**Risk Management Documentation Templates**

|  |
| --- |
| Information Security Management Document Set  [Project/Service and Supplier Name] |

*Author:*

*Owner:*

*Date:*

*Version:*

# **Executive Summary**

<*This section should contain a brief summary of the business context of the system, any key IA controls, the assurance work done, any off-shoring considerations and any residual risks that need acceptance by the Buyer. This should be completed at the end of the assurance process.>*

## List of Contents

[**Executive Summary 3**](#_3dy6vkm)

[List of Contents 4](#_1t3h5sf)

[Change History 5](#_4d34og8)

[References, Links and Dependencies 5](#_17dp8vu)

[**Background 6**](#_35nkun2)

[**Contractual Arrangements 6**](#_1ksv4uv)

[**Governance, reporting and accountability 6**](#_44sinio)

[**Customers 6**](#_2jxsxqh)

[**Information Assurance Assessment 6**](#_z337ya)

[Data/Information 6](#_3j2qqm3)

[Overview of technical architecture 6](#_1y810tw)

[Logical Data Flow Diagram 6](#_2xcytpi)

[Third Party Suppliers 6](#_1ci93xb)

[Location of data processing, storage, transfer, back-up tapes 7](#_2bn6wsx)

[Off Shoring 7](#_qsh70q)

[Risk Management 7](#_3as4poj)

[Risk Register 7](#_1pxezwc)

[Security controls 7](#_49x2ik5)

[Table of Hardware and Software relevant to the service 7](#_2p2csry)

[**Incident Management Process 9**](#_147n2zr)

[**Required Changes Register 9**](#_3o7alnk)

[**Personal Data Processing Statement 9**](#_23ckvvd)

[**Annex A. ISO 27001:2013 and Cyber Essential Plus certificates 10**](#_ihv636)

[**Annex B. Cloud Security Principles assessment (a spreadsheet may be attached). 10**](#_32hioqz)

[**Annex C. Protecting Bulk Data assessment if required by the Buyer/Customer (a spreadsheet may be attached). 10**](#_1hmsyys)

[**Annex D. Latest ITHC report and Vulnerability Correction Plan 10**](#_41mghml)

## 

## Change History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Date of Change** | **Change made by** | **Nature and reason for change** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 

## References, Links and Dependencies

This document is dependent on the supporting information and assurance provided by the following documents.

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Document Title** | **Reference** | **Date** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Background

*< A short description of the project/product/system. Describe its purpose, functionality, aim and scope.>*

# Contractual Arrangements

*< Please provide detail of how the system/product/service has been procured including what contracts (service model, call-off, framework, security schedules) are in place.>*

# Governance, reporting and accountability

*<Include a list of the lead security roles for the project and the reporting structures/decision making process for the security work.>*

# Customers

*< Include list of participating departments/organisations if appropriate and known.>*

# Information Assurance Assessment

## Data/Information

*<Include a list of the type and volumes of data that will be processed, managed and stored within the supplier system. If Personal Data, please include the fields used such as name, address, department DOB, NI number etc.>*

## Overview of technical architecture

*< In this section, please provide an architectural diagram of the system. A brief explanation of the relevant components should be included.>*

## Logical Data Flow Diagram

*< Include a diagram of the logical data flows. The scope of the assurance assessment should be clearly indicated, with components of the architecture upon which reliance is placed but assurance will not be done clearly shown e.g. a cloud hosting service.>*

## Third Party Suppliers

*< Include a list/table of the Suppliers, what function they perform, what data they store/process and what assurance activities/due diligence activities have been taken place. Also, include evidence of compliance with ISO 27001:2013 or Cyber Essential/Cyber Essential Plus. Please ensure that the service/system or product that you are procuring is included in the scope of certification>*

## Location of data processing, storage, transfer, back-up tapes

*< This section to include third party suppliers>*

## Off Shoring

*< Please provide detail of any off-shoring arrangements/location, including third party suppliers. Please specify what products, systems, data will be off-shored and where. Also include any detail of what assurance and due diligence has taken place.>*

## Risk Management

*< Include a short explanation for what methodology will be used to assess risks to this system/service/product. Have you used a formal methodology or an informal? Please note that advice on risk management can be found via this link:* [*https://www.ncsc.gov.uk/guidance/risk-management-collection*](https://www.ncsc.gov.uk/guidance/risk-management-collection)*.>*

## Risk Register

*<This section to include a table containing a prioritised risk list which contains the output from the risk assessment and lists technical, personnel, physical and procedural controls that are being implemented to mitigate those risks. An example table is shown below. Any significant residual risks should be agreed with the Buyer/Customer and included in the Executive Summary of this document.>*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk ID | Risk Description | Vulnerability | Untreated Risk Level | Security Controls | Residual Risk Level |
| R1 | Internet attackers could hack the system. | The service systems are exposed to the internet via the web portal. | High | Internet-facing firewalls  Internet-facing IP whitelist  Protective monitoring  Application access control  Anti-virus for incoming files  Patching | Low |

## Security controls

*< Provide a short explanation of the security controls relied upon to treat the risks in the Risk Register.>*

## Table of Hardware and Software relevant to the service

*<This should be a table which lists the end of support dates for hardware and software products and components. An example table is shown below.>*

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Version | End of mainstream Support/Extended Support | Notes/RAG Status |
| Server Host | HP XXXX | Feb 2020/ March 2022 |  |

# Incident Management Process

*<The suppliers’ process, as agreed with the Buyer/Customer, should be included here. It must as a minimum include the protocol for how and when incidents will be reported to the Buyer/customer and the process that will be undertaken to mitigate the incidents and investigate the root cause.>*

# Required Changes Register

*<The table below shows the headings for the Required Changes Register which should be maintained and used to update the contents of this document at least annually.>*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Ref | Section | Change | Agreed With | Date agreed | Documentation update | Status |
| 1 | 6.4 | A new Third Party supplier XXXX will be performing the print capability. | Buyer name | 11/11/2018 | Jul-2019 | Open |

# Personal Data Processing Statement

*<This should include: (i) the types of Personal Data which the Supplier and/or its Subcontractors are Processing on behalf of the Buyer; (ii) the categories of Data Subjects whose Personal Data the Supplier and/or its Subcontractors are Processing on behalf of the Buyer; the nature and purpose of such Processing; (iii) the locations at which the Supplier and/or its Subcontractors Process Buyer Data; and, (iv) the Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect the Buyer Data against a Security Breach including a Personal Data Breach.>*

# Annex A. ISO 27001:2013 and Cyber Essential Plus certificates

# Annex B. Cloud Security Principles assessment (a spreadsheet may be attached).

# Annex C. Protecting Bulk Data assessment if required by the Buyer/Customer (a spreadsheet may be attached).

# Annex D. Latest ITHC report and Vulnerability Correction Plan