***[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

[1 Introduction 3](#_Toc96091685)

[1.1 Overview 3](#_Toc96091686)

[1.2 Location 3](#_Toc96091687)

[1.3 Overview 3](#_Toc96091688)

[2 Background & Technical Information 4](#_Toc96091689)

[1.4 Background 4](#_Toc96091690)

[1.5 Scope 4](#_Toc96091691)

[1.6 External Network Assessment 4](#_Toc96091692)

[1.7 Internal Network Assessment 4](#_Toc96091693)

[1.8 Firewall Configuration & Ruleset Review 4](#_Toc96091694)

[1.9 Web Application Testing 4](#_Toc96091695)

[1.10 Application Code Review 5](#_Toc96091696)

[1.11 AWS Review and AWS Connect 5](#_Toc96091697)

[1.12 Docker Container Build Review 5](#_Toc96091698)

[1.13 Office 365 Review 5](#_Toc96091699)

[1.14 MS Dynamics CRM Review 5](#_Toc96091700)

[3 Standards and Requirements 7](#_Toc96091701)

[4 Reporting 8](#_Toc96091702)

# Introduction

## Overview

This document defines the scope for the IT Health Check (ITHC) 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 Council’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 Council’s IT estate.]***

# Background & Technical Information

## Background

***[Insert any background information and drivers to requesting this assessment. Include an overview of the systems in scope 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, please advise on 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 areas - example areas given below]***

## External Network Assessment

As part of the ITHC we require testing of all external IP addresses which are within scope of services provided. External exposure testing of the following public internet addresses representing the perimeter network are in scope of this ITHC.

|  |  |  |
| --- | --- | --- |
| IP Address / Network Range | Number of Live hosts | Description |
|  |  | *Boundary firewall IP range* |
|  |  | *IPsec endpoint* |
|  |  | *CE router* |
|  |  |  |

***Insert relevant concerns listed in ITHC Principle Security Concerns- section 2.9 Network configurations.***

## Internal Network Assessment

Internal network exposure testing

|  |  |  |
| --- | --- | --- |
| IP Address / Network Range | Number of Live hosts | Name of VLan / LAN |
|  |  |  |
|  |  |  |
|  |  |  |

***Insert relevant concerns listed in ITHC Principle Security Concerns- section 2.9 Network configurations***

## End User Device Assessment

End User Device testing

|  |  |  |  |
| --- | --- | --- | --- |
| IP Address / Network Range | Number of Live hosts | Operating System | Build review/ Authenticated scan |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

***Insert relevant concerns listed in ITHC Principle Security Concerns- section 2.3 Operating Systems***

## 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 |
|  |  |  |
|  |  |  |

***Insert relevant concerns listed in ITHC Principle Security Concerns- section 2.8 Firewall configurations***

## Web Application Testing

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

***Insert relevant concerns listed in ITHC Principle Security Concerns- section 2.7 OWASP API Security Top 10***

## 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.

***Insert relevant concerns listed in ITHC Principle Security Concerns- section 2.6 OWASP Application Top 10 categories***

## AWS Review

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

* AWS Service configuration review
* AWS Core services review
  + IAM configuration
  + S3 bucket configuration
  + KMS
  + Security Groups & NACLS
* CloudWatch
* CloudTrail
* AWS Parameter Store / Secrets Manager

The review will be carried out from the AWS console against NCSC AWS best practice recommendations.

## 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.

## Office 365 Review

The solution relies upon Microsoft Office 365 for providing a secure end user access mechanism to email. The testers shall ensure that Office 365 has been appropriately configured. Email shall also be aligned to NCSC secure email best practice. Therefore, the tester shall review:

* Office 365 user configuration
* Office 365 email configuration

Configuration will be reviewed against Microsoft and NCSC best practice, such as secure government email.

## MS Azure Review

The solution relies upon Microsoft Azure at the ***core [Insert role- e.g. providing a customer relationship management function for XXX / XXX****]*. As part of the test, the testers shall review the components used and configured against manufacturer and industry best practice. The Microsoft Azure review shall include:

* MS Azure configuration review including validation of the RBAC
* MS Azure authentication configuration
* Review of the MS Azure solution front-end against OWASP Top 10 guidance
* Review of the configuration of API endpoints

The review will be carried out from the MS Azure console against NCSC and Microsoft best practice recommendations.

# Standards and Requirements

All testing must be carried out by a CREST certified company. Possession of the ISO 9001 accreditation would be beneficial, however is not a specific requirement for this assignment.  
Acquiring ISO27001 certification would be advantageous.

**Security Clearance**

Personnel must hold a minimum of SC clearance.

**Skills**

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

The test team must be proficient in the testing of:

* Application security
* Web applications
* Linux server security
* Virtualization server security
* Firewall technologies and rule base reviews
* Oracle
* Database technologies (PostgreSQL , Redis, MySQL & MongoDB)
* AWS Technologies such as Connect, S3, ElastiCache, Elasticsearch

# Reporting

One holistic report is expected, with a draft and/or interim release being made available as soon as possible after the completion of testing, prior to any optional re-testing.

The reports **must**:

* include details on what was tested, how it was tested, what results were found and what impact any discovered vulnerabilities would have on a live service.
* include what techniques and tools were used to carry out the test.
* use the CVSS marking scheme.
* clearly identify / number the vulnerabilities found for tracking purposes.
* include an accompanying results summary in spreadsheet format.
* provide a heat map the results, Red-Green on exposure vs risk.

At the end of each day of testing an informal update is requested. This could take the form of a verbal update or a brief highlight report listing the issues found.

Documented report output to include:

* + Readable and accessible presentation to the Council containing a clear summary of the number, type and severity of the issues identified.
  + Details of the individuals involved in the ITHC.
  + Communication of the background, scope and context of the health check in full.
  + Accurate identification and explanation of vulnerabilities.
  + For each identified vulnerability, an associated remedial solution. The remedial solution should not necessarily be seen as the sole method for reducing the risk, a short-term remedial action may be appropriate until such time that a strategic fix can be put in place. Typical short-term remediations may include a combination of network segregation, limiting access, increased monitoring and further hardening.