Shape

Description automatically generated with medium confidence



Solution Name

High Level Solution Design

Remove this how-to section before the final draft.

**How to complete this document.**

1. All sections are to be completed by the Solution Architect of the system being described. Sections that are not relevant should be marked as ‘Not Relevant’.
2. Drafting and guidance text in **RED** must be deleted for the final draft.
3. The **GREEN** text in needs to be replaced with system specific information in black text.
4. **Black** text remains in the document; however, this may be modified where necessary.
5. Once all sections are complete, this document should be reviewed and endorsed by the Technical Review Forum (TRF).
6. Remember to **delete the DRAFT** watermark and **DRAFT in the title** once the document is considered FINAL.
7. Change the document **version number to V1.0** once the document is considered FINAL
8. Refer to **Appendixes A1 – A5** for reference whilst completing this document.

**<> End of Section**

ISBN

xxx-x-xxx-xxxxx-x [PRINT]  
xxx-x-xxx-xxxxx-x [PDF]  
xxx-x-xxx-xxxxx-x [DOCX]

With the exception of the Commonwealth Coat of Arms, the Department’s logo, any material protected by a trade mark and where otherwise noted all material presented in this document is provided under a [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) (<https://creativecommons.org/licenses/by/4.0/>) licence.

The details of the relevant licence conditions are available on the Creative Commons website (accessible using the links provided) as is the full legal code for the [CC BY 4.0 International](https://creativecommons.org/licenses/by/4.0/legalcode) (https://creativecommons.org/licenses/by/4.0/legalcode)

The document must be attributed as the High Level Solution Design - Solution Name.

# Document Brief

## Template Version History

The version history of updates made to this document are listed below.

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author(s) | Description of Change |
| 0.1 | 19/10/2022 | Jodie Davis | Initial draft |
| 0.2 | 20/10/2022 | Craig Bornholm | Review, feedback, edits |
| 1.2 | 27/10/2022 | Tom Tindal | Align to SOD |
| 1.3 | 17/11/2022 | Tom Tindal | Add more security architecture |
| 1.4 | 30/11/2022 | Tom Tindal | Edits based on feedback |

## Stakeholders

|  |  |  |
| --- | --- | --- |
| Role | Name | Job Title |
| **System Owner (SES)** |  |  |
| **Information Owner** |  |  |
| **Certification Authority** |  |  |
| **Accreditation Authority** |  |  |
| **System Manager / Technical Owner (EL2)** |  |  |
| **Primary Business Contact** |  |  |
| **Primary Technical Contact** |  |  |
| **Architecture Board** | TBD | TBD |

## Review

| Name | Role | Division | Date |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Approval

| Name | Title | Signature | Date |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Document Contact Details

| Name | Title | Signature | Date |
| --- | --- | --- | --- |
|  |  |  |  |

# About this Document

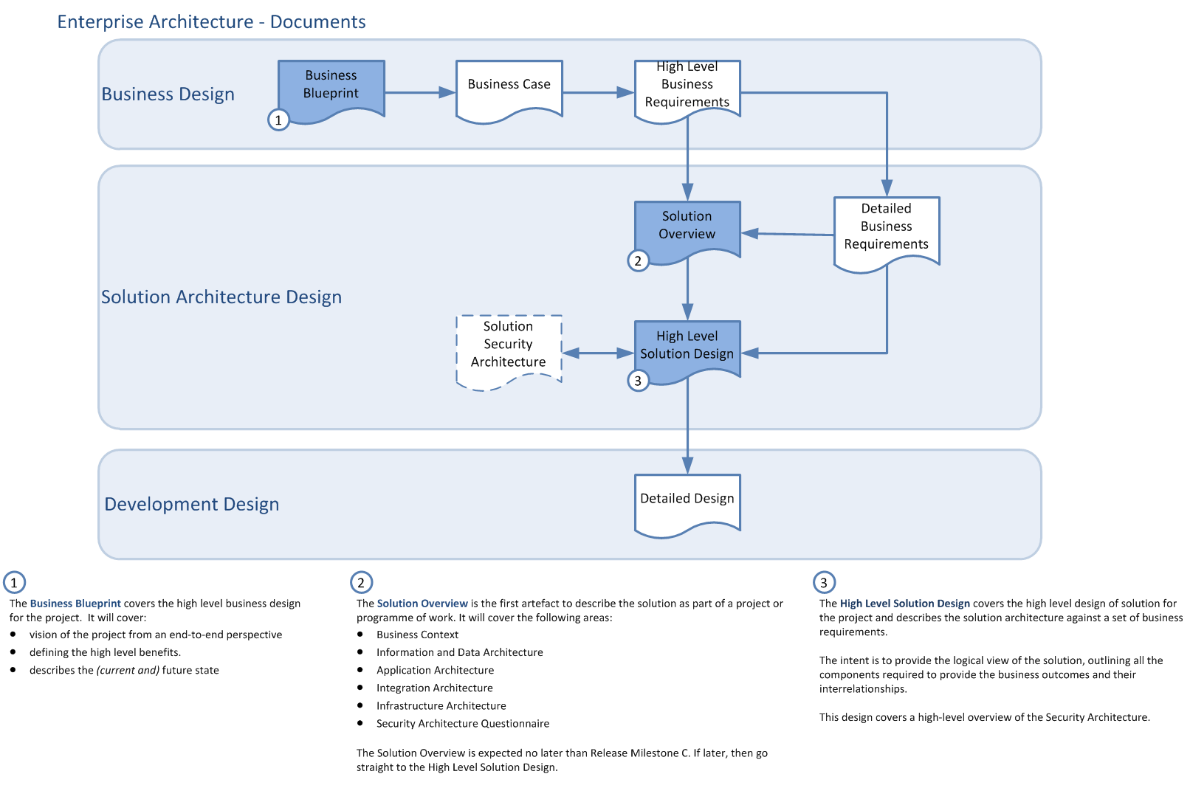
The High-Level Solution Design describes the solution architecture against a set of business requirements. The intent is to provide a logical view of the solution outlining all the components required to provide the business outcomes and their interrelationships.

The High-Level Solution Design is the second technical artefact to describe the solution as part of a project or programme of work as represented in *Figure 1: Document Context* below. The scope and/or complexity of the program / project will determine whether this artefact is required.

The purpose of this document is to describe the design and architecture for the implementation of a System/Solution which:

* 1. complies with the Department of Employment and Workplace Relations (DEWR) Enterprise Architecture standards, patterns, best practices; and
  2. provides the information needed for the relevant delivery team(s) to develop and document detailed designs for the actual implementation of the solution.

Figure : Document Context



## Audience

This document is intended for Project Managers, Delivery Managers, Enterprise Architects, Solution Architects, IT Security Assurance Architecture Board, Developers, Testers, <…list more people / groups / roles…> to gain an understanding of the solution and its impacts across architectural domains.

* Technical Review Forum (TRF) and Platform Architecture Board (PAB) members use this document to understand the solution’s architecture from a business, information, application, integration, infrastructure, and security perspective.
* The PAB reviews and endorses this document (particularly for Architecture Decisions) as a part of the architecture governance process.
* Once this document and associated SSA has been endorsed, the Security Accreditation process can be initiated.

## Related Documents

| **Title** | **Version, Date** | **Author** | **Location** |
| --- | --- | --- | --- |
| Digital Backup and Restore Policy | 3.0 |  |  |
| ICT System and Services Authorisation Policy | 3.3 |  |  |
| Information Management Policy | 0.8 |  |  |
| Protective Security Policy Framework | 2018.6 |  |  |

## Definitions

| **Term / Acronym** | **Definition** |
| --- | --- |
|  |  |
|  |  |

# Contents

[Document Brief 3](#_Toc121922794)

[Template Version History 3](#_Toc121922795)

[Stakeholders 3](#_Toc121922796)

[Review 3](#_Toc121922797)

[Approval 4](#_Toc121922798)

[Document Contact Details 4](#_Toc121922799)

[About this Document 5](#_Toc121922800)

[Audience 5](#_Toc121922801)

[Related Documents 6](#_Toc121922802)

[Definitions 6](#_Toc121922803)

[Contents 7](#_Toc121922804)

[1. Introduction 13](#_Toc121922805)

[1.1. Overview 13](#_Toc121922806)

[1.2. Business Context 13](#_Toc121922807)

[1.2.1. In Scope 14](#_Toc121922808)

[1.2.2. Out of Scope 14](#_Toc121922809)

[1.2.3. Assumptions 14](#_Toc121922810)

[1.2.4. Constraints 14](#_Toc121922811)

[1.2.5. Risks 14](#_Toc121922812)

[1.3. Organisational Impact 14](#_Toc121922813)

[1.4. Business Process 15](#_Toc121922814)

[1.5. Business Impact 15](#_Toc121922815)

