# [System Qualities (Non-Functional Requirements)](#_Toc428542023)

## [Runtime NFRs](#_Toc428542024)

### [Availability](#_Toc428542025)

“Planned Operational Availability”

The times the solution is required to be available and offering non-degraded service in its primary role under normal conditions. This represents the negotiated and agreed ‘up-time’ and excludes planned and agreed outages for system upgrades and maintenance.

| Ref | Description | Target | Solution Traceability |
| --- | --- | --- | --- |
| DNFR-01 | Availability of system for “primary role” functions. | The system must provide service to end-users between 09:00 and 17:00 Monday to Friday (refer decision #217). | Solution:   1. {Org} supporting network infrastructure designed for maximum resiliency. 2. All on-premise virtualised hosting and public cloud platform service levels meet or exceed those required by the solution (refer section 8.3 NFR Alignment). 3. Active monitoring of solution availability (refer section 7.2.2 Operational Monitoring). |
| DNFR-02 | The ability to carry out essential, scheduled maintenance and releases within the agreed service or change window. | Maintenance windows for on-premise systems are reserved between 12:00 and 18:00 on Sundays. Access will be provided by negotiation outside of these times. | Solution:   1. Highly automated (scripted) deployment for platform and application deployments. 2. User facing platform maintenance mode support. Salesforce supports the ability to display a maintenance page during deployment activities as follows:    * Back office (Service Cloud) – Bulk freezing of internal user accounts.    * External portals (Community Cloud) – Deactivating the community portal. |

### [Recoverability](#_Toc428542027)

“Disaster Recovery and Business Continuity”

Recoverability is the ability to re-establish business operations after a service disruption. A disruptive incident and its response are categorised at two levels:

* A Business Continuity Response is triggered by a localised event and will be tailored according to the scale of the event.
* A Disaster Recovery Response is triggered from a significant external event implying a total loss of production capacity.

For more detail of the recoverability solution refer to Section 7.3 Business Continuity View.

| Ref | Description | Target | Solution Traceability |
| --- | --- | --- | --- |
| DNFR-03 | Return to Operation (RTO) | The mean time to recovery (MTTR) in the event of loss of the production processing capacity of the system must be no more than 1 working day. | Interpretation/Assumptions:   1. Measurement of system recovery time applies to core availability hours (refer DNFR-01). 2. The RTO excludes the time required to resolve business transaction consistency errors (once the system is restored).   Solution:   1. Failover to the {Org} Secondary data centre (Orbit) for ArcGIS on-premise components (refer 7.3.5.2 ArcGIS Enterprise). 2. Pipeline-based redeployment of {Soltn} Azure non-global services (refer 7.3.5.3 Azure Services). 3. Salesforce managed DR from a primary to secondary data center (refer 7.3.5.1 Salesforce). 4. Comprehensive backup of solution business data and on-premise servers (refer 7.2.6 *Backup and Restore*). 5. The programme Business Change stream will ensure that relevant business continuity plans are updated to accommodate the new {Soltn} solution. |
| DNFR-04 | Recovery Point Objective (RPO) | In the event of sudden loss of the production processing capacity of the system there must be no loss of committed data older than 4 hours. | Interpretation/Assumptions:   1. The RPO applies to Site Recovery and Local Data Protection. 2. The RPO applies to business/transactional data only (not OS/Platform log files).   Solution:   1. Intraday local recovery of ArcGIS databases from local SQL logs (refer7.3.4 Local Recovery). 2. Intraday backups of the solution Azure SQL database(s) and locally replicated cloud storage accounts (refer 7.3.5 Disaster Recovery). |
| DNFR-05 | Alternate environment capacity. | An alternate environment for operating the system must provide 100% of capacity of the primary environment and deliver full functionality. | Solution:   1. Solution DR provisions can support 100% of capacity requirements (refer 7.3.5 Disaster Recovery). |

### [Security](#_Toc428542028)

“Data Confidentiality, Privacy and Integrity”

The ability to authenticate users and provide authorised service access at the appropriate level. To ensure information confidentiality through authorisation of access within the Ministry, privacy through protection of client information and integrity, protection of information from unauthorised, accidental, or malicious modification.

