DRAFT - ICT Project Guidance

Definition:  
Default System Functional Requirements

Version:

0.1

Author:

Sky Sigal, Solution Architect

## Purpose

This document catalogues functional requirements common to systems, irrespective of the system’s business purpose.

## Synopsis

All systems are constrained by legislation to provide all users specific functionality. In addition, all systems are expected to provide well-known functionality to support the tasks of default roles, such as customer support specialists, operations specialists and maintenance specialists and others.

## Contents

[Description 1](#_Toc154927865)

[Synopsis 1](#_Toc154927866)

[Contents 2](#_Toc154927867)

[Purpose 3](#_Toc154927868)

[Background 3](#_Toc154927869)

[Outcomes [Objectives] 3](#_Toc154927870)

[Options [Considered & Selected] 3](#_Toc154927871)

[Constraints 3](#_Toc154927872)

[Assumptions 3](#_Toc154927873)

[Dependencies 3](#_Toc154927874)

[Decisions 3](#_Toc154927875)

[Deliverables/Outputs 3](#_Toc154927876)

[Heading Level 3 3](#_Toc154927877)

[Heading Level 4 4](#_Toc154927878)

[Appendices 5](#_Toc154927879)

[Appendix A - Document Information 5](#_Toc154927880)

[Versions 5](#_Toc154927881)

[Images 5](#_Toc154927882)

[Tables 5](#_Toc154927883)

[References 5](#_Toc154927884)

[Review Distribution 5](#_Toc154927885)

[Audience 5](#_Toc154927886)

[Structure 5](#_Toc154927887)

[Diagrams 6](#_Toc154927888)

[Terms 6](#_Toc154927889)

## Background

…

# Roles

The following Sub Permissions are used in the role matrix that follows.

|  |  |
| --- | --- |
| Title | Description |
| **D**elete | Logically Delete an existing record or resource. |
| e**X**ecute | Execute workflows on record or resource, changing state and/or properties. |
| **E**dit | Edit an existing record or resource |
| **A**dd | Add a new individual record or resource. |
| **S**tate | Change State of Record (Approve) |
| **C**omment | Comment on an individual record or resource. |
| **R**ead | View the individual record or resource. |
| **B**rowse | List item *summaries*, potentially with confidential information summarised |
| **L**ist | List items titles, with confidential information removed. |

The above logical permissions have a logical progression of: D>E>A>S>C>R>B>L.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | All  Users | Daemon | Public (Anon) Users | Authenticated Users | Service Module Consumers | Service Providers | Support Specialists | System Operations | System Monitoring | System Maintainers |  |
| Diagnostic Tracing | A |  |  |  |  |  |  |  |  | R |  |
| Error Recording | A |  |  |  |  |  |  |  |  | R |  |
| System Configuration |  |  |  |  |  |  |  |  |  | E |  |
| System Settings |  |  |  |  |  |  |  | E |  |  |  |
| Culture/Lang Choice | E |  |  |  |  |  |  |  |  |  |  |
| Tracking Choice | E |  |  |  |  |  |  |  |  |  |  |
| Session | A |  |  |  |  |  |  |  | R |  |  |
| Session Operations | A |  |  |  |  |  |  |  |  |  |  |
| System Permission |  |  |  |  |  |  |  | R |  |  |  |
| System Users | **A** |  |  |  |  |  |  |  |  |  |  |
| System Notifications | A |  |  |  |  |  |  |  |  |  |  |
| User Groups |  |  |  |  |  | D |  | D |  |  |  |
| Permissions to Roles |  |  |  |  |  |  |  | D |  |  |  |
| Role Applying |  |  |  | A |  |  |  |  |  |  |  |
| Application Accepting |  |  |  | A |  |  |  |  |  |  |  |
| Invitations Issuing |  | X |  | A |  |  |  |  |  |  |  |
| Invitation Accepting |  |  |  | A |  |  |  |  |  |  |  |

# Business Rules

Traction corrections, adjustments, cancellations

Administrative functions

Authentication

Authorisation Levels

Audit Tracking

External Interfaces

Certification Requirements

Reporting Requirements

Historical Data

### Flows

Functional Requirements can describe flows.

When a User selects X, then Y is done.