[1.6. Locations 15](#_Toc121922816)

[2. Requirements 17](#_Toc121922817)

[2.1. Functional Requirements 17](#_Toc121922818)

[2.2. Epics and User Stories 17](#_Toc121922819)

[2.3. Non-Functional Requirements 17](#_Toc121922820)

[2.3.1. Classification of Data 18](#_Toc121922821)

[2.3.2. System Category 18](#_Toc121922822)

[2.3.3. Performance and Volumes 18](#_Toc121922823)

[2.3.4. Availability 19](#_Toc121922824)

[2.3.5. Security 19](#_Toc121922825)

[2.4. Users 19](#_Toc121922826)

[2.5. Use Cases 20](#_Toc121922827)

[2.5.1. Use Case 1 20](#_Toc121922828)

[2.5.2. Use Case 2 20](#_Toc121922829)

[2.5.3. Use Case 3 20](#_Toc121922830)

[3. Solution Overview 21](#_Toc121922831)

[3.1. Solution Description 21](#_Toc121922832)

[3.2. Solution Overview Diagram 21](#_Toc121922833)

[3.3. Change to Baseline 22](#_Toc121922834)

[3.3.1. Current State 22](#_Toc121922835)

[3.3.2. Target State 22](#_Toc121922836)

[4. Application Architecture 23](#_Toc121922837)

[4.1. Application Logical View 23](#_Toc121922838)

[4.1.1. Application Element 1 <add a name> 23](#_Toc121922839)

[4.1.2. Application Element 2 <add a name> 24](#_Toc121922840)

[4.2. Application Process View 24](#_Toc121922841)

[4.2.1. Application Use Case 1 scenario 24](#_Toc121922842)

[4.2.2. Application Use Case 2 scenario 24](#_Toc121922843)

[5. Information and Data Architecture 25](#_Toc121922844)

[5.1. Information and Data Impacts 25](#_Toc121922845)

[5.2. Information Requirements as Business Data Objects 25](#_Toc121922846)

[5.3. Logical Data Model 26](#_Toc121922847)

[5.4. System Data Requirements 27](#_Toc121922848)

[6. Integration Architecture 28](#_Toc121922849)

[6.1. Service Model System Context 28](#_Toc121922850)

[6.2. Service Portfolio 29](#_Toc121922851)

[6.3. Service Definitions 29](#_Toc121922852)

[6.3.1. <add Application> Provider Service Information 29](#_Toc121922853)

[6.3.2. <add Application> Consumer Service Information 30](#_Toc121922854)

[6.3.3. <add Application> Publish Event Information 31](#_Toc121922855)

[6.3.4. <add Application> Schedule Event Information 31](#_Toc121922856)

[7. Infrastructure Architecture 33](#_Toc121922857)

[7.1. Hosting 33](#_Toc121922858)

[7.2. Internal Domains 33](#_Toc121922859)

[7.3. Environments 34](#_Toc121922860)

[7.4. Infrastructure Overview Model 34](#_Toc121922861)

[8. Infrastructure Impacts 36](#_Toc121922862)

[8.1. Platform Impacts (On-Premises) 36](#_Toc121922863)

[8.1.1. Platform Impacts (On-Premises) 37](#_Toc121922864)

[8.1.2. Storage Impacts (On-Premises) 37](#_Toc121922865)

[8.2. Platform Impacts (Cloud) 38](#_Toc121922866)

[9. Network Architecture 40](#_Toc121922867)

[9.1. On-Premises Network Architecture 40](#_Toc121922868)

[9.1.1. Network Overview 40](#_Toc121922869)

[9.1.2. Wide Area Network 40](#_Toc121922870)

[9.1.3. Gateway Architecture 40](#_Toc121922871)

[9.1.4. Load Balancing 40](#_Toc121922872)

[9.1.5. Firewall Rules / Ports 41](#_Toc121922873)

[9.2. Cloud Network Architecture 41](#_Toc121922874)

[9.2.1. Network access overview 41](#_Toc121922875)

[9.2.2. Network Overview 41](#_Toc121922876)

[10. Business Continuity / Operations management 42](#_Toc121922877)

[10.1. Backup 42](#_Toc121922878)

[10.2. Monitoring 43](#_Toc121922879)

[10.3. Data Replication 44](#_Toc121922880)

[10.4. Disaster Recovery 44](#_Toc121922881)

[11. Security Architecture 46](#_Toc121922882)

[11.1. Identity and Access Management 46](#_Toc121922883)

[11.2. Data Protection 47](#_Toc121922884)

[11.3. Network Security 47](#_Toc121922885)

[11.4. Audit and Logging 48](#_Toc121922886)

[11.5. COTS Products and Cloud Services Assessment 49](#_Toc121922887)

[11.5.1. <add Application> COTS Product or Cloud Service 1 49](#_Toc121922888)

[11.5.2. <add Application> COTS Product or Cloud Service 2 50](#_Toc121922889)

[12. Development View 51](#_Toc121922890)

[12.1. Development Approach 51](#_Toc121922891)

[12.2. Environments Used 51](#_Toc121922892)

[12.3. Release Management 51](#_Toc121922893)

[12.4. Packaging Requirements 51](#_Toc121922894)

[12.5. Maintenance and Enhancement Guidelines 51](#_Toc121922895)

[13. Architecture Decisions 52](#_Toc121922896)

[13.1. Architecture Decision 52](#_Toc121922897)

[13.1.1. Decision Constraints 53](#_Toc121922898)

[13.1.2. Options Considered 53](#_Toc121922899)

[13.1.3. Recommended Decision 54](#_Toc121922900)

[13.1.4. Related Decisions 54](#_Toc121922901)

[Appendix A. References 55](#_Toc121922902)

[A.1. System Recovery Ratings 55](#_Toc121922903)

[A.2. Pattern Type 55](#_Toc121922904)

[A.3. Application Impact Type 55](#_Toc121922905)

[A.4. Integration Impact Type 56](#_Toc121922906)

[A.5. Architecture Impact Type 56](#_Toc121922907)

**Tables**

[Table 1: Impacted organisations and stakeholders 14](#_Toc121922908)

[Table 2: Locations 15](#_Toc121922909)

[Table 3: Functional Requirements 17](#_Toc121922910)

[Table 4: System Category 18](#_Toc121922911)

[Table 5: Types of System Users 19](#_Toc121922912)

[Table 6: Business Data Objects derived from Business Process Models 26](#_Toc121922913)

[Table 7: Entities 26](#_Toc121922914)

[Table 8: Entity/Attribute Mapping 27](#_Toc121922915)

[Table 9: Used/Dependent/Impacted Systems of Engagement and Data Stores of Record 27](#_Toc121922916)

[Table 10: Service Portfolio 29](#_Toc121922917)

[Table 11: <Application> Provider Service Information - <Service ID> 29](#_Toc121922918)

[Table 12: <Application> Consumer Service Information - <Service ID> 30](#_Toc121922919)

[Table 13: <Application> Publish Event Information - <Service ID> 31](#_Toc121922920)

[Table 14: <Application> Subscribe Event Information - <Service ID> 31](#_Toc121922921)

[Table 15: Type of Hosting Provider 33](#_Toc121922922)

[Table 16: Cloud Components 35](#_Toc121922923)

[Table 17: On-Premise Components 35](#_Toc121922924)

[Table 18: Infrastructure Configuration 36](#_Toc121922925)

[Table 19: Platform Configuration 37](#_Toc121922926)

[Table 20: Indicative Impacts on Storage 37](#_Toc121922927)

[Table 21: Infrastructure Configuration - Cloud 38](#_Toc121922928)

[Table 22: Firewall Rules / Ports 41](#_Toc121922929)

[Table 23: Impact on Data Protection 42](#_Toc121922930)

[Table 24: Monitoring Specification 43](#_Toc121922931)

[Table 25: Architectural Decision - <TITLE> 52](#_Toc121922932)

[Table 26: System Recovery Ratings 55](#_Toc121922933)

[Table 27: Pattern Type Legend 55](#_Toc121922934)

[Table 28: Application Impact Type Legend 55](#_Toc121922935)

[Table 29: Integration Impact Type Legend 56](#_Toc121922936)

[Table 30: Architecture Impact Type Legend 57](#_Toc121922937)

**Figures**

[Figure 1: Document Context 5](#_Toc121922938)

[Figure 2: High Level business process flow 15](#_Toc121922939)

[Figure 3: <Add Figure Title> 20](#_Toc121922940)

[Figure 4: <Add Figure Title> 20](#_Toc121922941)

[Figure 5: <Add Figure Title> 20](#_Toc121922942)

[Figure 6: Solution Overview Diagram 21](#_Toc121922943)

[Figure 7: Solution Overview Diagram 23](#_Toc121922944)

[Figure 8: Application Use Case – <Application use Case 1 Scenario> 24](#_Toc121922945)

[Figure 9: Business Process Model with Business Data Objects exposed 26](#_Toc121922946)

[Figure 10: Project Logical Data Model 26](#_Toc121922947)

[Figure 11: System Integration / Data Flow Diagram 27](#_Toc121922948)

[Figure 12: Enterprise Integration Architecture layers 28](#_Toc121922949)

[Figure 13: Service Model System Context 28](#_Toc121922950)

[Figure 14: Platform Overview Model 34](#_Toc121922951)

[Figure 15: Platform Overview Model 40](#_Toc121922952)

[Figure 16: WAN Overview 40](#_Toc121922953)

[Figure 17: Gateway Overview 40](#_Toc121922954)

[Figure 18: Network Security Elements 48](#_Toc121922955)

[Figure 19: Network Security Physical Elements 48](#_Toc121922956)

Introduction

<This section should provide the project’s contextual general description of the solution / system that provides a frame for the rest of the document. This can be an extract from the Project Initiation Document (PID), Concept Brief (CB) or other business requirements document.