| Ref | Description | Target | Solution Traceability |
| --- | --- | --- | --- |
| DNFR-06 | The ability to deliver a secure system i.e. one with a level of security risk that has been accepted by {Org}. | This NFR is met via the security accreditation process. | Solution:   1. This NFR is met via application of relevant security principles to the design (validated by the {Soltn} {Soltn} solution security accreditation process).   Refer: 7.1 Security View |

### [Performance](#_Toc428542029)

“Efficiency, Throughput, Response Time, Batch Windows and Capacity”

The system’s ability to complete defined volumes of business transactions (real-time and batch operations) consistently within acceptable times.

| Ref | Description | Target | Solution Traceability |
| --- | --- | --- | --- |
| DNFR-07 | The ability to deliver acceptable response times including during periods of peak demand. | Once platforms and systems are available {Org} and the project vendors will jointly identify inviolable constraints for different transaction/operation types, and what measurement conditions should apply. This will allow baselines to be established and fit-for-purpose measures for the non-functional requirements to be agreed. | Interpretation/Assumptions:   * Measured from when the user selects a destination until the page becomes responsive to user input.   Solution:   1. The candidate transactions and response times will be utilised for capacity planning and acceptance test activities. 2. Capacity planning to ensure sufficient headroom exists for technical platforms. 3. The results of per-release performance testing is used to right-size capacity for Production. |

### [Scalability](#_Toc428542030)

“Expandability and Organic Growth Capability”

The ability of the system to accommodate future increases in the number of users, records and processing load without requiring significant redesign or development.

| Ref | Description | Target | Solution Traceability |
| --- | --- | --- | --- |
| DNFR-08 | The ability to accommodate future growth in number of users, data, and processing load. | The system must be able to support the following (approximate) operational load defined as follows with no/minimal degradation in performance:   * 2,150 users (current total) * 500 concurrent users at peak times (MER and VER periods) * An estimated 500,000 new pieces of work created each month. This includes system-generated tasks, received emails, and received calls. | Solution:   1. All solution cloud platforms support the ability to scale to the required operational load. 2. ArcGIS on-premise server deployments can be scaled up and/or out as required to support the required operational load.   Refer Appendix A: Software Licencing regarding potential licencing impact. |

### [Traceability](#_Toc428542031)

“Audit-ability and Audit trail”

Traceability refers to the ability to retain details of specified business, transactional and system activity and data changes including normal, abnormal and error conditions with selective control.