On the login view, when a User submits a correct username and password

On the Header, a User can navigate to their User Profile information.

On their

Features

Capabilities

# Capability Requirements

The following requirements are organised by capability.

## Configuration

While often used interchangeably, Configuration is distinct from System Settings in that in this case it is specific to integrating components, is deployed with the system, and cannot be changed without restarting or even redeploying the system.

##### FR-USER-ID: **Configuration**

|  |  |
| --- | --- |
| **Category** | Functional/Capabilities/System |
| **Statement** | **IF** **SaaPs THEN**  the solution system(s) **MUST** permit system maintainers and/or system deployers specialists to modify infrastructure configuration settings without redeployment. |
| **Rationale** | While not optimal, there are conditions where a configuration change must be individually deployed as opposed to deploying configuration changes via automated deployments. |
| **Details** | (immutable) Capabilities, which define how a system is integrated, are distinct from (mutable) System Settings, which define how a system operates.  **Important:** Quality requirements have outlined that confidential configuration settings (e.g., 3rd party service credentials) must be encrypted. |
| **Prompts** | … |

## Analysability

### Diagnostics

Diagnostics tracing are distinct from error logging. The tracing level used is configurable at deployment.

##### FR-USER-ID: **Diagnostic Trace Management**

|  |  |
| --- | --- |
| **Category** | Functional/Capabilities/System |
| **Statement** | **IF** **SaaP**s **THEN**  the solution system(s) **MUST** permit system maintainers  to query and view diagnostics logging entries. |
| **Rationale** | Permits maintenance specialists to diagnose sequences of events that led up to an exception occurring. |
| **Details** | Diagnostic records:   * Must be cleansed of confidential information. * Must be read only. * Must be thin/light. * Must include UTC date/time, and Session and User identifiers (no other attributes). * Must include the thread Id. * Must be temporary, rolling, individual records deleted after a configurable duration (e.g.: 31 days). * Must be remotely accessible (e.g. via APIs) via a system distinct from the business service itself. * Should be non-tamperable. Consider cryptographic signing. * May be queryable via the system itself (e.g.: via its UI) |
| **Prompts** | What of the above details list can not be delivered? |

### Error Recording

Error Records contribute to the Analysability of a system, but are maintained longer than Diagnostic Trace records, for measuring current system health (errors/time) and quality improvements (change in errors/time).

##### FR-USER-ID: **Error Record Management**

|  |  |
| --- | --- |
| **Category** | Functional/Capabilities/System |
| **Statement** | **IF** **SaaP**s **THEN**  the solution system(s) **MUST** permit **system maintainers** and **system operators** to browse and view curated error report records. |
| **Rationale** | Permits maintenance specialists, and maybe operations specialists and/or customer support specialists to view records of errors. |
| **Details** | Error Records:   * Must be cleansed of confidential information. * Must be read only. * Must be thin/light. * Must include UTC date/time, and Session and User identifiers (no other attributes). * Must be persisted permanently. * Accessible remotely (e.g. APIs) via a system distinct from the business service, that provides functionality. * May be accessed from within the service itself (via UI). * Should be non-tamperable. |
| **Prompts** | What of the above details list can not be delivered? |

## Monitoring and Auditability

## Session & Session Operation Management

Sessions are used to provide users individual experiences accessing stateless services, while contributing to auditability qualities of a system.

##### FR-USER-ID: **Session Management**

|  |  |
| --- | --- |
| **Category** | Functional/Capabilities/System |
| **Statement** | **IF** **SaaPs**, **THEN** the solution system(s) **MUST** permit system monitors to investigate active Sessions. |
| **Rationale** | System Monitors must be able to investigate irregular behaviour by browsing and viewing active Sessions, and from there investigate a Sessions Operations. |
| **Details** | Existing Session tokens are regularly updated. Check the User’s status first.  Session records:   * Are Immutable * Are Untamperable * Record the UTC date and time of the start of the session * Persist the user identifier (no user information) * Do not persist the variable IP of the session client. |
| **Prompts** | … |