This section should consider and answer, where applicable, the following questions:

1. What is the business problem that this solution will address? Are there business architecture artefacts that are inputs into this document?
2. Does this solution have any impact on business processes? Will there be business capabilities that this solution creates/changes/removes?

It is expected that this High-Level Solution Design aligns with the Concept Brief (if this is produced prior to commencing this HLSD), its predecessor document. Sometimes changes to the design may occur as design development continues after the approval of the Concept Brief. Therefore, any deviations from the design as documented in the Concept Brief should be clearly documented along with its reasons.>

* 1. Overview

<Insert a high-level summary of the business problem and a brief description of what the system will do including system name.

Refer to ICT System and Services Authorisation Policy for service type definitions>

ICT Service Type is Choose an item.

Current system status is Choose an item.

* 1. Business Context

<Provide a description on the capability or business outcome that this project/programme is intending to deliver for this release. This may be a specific business problem or need.

The depth and breadth of detail in this section depends on the complexity of the solution. There should be enough detail to provide context within this document without needing to reference a separate document. Where possible, identify the strategic focus of the solution and risk profile.

Describe how this solution proposes to address the business problem. Consider the people, organisations and systems that play a significant role in the business process or domain that are relevant to the scope of work and potential change. More detail on this is provided in subsequent sub-sections.>

* + 1. In Scope

Provide specific details as to what is in-scope for the solution.

* + 1. Out of Scope

<Provide specific details as to what is out-of-scope for the solution.>

* + 1. Assumptions

<Provide specific details as to the assumptions that have been made regarding the solution.>

* + 1. Constraints

<Provide specific details as to the constraints that have influenced the solution.>

* + 1. Risks

<Provide specific details as to any risk that the solution may not address or may introduce.>

* 1. Organisational Impact

<State the business domain the solution is located within where business domain may be a department or agency, or a business group or division within DEWR.>

This solution is a part of the business domain(s).

<Describe where and how the project has an impact on Organisations and Stakeholders (internal and external). Consider business groups, sections and/or work staff and other Australian Government Departments and Agencies.>

The following table identifies the organisation units and stakeholders (internal and external) that are impacted by this project.

Table : Impacted organisations and stakeholders

| Organisations / Stakeholder | Business Function | Description of Impact |
| --- | --- | --- |
| *FWO* |  |  |
| *Education* |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

* 1. Business Process

<Describe the business processes affected by this change. Where possible, use the Business Process Model and Notation (BPMN) to illustrate this.  
Consider the business capabilities that this solution will create, change and/or remove.>

Figure : High Level business process flow

<Insert High Level business process flow figure>

* 1. Business Impact

<Describe the business roles affected by this change including system users.  
Select a Business Impact level and provide a justification. Refer to the Business Impact Levels tool on the Protective Security Policy Framework site.>

Business Impact is classified as Choose an item.

* 1. Locations

<Identify the locations affected by the solution. Detail existing locations as well as what is being added, removed, or changed at that location.

Examples include:

1. Primary and Secondary Data Centres – Storage and server infrastructure hosting backend transactional systems.
2. Cloud locations>

The following table outlines the locations of where clients, users, infrastructure, and other platforms that support the solution are located.

Table : Locations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Server, service, or Virtual Instance | New or Existing | Asset Type | Location | DR Location |
| *External client* | *Existing* | *User* | *Internet* | N/A |
| *Virtual Server* | *New* | *Server* | *Primary DC* | Secondary DC |
| *Physical Server* | *New* | *Hardware* | *Gateway* | Gateway |
| *Azure Cloud* | *New* | *Subscription* | *Australian Region* | xxxxx |
|  |  |  |  |  |

Requirements

<This section should provide the key requirements addressed by this solution. It should include references into the full business requirements documents (High Level Requirements and Detailed Level Requirements) for traceability.

Alternatively, if this is an agile project then present the epics and high-level user stories and user profiles/ personas.>

* 1. Functional Requirements

<A functional requirement specifies something a system should do.>

< If using agile and the epics and user stories are to be provided then mark this section as ‘N/A – see Epics and User Stories’.>

Table : Functional Requirements

|  |  |  |
| --- | --- | --- |
| Requirement ID  (If known) | Requirement Description | Proposed Solution |
|  |  |  |
|  |  |  |
|  |  |  |

* 1. Epics and User Stories

< If using agile then provide the epics and user stories here otherwise mark this section as ‘N/A – see Functional Requirements’.>

* 1. Non-Functional Requirements

<A non‑functional requirement (NFR) describes how the system works (behaves).

Consider NFRs such as performance, scalability, capacity, availability, reliability, recoverability, maintainability, serviceability, security, regulatory, manageability, environmental, data integrity, usability, and interoperability.

If a solution consists of multiple systems, then each system must be identified and the system category for each system must be listed.

Consider the following:

1. Performance: Is there an increase in performance required? What are the performance parameters required by the solution?
2. Volumes: Is there an increase/decrease in data volumes associated with this solution? Is there a potential for bottlenecks to develop due to an increase in volumes?
3. Availability: What is the intended availability profile for the solution based on the business need?

NFRs that do not align with the System Class must be identified and clearly highlighted in this section.>

* + 1. Classification of Data

<The classification of data referenced, consumed, and generated by the solution needs to be defined. Where a solution stores, transacts or creates different data, each needs to be identified and the classification identified for each type. Refer to the Information Management Policy for classification guidelines.>

* + 1. System Category

<Determine the solution’s System Category by using known or indicative values for Strategic Focus, Risk profile, Availability Profile, Architecture, Business Characteristics, Availability Outages/Month and Recoverability. Provide a rationale for the system class value selected. Refer to the Disaster Recovery Plan for further details of System Class definitions.>

Table : System Category

| **Category** | **Recovery point Objective (RTO)** |
| --- | --- |
| Infrastructure (I) | First to Restore, Infrastructure systems |
| A | 24 hours, Critical systems supporting key components of the Department’s business. |
| B1 | 24 to 48 hours, High availability externally facing systems |
| B2 | 24 to 48 hours, Medium availability externally facing systems |
| C1 | 48 hours to 5 days, High availability internally facing systems |
| C2 | 48 hours to 5 days, Medium availability internally facing systems |
| D | More than 5 days. Non-standard hardware (Default) |

The System Category for the solution is Choose an item.

* + 1. Performance and Volumes

<For new applications, this is particularly important as it assists in the comparison of current vs required platform requirements.

For existing systems, indicate there may be a moderate or significant increase or decrease in the performance and/or volumetrics. Where the solution proposes no change to existing performance and/or volumetrics then state so rather than delete this section.>

* + 1. Availability

<Provide the solution’s availability requirements. Availability values stated here must be in alignment with the System Category of the solution defined above. Where a solution proposes to change its existing availability (uplift or downgrade) then clearly states the current and target availability requirements.>

* + 1. Security

<Security requirements are divided into the three categories of design, technical and non-technical.

* + - 1. The design requirements describe how the system should be designed with security.
      2. The technical requirements represent the functional and non-functional security expectations for the system.
      3. The last category is the non-technical requirements that represent the people and process security requirements for the development, operation, and use of the system

Document any solution-specific security requirements that have been identified. Complete this section after discussions with the Cyber Assurance team. It may be more suitable to include the security content in the Security Architecture section of this document instead.