| Ref | Description | Target | Solution Traceability |
| --- | --- | --- | --- |
| DNFR-09 | All production changes to the system must be executed in accordance with {Org}’s standard Production Change Process and will be logged as part of that process. | N/A | The project will adhere to applicable {Org} ITSM change and release management processes. Specifically:   * Obtaining the necessary approvals via both Technical Change and Change Advisory (business) boards. * For each major release, the Acceptance Into Service (AIS) schedules will include {Org} Operations validation that appropriate Change Requests have been loaded (and approved) via the {Org} enterprise Change Management function. |
| DNFR-10 | The system must maintain a detailed audit log of all user actions. At a minimum, these logs must:   * Record the individual who executed the action. * Record the date and time the action was executed. * Record the significant data elements referenced, manipulated, or changed by the action. * Be retained for no less than 18 months | N/A | Solution:   1. All solution technical platforms support fine grained logging of user activity (refer section 7.2.3 Event Collection and Management). 2. ArcGIS Enterprise (on-premise) supports the required 18 months retention (refer section 7.2.3.3 Diagnostic Event Map). 3. The ArcGIS Online and Salesforce platform user activity and data modification audit logs will be extracted and persisted to Azure Storage via a custom Azure application service (refer section 6.1.4.2.1 Log Aggregation). |
| DNFR-11 | The system must enable {Org} to limit audit log access to authorised users. | N/A | Solution:   1. Audit logs protected via platform and OS-level RBAC (refer section 7.2.3.3 Diagnostic Event Map). |
| DNFR-12 | The system logs should provide for clear, relevant, and timely end to end transaction traceability. | N/A | Solution:   1. Comprehensive logging of user activity and platform events (refer section 7.2.3.3 Diagnostic Event Map). |
| DNFR-13 | Logging configuration must be external to the system so that changes can be made without affecting the system | N/A | Solution:   1. All solution platforms support the ability to configure audit logging independent of application deployment (refer section 7.2.3.3 Diagnostic Event Map). |
| DNFR-14 | The system must produce a detailed log of all system administration activity and any other changes at the system level that will be kept for at least 18 months. | N/A | Solution:   1. All solution technical platforms support fine grained logging of user (inc. admin user) and deployment and configuration activity (refer section 7.2.3.3 Diagnostic Event Map). 2. ArcGIS Enterprise (on-premise) supports the required 18 months retention (refer section 7.2.3.3 Diagnostic Event Map). 3. The ArcGIS Online and Salesforce platform user activity and data modification audit logs will be extracted and persisted to Azure Storage via a custom Azure application service (refer section 6.1.4.2.1 Log Aggregation). |
| DNFR-15 | The system should be able to provide detailed logs for troubleshooting if required | N/A | Interpretation/Assumptions:   1. The ability to configure logging verbosity applies to system activity only. The verbosity of business activity logging is specified in the functional requirements.   Solution:   1. All solution platforms provide detailed logs to support troubleshooting and diagnostics (refer section 7.2.3.3 Diagnostic Event Map). |
| DNFR-16 | The system or connected systems must maintain a log of all managed actions. A “managed action” will include any action that alters a record and is recognised as requiring an audit trail. | N/A | Refer DNFR-10, DNFR-14. |

### [Usability](#_Toc428542032)

“Look and Feel, System Ergonomics, Ease of Use and Safety”

The extent to which the services can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.

| Ref | Description | Target | Solution Traceability |
| --- | --- | --- | --- |
| DNFR-17 | Screens in the system should be in a print friendly format or have a downloadable version of the page. | System should have a print CSS and support best practice for the printing of pages where users would need such functionality. This would exclude the printing of non-content specific areas such as menus, footers etc.  System is proven to support a “Print to PDF” function if this is available on a user’s device. | Interpretation/Assumptions:   1. A consequence of the Information Architecture (UX) process.   Solution:   1. Covered by the solution style guide (refer to Solution Style Guide). |
| DNFR-18 | Any function in the system that takes longer than 10 seconds to load should indicate progress | Where a function with a response to the user has a delay (saving, loading, or retrieving etc.) then the system should indicate progress to the user where the length or the nature of the delay could impact on the user experience.  Note: In general, all interactions between the user and the UI should have some type of visual feedback to indicate system responsiveness. | Solution:   1. The Salesforce platform provides OOTB support for progress indication (refer [here](https://developer.salesforce.com/docs/component-library/bundle/lightning-spinner/example) for an example). In addition, file uploads will include a progress bar. 2. The ArcGIS Web App will display an animated progress indicator for all user requests. |
| DNFR-19 | The system must, at a minimum, be capable of supporting n-1 of the currently supported {Org} web browsers (Google Chrome, Microsoft Edge and Microsoft Edge Chrome). | The system must support the most popular recorded browsers at the date of this being published, as supplied by {Org} GA stats.  For a public facing site, we use {Org}.govt.nz GA stats.  The latest version of Chrome, Safari, Internet Explorer and the last major version and all minor versions before them are currently the most popular. | Solution:   1. Specific OS, browser, and device testing requirements to be defined and included in test plans for each major release. 2. The Salesforce platform has a number of known limitations with the Microsoft Edge Chromium, Firefox and Safari browsers (for more detail refer [here](https://help.salesforce.com/s/articleView?id=sf.getstart_browsers_sfx.htm&type=5)). |
| DNFR-20 | The system must provide all user interfaces using responsive web design approaches, to enable the solution to be utilised across a multitude of devices and resolutions | The system must support mobile devices and follow the progressive enhancement principle.  This is in addition to the browsers mentioned and screen resolution supplied | Solution:   1. The Salesforce Lightning Design System (SLDS) fully supports responsive web design principles and mobile form factors (refer [here](https://developer.salesforce.com/blogs/developer-relations/2017/04/mastering-salesforce-lightning-design-system-grids-lightning-layouts)). 2. The GIS Web App will be built with components that support responsive web design enabling the component to resize and render in a variety of screen sizes and resolutions within the constraints imposed by the Salesforce canvas app. 3. The Solution Style Guide and the project Test Strategy both include support for responsive layouts and associated testing. |

