directed to:

|  |  |
| --- | --- |
| **Document Owner**  **Name:** Hamish Toll  **Title:** Director  **Email:** Hamish.toll@circlet.com.au | **Subject Matter Expert**  **Name:**  Neil Spencer  **Title:**  M365 Architect  **E-mail:**  neil.spencer@circlet.com.au |

## Document Properties

|  |  |
| --- | --- |
| Title | Details |
| Version | 4 |
| Effective Date | [Effective Date] |
| Review period | 12 months |
|  |  |

# Guidelines

## Design

1. **Define the Scope**: Determine the boundaries and extent of the audit. This includes identifying the systems, networks, and data to be audited
2. **Evaluate Security Controls**: Review the existing security controls in place to protect the organization's IT assets. This includes assessing the effectiveness of firewalls, intrusion detection systems, access controls, and encryption mechanisms
3. **Conduct Risk Assessment**: Evaluate the risks associated with identified threats and vulnerabilities. This involves determining the likelihood and impact of potential security incidents
4. **Develop Audit Plan**: Create a detailed plan for conducting the audit. This includes defining the audit objectives, methodologies, and timelines

## Capture

1. **Gather Information**: Collect relevant information about the organization's IT infrastructure, policies, and procedures. This includes network diagrams, system configurations, and security policies
2. **Identify Threats and Vulnerabilities**: Assess the potential threats and vulnerabilities that could impact the organization's IT assets. This involves reviewing past security incidents, conducting vulnerability scans, and analysing threat intelligence
3. **Perform the Audit**: Execute the audit plan by conducting tests and assessments on the organization's IT systems and processes. This includes penetration testing, security assessments, and compliance checks

## Analyse

1. **Analyse Findings**: Review and analyse the results of the audit. Identify any security gaps, weaknesses, or non-compliance issues
2. **Report Findings**: Document the findings of the audit in a comprehensive report. This includes providing recommendations for improving the organization's security posture

## Respond

1. **Implement Recommendations**: Work with the organization to implement the recommended security improvements. This includes updating security policies, patching vulnerabilities, and enhancing security controls
2. **Monitor and Review**: Continuously monitor the organization's security posture and review the effectiveness of implemented security measures. This involves conducting regular security assessments and audits

# Managing Director Sign-off



………………………………………………

**Managing Director**