Refer to guidance on the [Protective Security Policy Framework](https://www.protectivesecurity.gov.au/publications-library/policy-8-sensitive-and-classified-information) site for security classification.>

* 1. Users

Table : Types of System Users

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type of System Users | approximate number of users | roles and responsibilities | clearance requirements | authentication Methods |
| Standard Users (Internal) |  |  | *e.g. Nil, Baseline, NV1* | *e.g. Single-Sign-On, MFA* |
| Privileged Users (Internal) |  |  |  |  |
| Other Government agency |  |  |  |  |
| Members of the public |  |  |  |  |
| Program participants |  |  |  |  |
| External Service Providers |  |  |  |  |

< If using agile then provide user profiles and personas here.>

* 1. Use Cases

<This section should provide the key use cases for the solution. Provide Use Case diagrams where appropriate. If using agile and the epics and user stories have been provided earlier then mark this section as ‘N/A – see epics and stories.>

* + 1. Use Case 1

Figure : <Add Figure Title>

<Insert Use Case Diagram here>

* + 1. Use Case 2

Figure : <Add Figure Title>

<Insert Use Case Diagram here>

* + 1. Use Case 3

Figure : <Add Figure Title>

Insert Use Case Diagram here

Solution Overview

<This section is to provide context as to what the solution will be delivering. This section requires three key elements:

1. Description of the solution
2. Overview diagram
3. The change the system provides from Baseline as-is to the Target / modernised state

Use discretion in the level of detail to be provided – consider how much detail is required compared to what will be provided in the Detailed Design document if one is being produced.>

* 1. Solution Description

<The Solution Description needs to identify all the elements of the solution including:

* Core systems required to deliver the business requirements, including new systems being added, existing systems being changed and systems that are being removed.
* Impacted systems required by the solution, including existing systems being leveraged: e.g., an Enterprise Service Bus (ESB) connection, authentication sources being used, and IT support services.
* Cloud based products and services used (PaaS, SaaS, IaaS and so on…).
* Overview of all the systems and elements that make up the solution and what they will be used for.
* How the solution is integrated into the DEWR environment.>
  1. Solution Overview Diagram

Figure 6: Solution Overview Diagram

<Insert an Overview Diagram here>

<The Overview Diagram is a pictorial view of all the systems and locations required to provide the solution.

1. The diagram foundation is based on locations with each location shown separately – e.g., Internet, Cloud, Gateway, Primary DC, Secondary DC etc
2. The diagram needs to clearly identify the cloud components, where they reside (Hub, Spoke etc.).
3. Each element needs to be located within a location area and the relationship between each element shown. This can be achieved by nesting information elements within application and database elements that reside within platform elements within a location.
4. The diagram needs to demonstrate (at a high level) how the components will work together and integration into the DEWR on and off-premises environment.>
   1. Change to Baseline
      1. Current State

<Describe the baseline (As Is) covering the:

* 1. Current Information flows
  2. People
  3. Organisation
  4. Technology
  5. Information>
     1. Target State

<Describe the target state (modernisation) covering the:

* 1. Target state Information flows
  2. People
  3. Organisation
  4. Technology
  5. Information>

Application Architecture

<The department should have existing application patterns that are in use and are applied.

Describe what is IN pattern and what is OUT of pattern. Where components are OUT of pattern and are of architectural significance then you will need to produce an Architecture Decision.

Consult with the department’s Enterprise Architect to discuss whether the change proposed is of architectural significance. **Refer to 12 Architecture Decisions** if an architecture decision is needed.>

* 1. Application Logical View

A logical view of the proposed application environment showing application components is shown in Figure 7: Logical view of system. The following sections of this document describe this view in more detail.

Figure 7: Solution Overview Diagram

<Insert Application Logical View figure>

<The following sections should describe each new application component. These sections need to be modified to accommodate each component of the application solution. The application component can include roles, databases, COTS products, vendor products, integration component (such as Web Services), exception handling, application-level failover, etc.>

* + 1. Application Element 1 <add a name>

Each section needs to describe one of the application elements outlined in the Application Logical View diagram. This can include a role, application component, or be based on the function that application element is performing.

The following information is required as a minimum for each element:

1. Description of the application function – vendor information, product name, etc.
2. Function the application element will be performing
3. Information it consumes through lookups, human input or locally stored
4. Information it generates – writes to DBs, returns to humans or stores passes on to other services
5. Platform it needs to reside on (e.g., windows on x86, AIX on P series, etc.)
6. Vendor – provide details of the vendor for this component e.g. Microsoft, include where the organisation’s headquarters and most developers are located
7. System Hosting – Is it Internally or Externally Hosted or Cloud?
   * 1. Application Element 2 <add a name>
   1. Application Process View

The following sections describe the use cases and how the application elements contribute to each step of the process flow. Describe as many scenarios as possible that are significant (key scenarios, risk, complexity) for the solution. Include diagrams where appropriate.

* + 1. Application Use Case 1 scenario

<Describe the application scenario and include diagrams where appropriate.>

Figure 8: Application Use Case – <Application use Case 1 Scenario>

<Insert Application Use Case figure>

* + 1. Application Use Case 2 scenario

Information and Data Architecture

<Information and Data Architecture promotes data quality and trust to support decision making in the Department, and the creation and maintenance of actionable, discoverable, information and knowledge.

Understanding how data is collected, represented, transformed, stored, accessed, and retired forms the foundation of the enterprise information and data architecture. Consult with the Architecture Team for assistance in filling out this section.>

* 1. Information and Data Impacts

<Provide an indication of how the solution proposes to use information and data.

Consider:

1. what information and data are input in and output by the solution?
2. what processing of that data is required (data transformation, data migration)?
3. where the data is stored (existing database, new database, Data Warehouse implications)
4. what is the System of Record for the solution’s information/data, or is this a System of Reference?
5. who uses this information (department or external)?

Provide a summary of where information will be received, how it is received, where it comes from, and where it will be distributed to. Use the Standard Service Overview and Standard Service Description figures to show this. Modify the Visio template below to reflect the solution:

Supplement these figures with explanatory text if necessary.

Ensure the solution’s use of information and data aligns with the enterprise information and data use and management policies.

<Insert Information and Data Impact statements>

* 1. Information Requirements as Business Data Objects

<Business Information Requirements are data objects identified by the business as critical components in performing business activities or delivering business services. These data objects exist as inputs to or outputs from the business activities, whether a core business activity or a supporting business activity. Examples include reports, queries, emails.

In this subsection, the business information/data requirements must be identified as Business Data Objects (BDOs) illustrated as data inputs and data outputs to business processes. To illustrate the BDOs properly, the business processes associated with the project need to be decomposed to the L2 or L3 level. Generally, L2 business processes provide enough detail for Business Data Objects (BDOs) to be present and meaningful. In some cases, Service Hierarchies or Business Function Value Chains can also be annotated with BDOs, however, some of the business context may not be clear.>

Figure 9: Business Process Model with Business Data Objects exposed

<Insert BPM with BDO exposed figure>

<BDOs should be described as an object. The components of the BDO can be a simple list of major data types (or subject areas). Presentation of this information should be presented in a table.>

Table : Business Data Objects derived from Business Process Models

|  |  |
| --- | --- |
| **Business Process** | **Business Data Objects** |
| *Business Process 1* | *BDO 1* |
|  | *BDO 2* |
| *Business Process 2* | *BDO3* |

* 1. Logical Data Model

<Logical Data Models (LDMs) are entity-relationship diagrams used to illustrate the structured relationship and dependencies of the data required by the business to perform business activities or provide business services. LDMs, and their associated data dictionaries, define the data environment as a set of interrelated entities, each with a collection of attributes, or data elements, which in turn are described by data properties, value ranges and other metadata.

In this subsection, Project LDMs should be used to describe the data, their relationships and structures required for the project to deliver its capability to the business. Project LDMs should reflect the major entities or subject areas identified as BDOs from the previous subsection. Project LDM should clearly identify those new data elements and structures as requirements.>

Figure 10: Project Logical Data Model

<Insert Logical Data Model figure>

<You can create a high-level conceptual data model first and then develop multiple subject areas LDMs. Additional data views may be required to help articulate data services requirements as well, based on the complexity of the information environment or the data requirements.

Typically, Project LDM Entities and Attributes should be described in a Project Data Dictionary. The components of the Data Dictionary can be presented in a table to identify every Entity with its Attributes and their Properties forming the Project LDM.>

Table : Entities

|  |  |
| --- | --- |
| **Entity Name** | **Description** |
| *Entity 1* |  |
| *Entity 2* |  |
|  |  |

<For traceability in the process, a BDO-to-Entity/Attribute mapping may be requested as well.>

Table : Entity/Attribute Mapping

|  |  |  |  |
| --- | --- | --- | --- |
| **Entity Name** | **Attribute Name** | **Description** | **Properties** |
| *Entity 1* | *Attribute 1* |  | *Date* |
|  | *Attribute 2* |  |  |
| *Entity 2* | *Attribute 3* |  |  |

* 1. System Data Requirements

Systems Data Requirements are high-level specifications that identify systems, applications and data stores used to collect, transport, transform, create, store, access, report, archive and destroy data. In this subsection, logical system components (systems, applications, and data stores) and required data flows are identified using data flow or systems integration diagram (take note: traditional DFDs, or Yourdon-DeMarco Decompositions, or UML Sequence diagrams are suitable).