##### FR-USER-ID: **Session Operation Management**

|  |  |
| --- | --- |
| **Category** | Functional/Capabilities/System |
| **Statement** | If a **SaaP**, the solution’s system(s) **MUST** permit system monitors to investigate active Session’s Operations. |
| **Rationale** | System Monitorers MUST be able to investigate irregular behaviour by browsing and viewing active Session Operations by specific types,to in turn identify Sessions and Users. |
| **Details** | Existing Session tokens are regularly updated. Check the User’s status first.  Session records are:   * Immutable * Untamperable * Record the UTC date and time of the operation start * Record the UTC date and time of the operation end,   + This permits reporting on operation durations. * Persist the session identifier (no session information) * Persist the variable IP of the session client. * Persists the identifier of the record of the first error raised if any. * Persists the user’s culture/language. * Persists the URL fragment (operation, plus arguments provided) * Persists the request payload (if PUT, POST). * Persists the operation summary result code (success, failure, etc.) |
| **Prompts** | … |

## Basic Accessibility and Privacy Management

All users, whether authenticated or not require the ability to making the system accessible to them while defining what privacy they are comfortable providing.

##### FR-USER-ID: **Culture/Language**

|  |  |
| --- | --- |
| **Category** | Functional/Capabilities/System |
| **Statement** | All Users MUST be able to set their Profile’s Session’s Culture/Language. |
| **Rationale** | To understand the system’s output. |
| **Details** | The choice is saved as a persistent cookie so as be usable by non-authenticated users, coordinated with the value in the user’s system preferences profile when they authenticate themselves to the system.  **Important:** The cookie is classified as “essential”[[1]](#footnote-2) therefore does not trigger the need to provide users an option to not persist it. |
| **Prompts** | … |

##### FR-USER-ID: **Tracking Options**

|  |  |
| --- | --- |
| **Category** | Functional/Public Users |
| **Statement** | All Users MUST be able to configure which cookies are persisted and how. |
| **Rationale** | It is legally required in many jurisdictions that users MUST be able to define what non-strictly necessary cookies are persisted, and how. |
| **Details** | The choice is persisted as a cookie as well as coordinated with the user’s system settings profile (if they authenticated). |
| **Prompts** | … |

## User Management

##### FR-XXX-ID: **User Creation**

|  |  |
| --- | --- |
| **Category** | Functional/R… |
| **Statement** | The system MUST be capable of creating Users Just In Time (JIT) when they are invited to a **role** within the **system**. |
| **Rationale** | Creating User accounts before they are actually used is a security risk. |
| **Details** | See Role Functionality |
| **Prompts** | … |

##### FR-XXX-ID: **User Disablement**

|  |  |
| --- | --- |
| **Category** | Functional/R… |
| **Statement** | **Permitted users**, such as monitoring specialists, MUST be capable of disabling a User now or at a future date and time. |
| **Rationale** | A security monitoring specialist may wish to terminate a user associated to unusual session activity. |
| **Details** | Disabling a User would disable both all following Operations and/or the creation of new Sessions. |
| **Prompts** | … |

## User Self Management

Users manage their own settings.

##### FR-USER-ID: **User Tracking Preferences**

|  |  |
| --- | --- |
| **Category** | Functional/User/Preferences |
| **Statement** | All Users MUST be able to configure which cookies are persisted and how. |
| **Rationale** | It is legally required in many jurisdictions that users MUST be able to define what non-strictly necessary cookies are persisted, and how. |
| **Details** | The choice is persisted as a cookie as well as coordinated with the user’s system settings profile (if they authenticated). |
| **Prompts** | … |

##### FR-XXX-ID: **User Settings**

|  |  |
| --- | --- |
| **Category** | Functional/R… |
| **Statement** | **Authenticated Users MUST be enabled to edit their digital profile within the system.** |
| **Rationale** | A user |
| **Details** | A digital profile may contain: - Usability: interaction culture/language - Accessibility: font size |
| **Prompts** | … |

##### FR-XXX-ID: **User Profile**

|  |  |
| --- | --- |
| **Category** | Functional/R… |
| **Statement** | **Authenticated Users MUST be able to manage their [System Preferences] Profile.** |
| **Rationale** | A user |
| **Details** | A system preferences profile may contain the following setting categories:   * Identity: their display name, display role, a description, a bio, an avatar, sex, gender * Channels: phone, email, social (X, etc.), postal * Usability: interaction culture/language, notification type subscriptions, etc. * Accessibility: font size   **Note:** In very current systems a Person may have more than one Identity. |
| **Prompts** | … |

