*[Insert Project or Service Name]*

**IT Health Check**

**Scoping Document**

**Origin/Author: [Insert Author of Document]**

**Date Approved: [Insert Approval Date]**

**Version: [Insert Version number,]**

Contents

[**Introduction**](#_30j0zll) **3**

[Overview](#_nwrzbyrvlzqr) 3

[Location](#_nwrzbyrvlzqr) 3

[Overview](#_nwrzbyrvlzqr) 3

[**Background & Technical Information**](#_e5b48qyjazou) **4**

[Background](#_nwrzbyrvlzqr) 4

[Scope](#_nwrzbyrvlzqr) 4

[External Network Assessment](#_nwrzbyrvlzqr) 4

[Internal Network Assessment](#_v3zk85qculvz) 4

[Firewall Configuration & Ruelset Review](#_mly8fz4z18le) 4

[Web Application Testing](#_z5hffgup40v6) 4

[Application Code Review](#_k1m5lro2p97y) 4

[AWS Account Configuration](#_112q62hymmq) 5

[Docker Container Build Review](#_o6wfpbx9n2r) 5

# Introduction

## Overview

This document defines the scope for the IT Health Check on *[Insert Project or Service Name]*.

## Location

The testing will take place at [insert location, additionally state if testing can be performed remotely form ITHC supplier offices].

## Overview

The IT Health Check will take place from [insert required dates of testing]. Testing will be conducted [during test supplier’s business hours 9-5pm, out of hours].

[Note: An ITHC should aim to provide assurance that your organisation’s internal and external systems are protected from unauthorised access or change, and they do not provide an unauthorised entry point into your systems and infrastructure. When major changes to infrastructure are made an ITHC should be performed to provide assurance that the changes do not weaken the security of the organisation’s IT estate.]

# Background & Technical Information

## Background

*[Insert the background including why you want to carry out the test? Include an overview of the system including any constraints. Please include infrastructure diagrams in this section to provide context. If testing is to be carried out across multiple VLANs or segregated networks, then you will need to advise the number of VLANs.]*

## Scope

The scope of this ITHC is targeted at the *[Insert Service / Scope Title],* the testing will comprise of the following areas,

*[Please remove / add relevant testing ares - example areas given below]*

## External Network Assessment

External exposure testing of the following public internet addresses representing the perimeter network are in scope of this ITHC.

|  |  |
| --- | --- |
| IP Address | Description |
|  | Boundary firewall IP range |
|  | IPsec endpoint |
|  | CE router |

## Internal Network Assessment

Internal network exposure testing

## Firewall Configuration & Ruleset Review

A firewall deployment configuration and ruleset review of the following is within scope of the ITHC.

Further detail is contained within the accompanying spreadsheet workbook.

|  |  |  |
| --- | --- | --- |
| Firewall Vendor | Description | Firewall Rules in Scope |
| E.g. Checkpoint | Internet facing firewall | 30 |
|  |  |  |

## Web Application Testing

The following internet / internal facing web applications which possess Graphical User Interfaces (GUI) for data garther will be performed directly against the web applications. Web applications within scope of this ITHC are contained within the accompanying spreadsheet workbook.

## Application Code Review

A full application source code review will be performed against the following deployed applications,

* Application 1
* Application 2

Details of the programming languages used and total lines of source code (main & dependencies) are covered within the accompanying spreadsheet workbook.

## AWS Account Configuration

A comprehensive AWS account configuration review will be performed encompassing the following areas,

* IAM
* S3
* KMS
* Security Groups & NACLS
* CloudWatch
* CloudTrail
* AWS Parameter Store / Secrets Manager

## Docker Container Build Review

Across the nominated Docker containers running within the environment a full build review and configuration review will be performed to identify any weaknesses or misconfiguration of installed binaries / application stack. Containers in scope are identified in the accompanying spreadsheet workbook.