At an L2 level, data flows between the project application components and external system boundaries or named data stores are satisfactory for the High-Level Solution Design.

Figure 11: System Integration / Data Flow Diagram

<Insert System Integration / Data Flow figure>

System Data Requirements must also include a table that maps the data requirements identified in the previous two subsections to each of the data flows identified in this subsection. This mapping can be represented as a table illustrating flows to/from systems, applications and data stores required by the project to deliver the desired capability.

Table : Used/Dependent/Impacted Systems of Engagement and Data Stores of Record

|  |  |  |
| --- | --- | --- |
| **Entity Name** | **To/ From Systems** | **Description** |
| *Entity 1* | *To Target 1* |  |
|  | *From Source 1* |  |
| *Entity 2* | *To Target 2* |  |
|  |  |  |

Integration Architecture

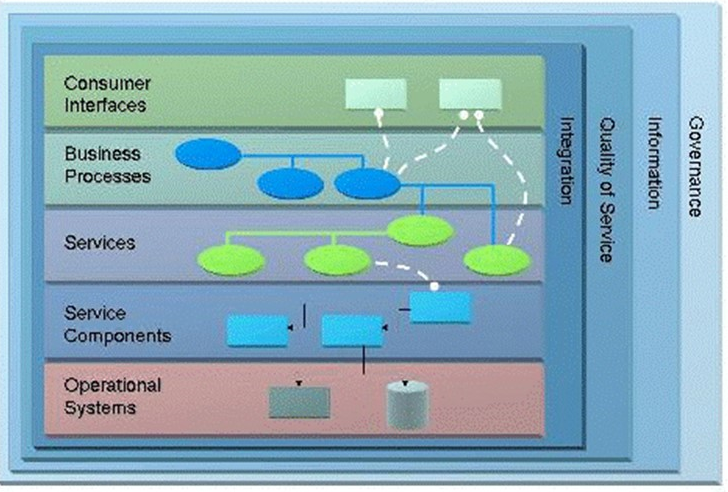
<The department should have existing integration patterns that are in use and are applied. Describe what is IN pattern and what is OUT of pattern.

Where components are OUT of pattern and are of architectural significance then you will need to produce an Architecture Decision. Consult with your Lead Architect and/or Enterprise Integration Architect to discuss whether the change proposed is of architectural significance. Refer to **Section 12 – Architecture Decisions** if an architecture decision is needed.

If there are no integration services being added, changed, or decommissioned, then state so. In this instance only, all sub-sections under Integration Architecture can be removed.>

This section contains the integration architecture for the solution. The integration architecture is the blueprint for how the solution will integrate with each system or component that it exchanges data with in realising the business requirements.

Figure 12: Enterprise Integration Architecture layers



* 1. Service Model System Context

Describe how the solution does what it is supposed to do from an integration perspective. Use a system context diagram showing the Service Providers, Service Components, Service Categories and Service Consumers required for the solution.

Clearly identify new services, updated services, and new providers/consumers of existing integration services.

Figure 13: Service Model System Context

<Insert Conceptual Integration View figure l>

* 1. Service Portfolio

<Detail the consumed and provided services required by the solution that are being added, changed, or decommissioned. Use **Appendix A3 Integration Impact Type** to determine the impact type.>

The following table catalogues the consumed and provided services required by the solution that are new or being changed.

Table : Service Portfolio

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Service ID** | **Service Category** | **Service Name** | **New /  Existing** | **Service Source (Provider)** | **Service Destination (Consumer)** | **Impact Type and Description of Changes** |
| *SV-NNN* |  |  |  |  |  | *Provide the Impact Type, the business purpose of the service, and a description of what is being changed.* |
|  |  |  |  |  |  |  |

* 1. Service Definitions

<Each sub-section has a specific application and integration service type combination.

For each application, choose the appropriate integration service type (Provider Service, Publish Event, Subscribe Event or Consumer Service) sub-section to fill in for each service to be described. A separate table is required for each service/event for that application.

Note that these sections may be accumulated as they are designed and deployed.>

The following section(s) document the new and/or changed internal and external services/events that are consumed and provided by this solution at a functional/logical level. It also provides release impact information on these services.

* + 1. <add Application> Provider Service Information

<Include in this section the details for each new or modified service that is being provided by this specific application as a part of the solution. Each service requires its own table. Replicate the table as required. If there are no Provider Services being added or changed, this section can be deleted.>

Table : <Application> Provider Service Information - <Service ID>

|  |  |
| --- | --- |
| **Item** | **Details** |
| Service Name: |  |
| Service ID: |  |
| Service Registry Status: | *New / Operational / Deprecated / Decommission* |
| Business Purpose: | *Business purpose of service* |
| Input data: | *Expected input data based on Logical Data Model* |
| Behaviour: | *Message Exchange Pattern, Assumptions, Dependencies, Service Variant, Non-Functional Requirements – volume and expected response time, etc.* |
| Output data: | *Expected input data based on Logical Data Model* |
| Release Impact: | *Describe the change to the service* |

* + 1. <add Application> Consumer Service Information

<Include in this section the details for each new or modified service that is being consumed by this specific application as a part of the solution. Each service requires its own table. Replicate the table as required. If there are no Consumer Services being added or changed, this section can be deleted.>

Table : <Application> Consumer Service Information - <Service ID>

|  |  |
| --- | --- |
| Item | Details |
| Service Name: |  |
| Service ID: |  |
| Business Purpose: | *Business purpose of service* |
| Input data: | *Expected input data based on Logical Data Model* |
| Behaviour: | *Message Exchange Pattern, Assumptions, Dependencies, Service Variant, Non-Functional Requirements – volume and expected response time, etc.* |
| Output data: | *Expected input data based on Logical Data Model* |
| Release Impact: | *Describe the change to the service* |

* + 1. <add Application> Publish Event Information

<Include in this section the details for each new or modified publish event that this specific application notifies as a part of the solution. Each publish event requires its own table. Replicate the table as required. If there are no Publish Events being added or changed, this section can be deleted.>

Table : <Application> Publish Event Information - <Service ID>

|  |  |
| --- | --- |
| **Item** | **Details** |
| Event Name: |  |
| Event ID: |  |
| Service Registry Status: | *New / Operational / Deprecated / Decommission* |
| Description: | *Description of Event* |
| Notification Data: | *List of attributes in the event notification based on Logical Data Model, and provide event type code and description if known* |
| Behaviour: | *Message Exchange Patterns, Assumptions, Dependencies, Service Variant, Non-Functional Requirements – volume* |
| Release Impact: | *Does this release change this event?* |

* + 1. <add Application> Schedule Event Information

<Include in this section the details for each new or modified subscribe event that this specific application subscribed to as a part of the solution. Each subscribe event requires its own table. Replicate the table as required. If there are no Subscribe Events being added or changed, this section can be deleted.>

Table : <Application> Subscribe Event Information - <Service ID>

|  |  |
| --- | --- |
| **Item** | **Details** |
| Name |  |
| Event ID |  |
| Description | *Description of Event* |
| Topic Name | *Refer Event Model* |
| Event Filter | *Specific subscriber requirements for filtering the event* |
| Notification Data | *List of attributes in the event notification based on Logical Data Model* |
| Behaviour | *Non-Functional Requirement such as volumes]* |
| Release Impact | *Does this release change this event?* |

Infrastructure Architecture

<Infrastructure Architecture is concerned with the physical requirements of the solution.

The department should have existing infrastructure patterns that are in use and are applied. Describe what is IN pattern and what is OUT of pattern. Consult with your Lead Architect and/or Enterprise Infrastructure Architect for assistance in filling out this section.

Where components are OUT of pattern and are of architectural significance then you will need to produce an endorsed Architecture Decision. Consult with the Architecture Team to discuss whether the change proposed is of architectural significance. Refer to Section 12 Architecture Decisions if an architecture decision is needed.

If there are no infrastructure components being added, changed, or decommissioned, then state so. In this instance only, all sub-sections under Infrastructure Architecture can be removed. Before removing this section, please consider whether the required **System Class** for the solution is supported by its current infrastructure.>

* 1. Hosting

<Provide the name of the hosting provider and the location of the data centre(s). Delete or add details as necessary.>

Table : Type of Hosting Provider

|  |  |  |
| --- | --- | --- |
| Hosting provider | data centre location | details |
| Canberra Data Centres | Hume and Fyshwick |  |
| Microsoft Azure | Australia Central  Australia Central 2  Australia East  Australia Southeast | {Provide tenant ID and name} |
| Amazon Web Services | Sydney |  |

* 1. Internal Domains

Select system domains in scope:

Internet Data Centre (IDC)

Enterprise Data Centre (EDC)

External Data Centre (XDC)

Internet Gateway Environment (IGE)

Secure Zone (SECOPS)

Fortress

Nation

Microsoft Azure

Not Applicable

* 1. Environments

Select system environments in scope:

Development

Test

Pre-Production

Production

* 1. Infrastructure Overview Model

<Describe the platform required to host the application. Use the platform overview model Visio template (Fig 15). Supplement the figure with explanatory text if necessary.