##### R-XXX-ID: **User Security Profile**

|  |  |
| --- | --- |
| **Category** | Functional/R… |
| **Statement** | **Authenticated Users MUST be able to view their Security Profile.** |
| **Rationale** | Support service specialists or a user themselves may wish to investigate and better understand why they can’t do an operation. |
| **Details** | A users security profile would permit listing the roles they have, potentially listing the permissions under each role. A user would not be able to add themselves to a role (see *Invitations*).  A user would be able to drop a role.  A user would not be able to edit any role, relationship to permissions, or the permission themselves. |
| **Prompts** | … |

##### FR-XXX-ID: **Principal Management**

|  |  |
| --- | --- |
| **Category** | Functional/R… |
| **Statement** | **Permitted users**, such as business support specialists setting up business service consumers, MUST be capable of listing requirements and the roles they are associated to. |
| **Rationale** | Permitted users may required reviewing which roles, and therefore which users, have a permission. |
| **Details** | … |
| **Prompts** | … |

##### FR-XXX-ID: **Role Management**

|  |  |
| --- | --- |
| **Category** | Functional/R… |
| **Statement** | **Permitted users**, such as system operation specialists setting up the service for multiple tenants, MUST be capable of listing current Roles, adding new or editing existing Roles, adding or removing other Roles and/or Permissions to them. |
| **Rationale** |  |
| **Details** | Roles should be nestable.  Permitting developing small variations of Roles quicker (e.g.: Head Accountant, Accountant, Junior Accountant).  Permitted users may develop Roles from other Roles, adding or removing a specific Permission. |
| **Prompts** | … |

##### FR-XXX-ID: **Title**

|  |  |
| --- | --- |
| **Category** | Functional/R… |
| **Statement** | A user MUST be able to view and manage the digital identities used to identify themselves to the system. |
| **Rationale** | A user may be able to sign in via one or more external IdP identities (public cloud identities, and/or work corporate identity). |
| **Details** | It is conventional that upon first sign-in, the User’s **display name** is developed from attributes within their external digital identity.  A user may disable all but the digital identity used to sign in (to remove the option of being locked out). |
| **Prompts** | … |

## Invitation Management

## All Users

##### FR-USER-ID: **Tracking Preferences**

|  |  |
| --- | --- |
| **Category** | Functional/Public Users |
| **Statement** | Public (Non-Authenticated) Users MUST be able to configure and retain their data tracking preferences. |
| **Rationale** | Users must not be required to sign in to persist settings regarding their tracking preferences. |
| **Details** | The traditional technical solution is to persist the setting as a Session or [long-duration, expiring] Persistent cookie.  The cookie value is persisted in the user’s system profile when they sign in. |
| **Prompts** | … |

##### R-XXX-ID: **System Wide Notifications**

|  |  |
| --- | --- |
| **Category** | Functional/Public Users |
| **Statement** | Users MUST be able to view system wide notifications. |
| **Rationale** | … |
| **Details** | The most common form of system wide messaging is as a “banner” message.  A common use of system-wide notifications is to notify users about an upcoming planned system downtime to upgrade the system.  A Notification should be displayable until turned off, indicating that the user has read the banner notification.  A method of persisting information as to whether the display has been seen or not is to persist as a cookie the incrementing number of the message.  The cookie value is persisted in the user’s system profile when they sign in. |
| **Prompts** | … |

##### FR-XXX-ID: **Role Application**

|  |  |
| --- | --- |
| **Category** | Functional/R… |
| **Statement** | A Authenticated User MUST be able to Apply for a Role within a Group or Resource. |
| **Rationale** | A User can apply to be Invited to a Role within a Group or Resource they are made aware of. |
| **Details** | An application notification is sent to the Group or Resource entity’s manager.  If denied, a notification is sent back to the Invitee’s email address.  If accepted, an invitation is created on behalf of the Inviting User.  **Important:** If invitations are permitted to be made by a non-authenticated user, the user’s email address is required to be entered. |
| **Prompts** | … |

## Non-Authenticated Users

All public users who visit publicly accessible pages develop a session, but remain non-authenticated until they sign in.