## [Non-runtime NFRs](#_Toc428542033)

### [Flexibility](#_Toc428542034)

“Extensibility and Adaptability to Changing Circumstances”

The ability to enhance existing services, accommodate new service and product types in the future without significant changes to the design.

| Ref | Description | Solution Traceability |
| --- | --- | --- |
| DNFR-21 | The system must be user configurable such that the majority of product configurations and incidental rule changes can be executed within the business without significant technical support. | The solution COTS platforms are specifically designed to improve development efficiency (through reducing the requirement for bespoke development). Preference will be given to delivering functionality via OOTB facilities and configuration vs. bespoke development (refer section 3.2 Architectural Principles).  Note that for the {Soltn} solution, customisation will be required as follows:   * *ArcGIS WebApp*   A custom ASP.NET Web App is required to implement web-based mapping requirements and associated business rules. This is based on ArcGIS web frameworks and is standard practice for the delivery of ArcGIS web-based mapping.   * *Salesforce Apex Script*   Used within the Salesforce platform on an as-required basis to support more complex business rules, object data management and service callouts (integrations).   * *Azure Functions*   Azure Function based Application Service implementations (supporting integration, security, and data management) are developed using .NET code and frameworks.   * *FME Workbenches*   Primarily configuration based but Python script will be required for geo-data management and/or service callouts e.g. orchestrating data with ArcGIS Online to support the offline capture.   * *Geoprocessing Scripts*   As deployed to the ArcGIS Geoprocessing Servers, several Geoprocessing functions will require use of Python script e.g. sample plot generation. |
| DNFR-22 | The system should be modular to allow swapping in or out of components / application functionality (including 3rd party software / components) without impacting on the core application or other components. | The {Soltn} solution architecture emphasises:   * Distinct subsystems representing logical groupings of related system functionality. * Use of modular COTS platforms that deliver capability for separate specific functions. * The promotion of reusable services and alignment with SOA principles and usage patterns. |
| DNFR-23 | The system must allow for customisation of functionality through a supported and managed framework; ensuring that core functionality and upgrades of the solutions are not impacted. | The key solution COTS platforms (Salesforce and ArcGIS) provide frameworks that support a clear separation between the base platform and any customisations. This approach ensures that any customisations remain unaffected through updates and/or upgrades to the underlying platforms. |
| DNFR-24 | The system should be capable of using a service-oriented architecture approach and creating a separation of concerns, allowing for functionality to be reused. | All solution technical platforms provide for comprehensive services-based (RESTful) access to functionality. In addition, integration between key subsystems is brokered via the {Org} Apigee middleware platform (refer decision #25). |
| DNFR-25 | Test scripts for the system must be documented and packaged so that they can be reused. | Test scripts to support manual testing will be developed using XMind and attached to test items in Azure DevOps. Test scripts to support automated testing will be maintained in the test automation tooling (for more detail refer to the {Org} {Soltn} Test Strategy). |
| DNFR-26 | System components, services, patterns, and processes must be documented in accordance with {Org} Architecture Standards, such that they may be readily identified should a future case for reuse be identified. | Solution architecture and design documentation will be developed in line with {Org} standards. applicable document templates and relevant governance and assurance processes. |
| DNFR-27 | System components must be designed and/or selected with reusability as a key driver. This implies:   * Use of standards-based interfaces between components. * Documentation of interfaces and component functionality. | All solution interfaces are standards-based (refer 6.2 Integration View).  During elaboration, best practice integration design principles (inc. consideration of reuse) will be applied to interface design. This will include API governance and assurance by the {Org} Middleware team. |