Clearly identify new and updated infrastructure components and what environments they will be deployed to:

1. Non-Prod, Stage, Prod
2. Internal Network, Gateway, AWS, Azure, etc>

Figure 14: Platform Overview Model

<Modify the below Visio Platform Overview Model >



Table : Cloud Components

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Cloud Resource | Monitoring | Backup & Recovery | High Availability | DR/ BCP | Service Plan/ Tier Used | Standard Pattern |
| *Azure AD* | *Standard* | *Standard* | *Yes* | *Geo redundancy* | *Premium* | *Yes* |
|  |  |  |  |  |  |  |

Table : On-Premise Components

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| On-Premise | Monitoring | Backup & Recovery | High Availability | DR/ BCP | Standard Pattern |
| *SQL Server* | *Standard* | *Standard* | *Yes* | *Geo redundancy* | *Yes* |
|  |  |  |  |  |  |

Infrastructure Impacts

<List any additions/changes to the infrastructure by identifying:

1. Infrastructure Component: Function/App
2. Status: New / Existing / Changing / Decommission
3. Location: FDC / HDC / Cloud
4. Domain: Gateway / Management Zone / On Premise / Nation
5. DEWR environment:
   * 1. Development
     2. System Test
     3. Staging
     4. Pre-Prod
     5. Production
6. Network segmentation
   * 1. Application X - UNCLASSIFIED / PROTECTED
     2. Gateway – Tier 1 / Tier 2
     3. On-Premises Internal Network – Common Zone / Data Zone / System Zone / Application Zone / Management Zone / etc
     4. Cloud Segmentation
     5. Management Zone – Tools / etc
7. Does this use a standard pattern that have been through the department’s approval process? Yes / No
8. Quantity- How many components are needed?

Examples of these are identified in the table below.

* 1. Platform Impacts (On-Premises)

Table : Infrastructure Configuration

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Infrastructure component | Status | Hosting Location | Domain | Environment | Network Segment | Standard Pattern | Quantity |
| *Production AD Server* | *New* | *FDC* | *Nation* | *Production* | *On-Premise Internal Network – Common Zone* | *Yes* | *3* |
| *Production AD Server* | *New* | *HDC* | *Gateway* | *Production* | *Gateway* | *Yes* | *3* |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

* + 1. Platform Impacts (On-Premises)

The following sections list the new and changing hardware, operating system, middleware, and cloud components that are required for this solution.

Table : Platform Configuration

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Platform component | Status | Device Type | Operating System | CPU | Memory | Network | Hosted Applications / Middleware |
| *Production AD Server* | *New* | *Virtual* | *Win Svr 2012 R2* | *8* | *32GB* | *Public / private / heartbeat / backup / etc….* | *Windows AD* |
| *Production AD Server* | *Existing* | *Virtual* | *Win Svr 2012 R2* | *8* | *32GB* | *N/A* | *Azure AD* |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

* + 1. Storage Impacts (On-Premises)

<Provide an indication of any additional storage requirements required for this solution by identifying the below. (Modify the below to suit the departments hybrid and hosting environment).

Describe how the data will be managed throughout its lifecycle. Consider:

1. Will the data be archived at a certain point?
2. What is the data retention period? Refer to Section [5.4 System Data Requirements](#_System_Data_Requirements)>

The following table outlines the indicative impact on storage to support the new and changing platforms delivering the solution.

Table : Indicative Impacts on Storage

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Platform Component | Storage Function | Status | Location | Type | Capacity (GB) | Read / Write Ratio | Vendor’s Recommended Application IOPS (IOPS/GB) | Projected rate of growth per year (%) | Is Storage Replication Required |
| *Production Exchange Server* | *System Drive* | *New* | *FDC* | *Block* | *100* | *40/60* |  | *0%* | *No* |
| *Production Exchange Server* | *Database* | *New* | *HDC* | *Block* | *150* | *50/50* |  | *25%* | *No* |
| *Production Exchange Server* | *Logs* | *New* | *CDC1* | *Object* | *20* | *20/80* |  | *5%* | *No* |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

* 1. Platform Impacts (Cloud)

<Provide a list of products and services used for the solution / application with additional details as outlined in the table below:>

Products and services used for the solution / application are outlined in the table below:

Table : Infrastructure Configuration - Cloud

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Product Group | Product / Service | Resource Group | Cloud Tenancy / Subscription (Hub / Spoke model) | Component Classification | URL (if applicable) | Standard Pattern |
| *Identity Management* |  |  |  |  |  |  |
|  | *Azure Active Directory* |  |  | *Official* |  |  |
|  | *Azure B2C* |  |  | *Official* |  |  |
|  | *myGovId* |  |  |  |  |  |
|  |  |  |  |  |  |  |
| *AppService* |  |  |  |  |  |  |
| *Web App* | *Web App* |  |  | *Official* |  |  |
| *API Management* |  |  |  | *Official* |  |  |
| *Key Vault* | *Key vault* |  |  | *Official* |  |  |
| *Orchestration Service* | *App Service Environment* |  |  | *Official* |  |  |
| *Azure Logic App* |  |  |  | *Official* |  |  |

Network Architecture

The following section outlines the logical network elements required to support and deliver the business requirements of the solution.

* 1. On-Premises Network Architecture
     1. Network Overview

<Describe any new network elements being implemented by the solution and how they relate to the existing network. This may include new or changing Managed Large Networks (MLN) interfaces, new locations, and new gateway zones or networks. Include relevant cloud networks and network resources.

The diagram needs to reflect the network in a logical context highlighting new sites, new WAN/LAN segments with relation to the existing network infrastructure. It should show key network links as well as network services like firewalls, load balancers and other network devices being implemented or leveraged. This includes Cloud network resources, connectors etc.>

Figure 15: Platform Overview Model

<Insert Network Overview figure>

* + 1. Wide Area Network

<Describe any new WAN links being implemented, removed or bandwidth changes on existing links. The diagram needs to reflect the new, existing WAN links, those WAN links being removed, and any bandwidth alterations.>

Figure 16: WAN Overview

<Insert Network Overview figure>

* + 1. Gateway Architecture

<Describe any changes in the gateway environment, including the logical placement of any new components within the Gateway environment. The diagram should depict the logical location of new systems within the gateway environment with relation to the Gateway services being leveraged (reverse proxy, load balancing, firewalls, etc.).>

Figure 17: Gateway Overview

<Insert Gateway Overview figure>

* + 1. Load Balancing

<Describe any load balancer components required by the solution. Separate references need to be made to internal and cloud related load balancers and the Gateway load balancers as they may be managed differently.

This needs to include information concerning the service needing load balancing and the type of load balancing (stateful connection, round robin, etc).>

* + 1. Firewall Rules / Ports

<Provide information on firewall rules (and cloud firewall services) and ports required for this solution.>

Table : Firewall Rules / Ports

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Server | Source | | | Target | | | Comments |
| **Name** | **Protocol** | **Port** | **Name** | **Protocol** | **Port** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

* 1. Cloud Network Architecture

Describe any new network elements being implemented / used by the solution and how they relate to the existing cloud network. This may include new or changing Managed Large Networks (MLN) interfaces, new locations, and new gateway zones or networks. Include relevant cloud networks and network resources.

The diagram needs to reflect the network in a logical context highlighting new tenants, subscriptions with relation to the existing cloud network infrastructure. It should show key network links as well as network services like firewalls, load balancers and other network devices being implemented or leveraged. This includes Cloud network resources, connectors etc.

* + 1. Network access overview
    2. Network Overview

Business Continuity / Operations management

Business continuity is a set of plans, processes and activities required to ensure an organisation’s critical business functions can continue to operate regardless of incidents or events that lead to disruptions in business processing. Business Continuity encompasses a wide range of activities to protect from minor disruptions through to large-scale disaster events. Business Continuity planning usually includes plans focused on people, business processes and ICT.

Business continuity within the context of ICT includes addressing resilience, contingency and recovery of technology to aid the business to continue operating. The main ICT processes used to support business include backup and restore of data, monitoring of systems for health, data replication and disaster recovery planning.

* 1. Backup

<Three areas need to be covered:

1. What is being backed up
2. What is doing the backup
3. What is the retention period of the backups?

These details need to be provided for each data source/type (including operating systems, application configurations, application data, and databases).