##### FR-XXX-ID: **Role Invitation Acceptance**

|  |  |
| --- | --- |
| **Category** | Functional/Unauthenticated User |
| **Statement** | Users can **accept** or **decline** an email based **invitation** to a **role.** |
| **Rationale** | A person, whether already a user or not, may accept the responsibilities associated to a role. |
| **Details** | The email has two Actions within it. Each Action is linked to a callback on the service.  If the invitation is declined, the system closes the invitation record.  If the invitation is accepted, the system proceeds with linking the [by then] authenticated user with the role specified in the invitation. |
| **Prompts** | … |

##### FR-XXX-ID: **Sign In**

|  |  |
| --- | --- |
| **Category** | Functional/Public Users |
| **Statement** | Non-Authenticated Users MUST be able to authenticate themselves to the system. |
| **Rationale** | … |
| **Details** | The system’s publicly accessible Home Page MUST provide functionality to sign in.  The view should provide multiple options to sign in.  The preferred option is via a 3rd party IdP broker service.  Note: young users may not be able to legally use a commercial IdP, in which case persisting username and password credentials in system is a reasonable position if done securely. |
| **Prompts** | … |

## Authenticated Users

##### FR-XXX-ID: **Sign out**

|  |  |
| --- | --- |
| **Category** | Functional/Authenticated User |
| **Statement** | An Authenticated User MUST be able to sign out and close their current session. |
| **Rationale** | … |
| **Details** | … |
| **Prompts** | … |

##### R-USER-ID: **Personal Settings**

|  |  |
| --- | --- |
| **Category** | Functional/Authenticated Users |
| **Statement** | Authenticated Users MUST be able to persist personal system preferences. |
| **Rationale** | Efficiency is improved when a User can view and customise their interactions with a system. |
| **Details** | The default technical method is for each System User record has an associated System User Settings Profile entity.  Common settings saved in a User System Settings Profile include:   * Presentation choices:   + Culture/Language   + Presentation Style choice * Accessibility choices:   + Overriding/supplementing default presentation type settings, may include font-size, colour schemes, etc. * Personal Choices:   + Display Name   + Display Default Role * Etc. |
| **Prompts** | … |

##### FR-USER-ID: **Digital Identities**

Each User has a digital identity. The digital identity can be a managed authenticated by a 3rd party identity but can also be managed and authenticated in-system (not everybody will accept to use a 3rd party IdP’s identity to gain access to the system).

A User requires functionality to sign in and out.

A User benefits from seeing which digital identities have been associate to his system record. Optionally, they can disable digital identities they are no longer using (that are not the digital identity they are currently using).

|  |  |
| --- | --- |
| **Category** | Functional/R… |
| **Statement** | Authenticated Users MUST be associated to one or more digital identities. |
| **Rationale** | Digital identities are 3rd party identities which are trusted. |
| **Details** | Traditionally, a User Record would have one or more Digital Identity records. |
| **Prompts** | … |

##### FR-XXX-ID: **Terms & Conditions**

|  |  |
| --- | --- |
| **Category** | Functional/R… |
| **Statement** | An authenticated user MUST be able to accept abiding to a version of a Terms & Conditions statement. |
| **Rationale** | Changes to agreements must be reaccepted or rejected. |
| **Details** | Over a service lifespan it is common for Terms & Condition statements to be updated several times.  The different versions of the statements are required to be kept, and the latest change re-accepted. |
| **Prompts** | … |

### Notifications

Notifications are in-system messages raised by the system upon certain events happening for viewing by target users.

Notifications can be shown for a set duration (e.g.: 30 seconds) or remain available until a person has read them.

Some notifications require being sent when a User is not using the system. In which case they are sent as emails or SMS notifications.

## Permitted Users

Permitted Users are Users who have a specific Permission.