### [Maintainability](#_Toc428542035)

“Modifiability, Enhancement, Fault Detection, Isolation and Repair”

The ability to maintain the system efficiently: find and remove faults, improve performance, carry out modifications and infrastructure upgrades.

| Ref | Description | Solution Traceability |
| --- | --- | --- |
| DNFR-28 | Any customisation of the system should not impede the maintainability of the solution software. | The key solution COTS platforms (Salesforce and ArcGIS) provide frameworks that support a clear separation between the base platform and any customisations. This approach ensures that any customisations remain unaffected through updates and/or upgrades to the underlying platforms.  In addition:   * Any customisations will only be applied via supported extension points. * Any requirement for significant customisation will require a formal governed decision. |
| DNFR-29 | Any customisations of the system should be done through extensions that are clearly identifiable as belonging to {Org}.  Any extensions should be able to be supported and maintained by {Org} without significant technical support. | Refer DNFR-21. |
| DNFR-30 | Development of {Org} Custom components/code modules for the system must utilise a supported industry standard and widely adopted programming and or scripting language and libraries. | Platform customisations (extensions) and custom code modules utilise platform mandated and/or industry standard development languages and libraries.  Specifically:   * *Salesforce* - Salesforce APEX Script, OmniScript, HTML and CSS (refer section 6.1.2 Salesforce Implementation). * *ArcGIS* – Python script for Geospatial services (refer section 6.1.3 ArcGIS Implementation). * *Azure Services* – Microsoft ASP.NET (GIS WebApp) and .NET (Azure Functions) (refer section 6.1.4 Azure Services Implementation). |
| DNFR-31 | The system must use widely adopted industry technologies, frameworks, and products to ensure longevity, supportability, and availability of expertise. | The {Soltn} solution is based on Salesforce, ArcGIS, and Azure Cloud Services. All platforms are already in active use within {Org} and have a strong local supply chain. |
| DNFR-32 | Third party products must only be incorporated into the production / run time system with {Org} approval via the {Org} Change Management Process. | Any use of third-party products by the solution will require a formal design decision and be subject to applicable {Org} architecture governance and assurance. |
| DNFR-33 | The system must use {Org}’s Incident Management Process to enable the monitoring and management of its components and processes by the relevant SIEM. | Refer to section 7.2.2 Operational Monitoring for an overview of solution monitoring integration (inc. incident alerting and ticketing). |

### Manageability

| Ref | Description | Solution Traceability |
| --- | --- | --- |
| DNFR-34 | The system must include appropriate tools and documented procedures to support its day-to-day operation. | To support production handover, a Solution Operations Manual will be developed. This will cover:   * BAU and/or routine maintenance procedures for the key technical platforms e.g. backup verification checks. * Guidance regarding the triage and diagnosis of production issues/incidents. * The solution support model including key ICT and vendor contact details. * Any third-party remote access requirements for support or BAU platform management. |
| DNFR-35 | The Operation Manual and System Handover Guide for the system must detail any requirement for remote management or support from third parties. | Refer DNFR-34. |
| DNFR-36 | If remote access into {Org}’s network is required by the support provider of the system, then this must be approved and should follow {Org} Change Management process | Any requests for remote access by third party support provides will follow {Org}’s established user and change processes. |
| DNFR-37 | The system must support SLA monitoring to confirm availability and performance. | The solution will support end-to-end monitoring of solution health and performance.   * Refer section 6.1.4.3 Health Monitoring for an overview of the Azure Monitor based solution health dashboard(s). * Refer section7.2.2 Operational Monitoring for an overview of health monitoring alert rule configuration. |
| DNFR-38 | The system should allow {Org} to use its standard SLA monitoring tool to confirm availability and performance. | At the time of writing, {Org} does not have a centralised, shared tool for availability and performance monitoring. Currently Azure App Insights is being trialled for several on-premise web applications.  The {Soltn} solution is proposing to use Azure App Insights in combination with Azure Monitor dashboards to provide end-to-end health and performance monitoring (refer section 7.2.2 Operational Monitoring). |