This needs to cover what alignment to existing backup standards and highlight where standards are NOT being followed.

Describe how data will be lifecycle managed. Will data be archived at a certain point and what are the data retention periods are (as per Section [5.4 System Data Requirements)](#_System_Data_Requirements)?

Data Protection is achieved by means of a daily backup (e.g. run every 24-26 hours) using the Department’s standard data protection suite using (where appropriate) an agent for applications or traditional file system backups.

Standard backup policy for all identified data will consist of:

* 31 daily backups (1 backup per day, for a cycle)
* Six monthly backups (1 backup per month, for a six−month cycle)

Customised backups may be implemented with a supporting business case and branch manager approval – refer to the Digital Backup and Restore Policy which also described departmental backup solutions by system type and standard retention times.

**Recovery Time Objective (RTO)** and **Recovery Point Objective (RPO)** should be addressed by the availability of the solution implemented. Disaster Recovery is undertaken on a ‘reasonable efforts’ basis.>

The following table outlines the anticipated impact on data protection to support the solution.

Table : Impact on Data Protection

|  |  |  |
| --- | --- | --- |
| Ref | Question | Answer |
| Q1 | What is the MAXIMUM data retention required for the solution? |  |
| Q2 | What archival systems are in place if solution requires retention longer than 13 months? |  |
| Q3 | What will be the initial data size and expected growth? |  |
| Q4 | Will this solution be a Source of Record or a Source of Reference? If so, provide details. |  |
| Q5 | What is the end-to-end information lifecycle management for this solution? |  |

|  |  |
| --- | --- |
| **Backup** | **Requirements** |
| **System Backup** | <Enter the server details and directory path required for backup or enter ‘N/A’ if not applicable> |
| **SQL Backup** | <Enter the server details and database names or enter ‘N/A’ if not applicable > |

* 1. Monitoring

<Three areas need to be covered:

1. What is being monitored (for example hardware health, application health, end user experience monitoring, capacity management, Cloud Service etc.)
2. What platform/tool is providing the monitoring (existing or new, tool location, etc.)
3. Who will be using each type of monitoring information (capacity management, IT Security, IT Service Management, ITO administrators)?

Note that DynaTrace and Azure Application Insights are the Department standard tools for Application Performance Monitoring, Microsoft SCOM is used for server monitoring and Microsoft Sentinel is used for SIEM. You should ensure that your application is compatible with DynaTrace or monitoring services might not be feasible.

Note that the basic service offering can be augmented with enhancements but these are ‘quotable’ services i.e. there are additional costs involved.>

Table : Monitoring Specification

|  |  |
| --- | --- |
| **Monitoring** | **Specification** |
| **Server Monitoring** | <Enter the server details which need to be monitored or enter ‘N/A’ if not applicable>   * Number of servers * Hostname |
| **Application Availability Monitoring** | <Enter the URL’s which need to be monitored or enter ‘N/A’ if not applicable> |
| **Application Performance Monitoring** | <Enter the URL’s which need to be monitored or enter ‘N/A’ if not applicable>  <Please include relevant URL’s, host headers, application servers and database names> |

* 1. Data Replication

<Four areas need to be covered:

1. What data is being replicated
2. Where it is being replicated to
3. How it is being replicated (synchronous, asynchronous, log shipping, SAN level replication, Cloud Service etc.)
4. What is the period between replication events or expected lag between sites?

This needs to cover what is aligned to existing replication standards and highlight where standards are NOT being followed.>

|  |  |
| --- | --- |
| **Data Replication** | **Specification** |
| **Data to be Replicated** | <What data is being replicated> |
| **Replication Location** | <Where it is being replicated to> |
| **Replication Method** | <How it is being replicated: synchronous, asynchronous, log shipping, SAN level replication, Cloud Service etc.> |

* 1. Disaster Recovery

<A description of the Disaster Recovery approach needs to be provided if not documented separately.

This is **not** the same as the Availability and Performance elements listed in the requirements section.

Disaster Recovery needs to describe how the systems will be recovered during an event of significant disruption that is declared by a person of authority as a disaster.

This needs to link to the System Category for the solution, particularly for the required return to operations (RTO) and recovery point objective (RPO) metrics. Refer to Appendix A1 for more information on the System Category.>

Infrastructure (I): First to Restore, Infrastructure systems

A- 24 hours: Critical systems supporting key components of the Department’s business

B1-24 to 48 hours: High availability externally facing systems

B2-24 to 48 hours: Medium availability externally facing systems

C1-48 hours to 5 days: High availability internally facing systems

C2-48 hours to 5 days: Medium availability internally facing systems

D-More than 5 days: Non-standard hardware (Default)

Security Architecture

<Security at its core is about the protection of things of value from those who intend harm. ICT security is the protection of digital assets and the associated ICT systems that hold these digital assets.

NIST defines Security Architecture as ‘A set of physical and logical security-relevant representations (i.e., views) of system architecture that conveys information about how the system is partitioned into security domains and makes use of security-relevant elements to enforce security policies within and between security domains based on how data and information must be protected.’

This section is a high-level view of the security context and select elements of the security architecture of the solution.

The Department has adopted a principle of ‘Secure by Design’ which means that we must consider security from the early stages of the design process. It has been well established that it is far more expensive and usually far less effective to bolt security into a system after it has been built.

Secure system design is foundational to:

* Establishing and maintaining trust in ICT systems, trust in the information they hold and trust in the outcomes they enable
* Ensuring effective protections against the very real and in some cases quite serious threats to our ICT systems

There are four key questions that will drive the security architecture of the solution.

* What are we protecting? Our assets – things of value
* Who are we protecting from? The threats – those who intend harm
* How will we protect? What protection mechanisms and controls will be implemented or relied upon
* How much protection is needed? Proportionate protection

Where required, a full description on the security architecture of this solution will be detailed in depth in a Solution Security Architecture (SSA) Document. The SSA is a logical chapter of the High-Level Solution Design but may be delivered as a separate document. If this is the case, then reference the document and do not replicate the content.

Solution architects/designers, in consultation with Security Architects and Advisors, are responsible for developing the security architecture of a solution.>

* 1. Identity and Access Management

<Select the relevant authentication methods.>

|  |
| --- |
| **Authentication Method (for non-public domain application)** |
| IAS  Verisign  Secure Sockets Layer (SSL)  Site Server 3.0 Membership Authentication (HTML Forms)  Clear Text/Basic Authentication  DB2/Connect /ACF2  Other (specify): |
| **Scope** |
| Apply to the whole site  A secure channel is required for all access to the application (using a server certificate)  A client certificate is required for access to the application  Site Server client certificate mapping is used by the application  Clear Text/Basic Authentication  Apply to partial site (specify)  Other (specify): |

* 1. Data Protection

<Describe mechanisms for data protection.>

|  |  |
| --- | --- |
| **Data Protection** | **Specification** |
| **Encryption in Transit** | e.g. SFTP, HTTPS |
| **Encryption at Rest** | e.g. SQL Encryption |
| **Data Leakage Protection** |  |

* 1. Network Security

< This section will ensure solution components are hosted in the right security zones and highlight at risk network flows.

Describe:

* Network security zones and sub-zones that host the solution components and the system actors
* Flows between system actors and solution components
* Flows between solution components
* Network security dependencies – for example firewall blocks access to a ‘management interface.’]
* Where Cloud technologies are adopted, describe network security components which do the task of traditional on-premise network appliances etc.

This section describes which security zones or <Cloud equivalent zones> the solution components will be hosted and the required network flows between components.

Figure : Network Security Elements

<Insert diagram showing the security network location of the solution elements e.g. zones, sub-zones, internal or external. Ensure flows are labelled with protocol type. The overview diagram may be suitable, or a separate diagram is done>

<Insert paragraphs providing an overview of the network location where the system is deployed, and the type of flows required>

<If available list the firewall (or Cloud equivalent) rules required. Otherwise indicate these will be provided separately>

Figure : Network Security Physical Elements

<Insert a physical diagram of the solution – showing the different physical parts of the solution and which network security zone / sub-zone they are connected to. It is intended to be a high-level physical view>

* 1. Audit and Logging

<Describe how services will be logged and audited.  
Note that DynaTrace and Azure Application Insights are the Department standard tools for Application Performance Monitoring and Microsoft Sentinel is used for SIEM.>

|  |  |
| --- | --- |
| **Logging** | **Specification** |
| **Product Name** | <What is being logged> |
| **Log Location** | <Where it is being logged to: File system location, shipping to SIEM> |
| **Log Storage** | <Size of log files, retention requirements, management requirements, etc.> |
| **Administered Reporting** | <Basic reporting is provided; additional reporting can be requested but is a quotable service> |
| **Additional Monitoring** | <Additional monitoring can be provided for Windows services, disk and network interface statistics, log monitoring, customer/server bandwidth usage, Transmission Control Protocol (TCP) Errors and application centric stats. This is a quotable service> |

* 1. COTS Products and Cloud Services Assessment

The following new products and services which are not yet on the Approved Software List are being introduced.