##### FR-XXX-ID: **Application Acceptance**

|  |  |
| --- | --- |
| **Category** | Functional/Permitted User |
| **Statement** | A permitted recipient of an invitation MAY accept a user’s application to a **role**. |
| **Rationale** | A resource creator must be able to accept or decline an application from a specific user to a specific role related to a specific group or resource. |
| **Details** | … |
| **Prompts** | … |

## Service Provider

Service Resource Developer

## Customer Support

## System Operator

##### FR-XXX-ID: **System Settings**

|  |  |
| --- | --- |
| **Category** | Functional/System Operators |
| **Statement** | A System Operator MUST have available functionality to manage system wide settings. |
| **Rationale** | … |
| **Details** | Default settings might include: - Sponsor Organisation Name & Logo  - Product Name and Description - Default Appearance Styling  - etc. |
| **Prompts** | … |

##### FR-XXX-ID: **Anonymous User Invitations**

|  |  |
| --- | --- |
| **Category** | Functional/System Operator |
| **Statement** | A permitted User MUST be able to configure whether anonymous users can apply for an invitation to a role. |
| **Rationale** | … |
| **Details** | **Anonymous users**, because they do not yet have a **user** record, with an associated email address, are required to submit their email address when applying for an invitation to a role.  There is the option (risk?) that a user submits someone else’s email address as opposed to their own. |
| **Prompts** | … |

##### FR-XXX-ID: **Terms & Condition Management**

|  |  |
| --- | --- |
| **Category** | Functional/R… |
| **Statement** | A permitted user MUST be able to create or upload a new version of a Terms & Conditions statement. |
| **Rationale** | Changes to agreements must be reaccepted or rejected. |
| **Details** | Over a service lifespan it is common for Terms & Condition statements to be updated several times.  The different versions of the statements are required to be kept, and the latest change re-accepted. |
| **Prompts** | … |

## System Monitor

...

## System Maintainer

##### FR-XXX-ID: **Diagnostics Trace Maintenance**

|  |  |
| --- | --- |
| **Category** | Functional/R… |
| **Statement** | System Maintainers MUST be able to view the queryable solution system(s) diagnostic log files. |
| **Rationale** | System Maintainers require being able to diagnose systems to determine what happened. |
| **Details** | Diagnostic logs must always be cleansed of confidential data prior to entries being written.  While beneficial, it is not always practical to develop a means to view diagnostic trace messages within a system. Secondary tools can be used. |
| **Prompts** | … |

##### FR-XXX-ID: **Title**

|  |  |
| --- | --- |
| **Category** | Functional/R… |
| **Statement** | A permitted user MUST be able to view a queryable source of Error reports. |
| **Rationale** | … |
| **Details** | A |
| **Prompts** | … |

Appendices

Appendix A - Document Information

### Versions

* 1. Initial Draft

### Images

[Figure 1: TODO Image 2](#_Toc144995112)

### Tables

[Table 1: TODO Table 3](#_Toc145048484)

[Table 2: TODO Table 2 3](#_Toc145048485)

### References

**There are no sources in the current document.**

### Review Distribution

The document was distributed for review as below:

|  |  |
| --- | --- |
| Identity | Notes |
|  |  |
|  |  |
|  |  |

### Audience

The document is technical in nature, but parts are expected to be read and/or validated by a non-technical audience.

### Structure

Where possible, the document structure is guided by either ISO-\* standards or best practice.

### Diagrams

Diagrams are developed for a wide audience. Unless specifically for a technical audience, where the use of industry standard diagram types (ArchiMate, UML, C4), is appropriate, diagrams are developed as simple “box & line” monochrome diagrams.

### Terms

Refer to the project’s Glossary.

##### IT

: acronym for Information, using Technology to automate and facilitate its management.

##### ICT

: acronym for Information & Communication Technology, the domain of defining Information elements and using technology to automate their communication between entities. IT is a subset of ICT.

Appendix B – FAQ

Appendix C – Requirement Record Template

Following guidance within *ITC Project Guidance – Definition – Requirements Development* the schema template for Requirements in this document is as shown below.

##### FR-XXX-ID: **Title**

|  |  |
| --- | --- |
| **Category** | Functional/R… |
| **Statement** | [**IF**](#Term_IF) … [**THEN**](#Term_THEN) … **ELSE** … |
| **Rationale** | … |
| **Details** | … |
| **Prompts** | … |

1. Common categories are: “performance”, “functionality [preferences]”, ”[advertisement] targeting”, “social media”, ”unclassified” [↑](#footnote-ref-2)