### [Deployability](#_Toc428542025)

| Ref | Description | Solution Traceability |
| --- | --- | --- |
| DNFR-39 | The system deployment must be compliant with {Org}’s Project Implementation Process, Production Change Management Process, and systems management process and tools. | The {Soltn} solution intends to comply with all applicable {Org} process and tooling standards. |
| DNFR-40 | The system should allow changes to be packaged in a manner that allows for scheduled automated distribution & implementation to the target environment e.g. distribution into the UAT or Production environments. | All solution technical platforms will utilise {Org}’s Azure DevOps tenant for source control, automated unit testing, code quality checks and automated build and packaging.  All solution public cloud platforms (Salesforce, ArcGIS Online, Apigee service proxies and Azure Cloud Services will utilise Azure DevOps Release Pipelines for deployment and deployment verification testing. |
| DNFR-41 | Changes to components must be version controlled, including web services. | All solution technical platforms will utilise {Org}’s Azure DevOps tenant for source control. |
| DNFR-42 | Changes to the system must be able to be rolled back as required. | Supported by all solution technical platforms. Appropriate system and data backups will be performed to support rollback for major releases. |
| DNFR-43 | Changes to the system must be audited to show what component was changed from and to what version, who enabled the execution of the change, when it was started and completed, and whether the change applied successfully or not. | All system deployment and configuration activity is logged by the solution (refer section 7.2.3.2 Audit Event Map). |
| DNFR-44 | Changes must be executed at a specified date / time. This is particularly important for configuration changes for example product rules that will be time bound. | Solution deployments will be planned and able to be scheduled for specific maintenance windows. |
| DNFR-45 | Unsuccessful deployments should generate an alert with reason code and text. | DevOps release pipelines will generate appropriate alerts (refer section 7.2.2 Operational Monitoring). |

### [Standards](#_Toc428542036)

Adherence to applicable {Org}, government and industry standards.

| Ref | Description | Solution Traceability |
| --- | --- | --- |
| DNFR-46 | The data architecture must conform to the {Org} Data and Information Architecture Standards, vocabularies and taxonomies, and consume these from the {Org} Master Data Management solution as required. No independent governance of vocabularies and taxonomies will be allowed with the proposed solution. | The solution data architecture will align with and support available {Org} data and information management standards. Currently identified standards are:   * Esri design guidelines: [System Design Strategies Wiki page](https://aus01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.wiki.gis.com%2Fwiki%2Findex.php%2FSystem_Design_Strategies&data=04%7C01%7Ccarlw%40datacom.co.nz%7C4a55663c87904d4a815d08d9603cc381%7C866c7a4c8a594bd3ad9f8512a581efc0%7C0%7C0%7C637646636992395713%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=nGFDnZbmq%2FXNQ7GjR%2FXcrnmuNFvZ0vnLRaITMvHJdL4%3D&reserved=0) * Implementations guidelines: [Architecting the Esri System](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.esri.com%2Fcontent%2Fdam%2Fesrisites%2Fen-us%2Fmedia%2Ftechnical-papers%2Farchitecting-the-arcgis-system.pdf&data=04%7C01%7Ccarlw%40datacom.co.nz%7C4a55663c87904d4a815d08d9603cc381%7C866c7a4c8a594bd3ad9f8512a581efc0%7C0%7C0%7C637646636992405666%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=UtoXT74QTdNTEPTiNF8HwR1efpldyNH5Kpc370Cfheg%3D&reserved=0) |
| DNFR-47 | The ability to comply with a common set of messaging and integration standards. | Refer to Appendix B: Applicable Standards. |
| DNFR-48 | The ability for the {Soltn} {Soltn} solution to align with government ICT standards. | Refer to Appendix B: Applicable Standards. |
| DNFR-49 | The ability for the {Soltn} {Soltn} solution to align with government web standards. | Refer to Appendix B: Applicable Standards. |
| DNFR-50 | The ability for the {Soltn} {Soltn} solution to align with applicable legislation. | Refer to Appendix B: Applicable Standards. |