* + 1. <add Application> COTS Product or Cloud Service 1

<Create one section per new COTS product and list approved software or services to be used.

This section is intended to provide information for the Cyber Assurance team in place of completing a separate Solution Overview Document (SOD).>

* + - 1. Security Certification

<Seek and provide details of evidence from vendor either through direct contact, or via online resources that the vendor or product has undergone a form of security certification e.g. IRAP, ISO 27001, SOC 1, 2 or 3, PCI-DSS, FEDRamp, HIPAA etc.>

* + - 1. Penetration Testing

<Seek evidence from vendor either through direct contact, or via online resources to confirm vendor regularly undertakes penetration testing on their systems. Ideally, request a copy of the most recent penetration test of the product in question and verify that any high-risk issues have been remediated.>

* + - 1. Vulnerability Assessment

<Seek evidence from vendor either through direct contact, or via online resources to confirm vendor regularly undertakes vulnerability assessments on their systems. Ideally, request a copy of the most recent vulnerability assessment report of the product in question and verify that any high-risk issues have been remediated.>

* + - 1. Secure Coding Practices

<Seek evidence from vendor either through direct contact, or via online resources to confirm vendor undertakes secure coding practices.>

* + - 1. Product Vulnerability History

<Capture findings as to whether the product has had any recent publicly known vulnerabilities and if they have been patched by the vendor in a timely manner. Capture details of any security issues raised which have not been resolved or in some way responded to or addressed by the vendor.>

* + - 1. Vendor Cyber Security Incident History

<Capture findings of publicly known cyber security incidents affecting the vendor, or security issues in other products owned by the vendor, where applicable.>

* + 1. <add Application> COTS Product or Cloud Service 2

Development View

<The Development view section will cover and answer the following questions.

* How are the solution components developed?
* What are the environments in place for each of the components?
* How are the solution components progressed through each of the environments?
* Automation for solution lifecycle management?
* Provides information to assist with future maintenance and enhancement including governance, configuration packaging and development environment access and usage
* Development tools used for the solution components.
* Configuration packaging
* Maintenance and enhancement guidelines>
  1. Development Approach
  2. Environments Used
  3. Release Management
  4. Packaging Requirements
  5. Maintenance and Enhancement Guidelines

Architecture Decisions

Architectural Decisions are required when the solution (or a component of the solution) does not comply with a Departmentally‑approved architecture pattern. This may be because the solution is seeking to introduce a new pattern, seek to replace an existing pattern, or implement a non-standard pattern for tactical reasons.

<Are there any Architectural Significant Decisions associated with the solution? Consult with your Lead Architect if unsure.

If the solution is IN pattern, then this section does not need to be completed and the subsections can be removed. State that the solution does not require any Architecture Decisions.

Architecture decisions will be approved by the departments Architecture Board.>

<The solution does not require any Architecture Decisions.>

OR

<The following <architectural decision is/ architectural decisions have been made> and require approval to be implemented.>

* 1. Architecture Decision

Table : Architectural Decision - <TITLE>

|  |  |  |  |
| --- | --- | --- | --- |
| **Subject Area** | Provide a one- or two-line summary of what the Architecture Decision relates to. | **Architecture Domain** | State the architectural domain the architecture decision relates to. One of:   * Business * Application / Integration * Technology * Information * Security |
| **Design Decision** | State the recommended decision detailing both the option number and its summary.  Recommend Option: | **ID.** | If Available |
| **Issue or Problem Statement** | Describe the issue or the problem. | | |
| **Motivation** | Describe the motivation behind the Architecture Decision. | | |

* + 1. Decision Constraints
    2. Options Considered

<Describe each of the options considered (including the recommended option) as a part of investigating the Architecture Decision. Each option should be a separate sub-section under this section. Each sub-section should describe that option in detail. Include details of the advantages & disadvantages, risks & issues, and assumptions & constraints that are associated with that option. A tabular form has been provided but this can be replaced with text if preferred.>

* + - 1. Option <Option Title>

|  |  |
| --- | --- |
| **Description:** | Provide details of what this option entails. Include diagrams where appropriate. |
| **Advantages:** | List the advantages associated with this option. |
| **Disadvantages:** | List the disadvantages associated with this option. |
| **Risks/Issues:** | List any risks and/or issues associated with this option. |
| **Assumptions/ Constraints:** | Describe any assumptions and/or constraints associated with this option. |
| **Implications** | Describe the implications associated with this option. |

* + 1. Recommended Decision

Recommend option:

* + - 1. Justification
      2. Implications
      3. Derived Requirements
    1. Related Decisions

1. References
   1. System Recovery Ratings

Use this table to determine the solution’s System Recovery Rating for Disaster Recovery purposes.

Table : System Recovery Ratings

| **Category** | **Recovery point Objective (RTO)** |
| --- | --- |
| Infrastructure (I) | First to Restore, Infrastructure systems |
| A | 24 hours, Critical systems supporting key components of the Department’s business. |
| B1 | 24 to 48 hours, High availability externally facing systems |
| B2 | 24 to 48 hours, Medium availability externally facing systems |
| C1 | 48 hours to 5 days, High availability internally facing systems |
| C2 | 48 hours to 5 days, Medium availability internally facing systems |
| D | More than 5 days. Non-standard hardware (Default) |

* 1. Pattern Type

A pattern is a general, reusable solution to a common scenario in software architecture within a given context. Another term for a pattern is a building block.

Table : Pattern Type Legend

|  |  |
| --- | --- |
| Pattern Type | Description |
| Current | The change will use existing patterns. |
| New | This is a significant change to the impacted component and will result in the establishment of a new pattern or patterns being introduced that is expected to be adopted by future solutions. |
| Hybrid | The change will use a combination of existing patterns and new patterns |

* 1. Application Impact Type

Table : Application Impact Type Legend

|  |  |
| --- | --- |
| Impact Type | Description |
| Only NFR Impact | The change is only to non-functional requirements (such as performance, volumetric scalability, capacity, availability, reliability, recoverability, maintainability, serviceability, security, regulatory, manageability, environmental, data integrity, usability, and interoperability) |
| Reference Data Only | The change is only to reference data. |
| Modify Small | The change results in small modifications to the impacted component.  This typically involves configuration and/or coding changes. |
| Modify Medium | The change results medium modifications to the impacted component.  This typically involves configuration and/or coding changes of a larger scale or complexity than Modify Small. |
| Modify Large | The change results large modifications to the impacted component.  This typically involves significant configuration and/or coding changes. |
| Decommission | The change results in the decommissioning of the component. |

* 1. Integration Impact Type

Table : Integration Impact Type Legend

|  |  |
| --- | --- |
| Impact Type | Description |
| Only NFR Impact | The change is only to non-functional requirements of a service (such as performance, volumetric scalability, capacity, availability, reliability, recoverability, maintainability, serviceability, security, regulatory, manageability, environmental, data integrity, usability, and interoperability) |
| New Provider / Consumer only | The change only   * adds a new provider of an existing service and/or * adds a new consumer to an existing service. |
| New | The change results in a new service. |
| Update | The change results in a change to the service not otherwise noted. |
| Decommission | The change results in the decommissioning of the service. |

* 1. Architecture Impact Type

The impact of the solution on the ICT architecture is described in the following table.

Table : Architecture Impact Type Legend

|  |  |
| --- | --- |
| Architecture Impact Type | Description |
| None | The scope of the work does not change the ICT architecture.  This is the lowest architecture impact. |
| Low | The scope of the work changes the architecture in a matter that results in little or no risk (unmitigated).   * Software upgrades * Known standard pattern is being used - the scenario is simple (e.g. new server or new service on existing integration points). * Introduce technical debt (simple) that incurs a low cost to the organisation in the maintenance of the alternate solution and the cost to remediate to the preferred solution (such as migration to the preferred solution during the next phase of the program/project or it has been accepted as a Business as Usual (BAU) activity for a subsequent release). |
| Complex | The scope of work changes the architecture in a well-understood manner and uses standard processes.  The complexity of the solution (such as the number of integration points or dependencies) is higher than a Low architecture impact.   * Known standard pattern is used but the scenario is complex. (e.g. new service with new Consumer / Provider). * Introduce technical debt (complex) that incurs a more significant cost to the organisation either through the ongoing maintenance of the alternate solution and/or the cost to remediate to the preferred solution (such as additional funding required for a new program/project to migrate to the preferred solution, the remediation cannot be accommodated through BAU activities). |
| High | The scope of work introduces new architecture where the experience in the Department is low or not well understood.   * New pattern being introduced * New major piece of software.   This is the highest architecture impact type. |