F

ICT Project Guidance

Common System Capabilities (HL)

Author:

Sky Sigal, Solution Architect

## Description

This document outlines standard functionality expected of ICT systems, describing the value the can offer, to better inform procurement and design decisions.

## Synopsis

Irrespective of the business reason for an ICT system, mature systems share a relatively standard set of Capabilities.

## Contents

[Description 1](#_Toc147310987)

[Synopsis 1](#_Toc147310988)

[Contents 2](#_Toc147310989)

[Introduction 3](#_Toc147310990)

[Objective 3](#_Toc147310991)

[Issue 3](#_Toc147310992)

[Resolution 3](#_Toc147310993)

[Services 4](#_Toc147310994)

[Diagnostic Trace Logging 4](#_Toc147310995)

[Error Logging 4](#_Toc147310996)

[Configuration Management 5](#_Toc147310997)

[Settings Management 5](#_Toc147310998)

[Session Management 5](#_Toc147310999)

[Sessions Management 5](#_Toc147311000)

[System Operation Management 6](#_Toc147311001)

[User Preferences and Security Profiles 6](#_Toc147311002)

[User [System Preferences] Profiles 6](#_Toc147311003)

[User Security Profile 6](#_Toc147311004)

[User Grouping and Management 7](#_Toc147311005)

[System User Groups 7](#_Toc147311006)

[Group Roles 7](#_Toc147311007)

[Group Role Applications, Invitations and Acceptances and Reminders 7](#_Toc147311008)

[Monitoring 8](#_Toc147311009)

[Report Management 8](#_Toc147311010)

[Appendices 10](#_Toc147311011)

[Appendix A - Document Information 10](#_Toc147311012)

[Images 10](#_Toc147311013)

[Tables 10](#_Toc147311014)

[References 10](#_Toc147311015)

[Review Distribution 10](#_Toc147311016)

[Audience 10](#_Toc147311017)

[Structure 10](#_Toc147311018)

[Diagrams 10](#_Toc147311019)

[Terms 10](#_Toc147311020)

## Introduction

Most ICT systems fail. The reasons are many, but key is the lack of understanding of what capacities to require of a system, as it in turn leads to mistakes in procurement or custom design.

### Objective

The objective is to procure or develop services that are assets rather than liabilities that improve their value over time by improving defined qualities[[1]](#footnote-2).

### Issue

A majority of ICT services do not meet these expectations.

### Resolution

To resolve this omission, it is important to have available a checklist of common capabilities expected of most systems to better inform the development of requirements used to guide procurement and/or development of ICT services.

# Services

The list of default services that a service is expected to deliver includes the following:

#### Diagnostic Trace Logging

Services are expected to output running logs of execution so that Maintenance Specialists can analyse them to diagnose unexpected behaviour.

The log files are expected to have the following characteristics:

* + - * The output is expected to be cleansed of Personal Information, so that they are not a source of personal confidential data leakage.
      * Whereas log files used to be to local files, dynamic allocation of cloud resources makes this impractical. Current best practice is to output to cloud service.
      * Diagnostic tracing can take considerable space. It is expected that diagnostics tracing be temporary, such that records older than 31 days are physically.
      * It is preferable that data can be filtered, sorted, paged and viewed remotely, in an audited environment (such as is offered by default by cloud service providers) , to facilitate diagnosing issues, but also to ensure the data is not downloaded to an unaudited environment.

#### Error Logging

Services are expected to keep records of Unexpected Behiavour that occurred.

* + - * For a similar reason to that given regarding Diagnostic Tracing, error records must be cleared of Personally Identifieable information.
      * Error logs are to be persisted permanently, so that they can be used as the basis for monitoring and decreasing the rate of error reporting, over time.
      * It is preferable that data can be filtered, sorted, paged and viewed remotely, in an audited environment (such as is offered by default by cloud service providers) , to facilitate diagnosing issues, but also to ensure the data is not downloaded to an unaudited environment.

#### Configuration Management

Services are expected to be configurable to fit the constraints of different deployment environments and available dependency services.

Configuration is a post-deployment exercise.

* + - * Configuration is expected to be done by remote editing of text files.

#### Settings Management

The difference between Configuration and Settings is Configuration is a post-deployment/ pre-run task, whereas Configuration is done after deployment, when running.

In other words, Configuration changes generally lead to a restart of an application, whereas Settings changes can be applied without restarting the system.

Best practice is that Settings is done in a repeatable automated manner – usually as a last step of an automated deployment process.

* + - * Settings should be applicable via APIs, post deployment – probably as a last step of the deployment process.
      * Settings should also be able to be done via User interfaces, if need be.
      * Settings would be expected in the following areas:
        + System Dependencies (URL, credentials to remote dependency services, operation settings)
        + Appearance (Logo, Title, Subtitle, Backgrounds, etc.)

### Session Management

Each User who opens a browser and invokes the service starts a new (or continues an existing) Session, during which they perform multiple Operations.

#### Sessions Management

System terminate Sessions after a configurable while, generally between 8 hours and 1 month. Whereas it used to be considered best practice to terminate sessions quicker, current best practice is to keep sessions going as long as possible.

Legacy systems used to associate Sessions to Client IPs but this practice is deprecated recognising that the IPs of mobile clients change often as they travel, making for a poor user experience. IPs are now tracked in System Operations.

#### System Operation Management

During a single Session a User may perform many different Operations. Permanently recording these operations is the basis of non-deniabile auditability.

* + - * Session Operations are expected to be recorded permanently.
      * Auditing of Operations should record all operations that cahgne state (ie all Create and Update and Delete operations).
      * In the past, when storage space was more of a constraint, it was common practice to audit only Operations that change State. It is now considered best practice to audit both Browse/List and record Viewing Operations, to better understand who has accessed and seen information.

### User Preferences and Security Profiles

Maturely designed systems provide each user a means for users to optimise the efficiency of their interactions with the system and save their personal settings and provide a flexible way of assigning permissions and roles to a person.

#### User [System Preferences] Profiles

Rather than having to reconfigure a system each time they start a new Session, System Users should have a means to persist personal Preferences. This is commonly referred to as their User Profile or User System Preferences.

User profiles:

* + - * for Usability reasons, should record their preferred system Identity information such as their preferred Display Name, Avatar image, Role description, preferred communication Channels (e.g. email address and/or cell phone number), and maybe even a mini bio,
      * for Accessibility quality reasons, should including their Culture and Language preferences, display preferences (backgrounds, colour schemes, font sizes, etc.) that may address visual impairment issues, etc.
      * for Performance quality reasons, should be developed separately from the User object, to enable independent caching if desired.

#### User Security Profile

Related, but kept separate from both the User and their associated User [system] Profile, a User should have a User Security Profile. This is their personal collection of assigned Group and Resource Roles and associated Permissions.

* + For Usability quality reasons, a User should be assignable one or more Roles, which are just named groups of Permissions and their associated Responsibilities if any.
  + For flexibility quality reasons, it should be possible to add or remove specific Permission on top of the Permissions assigned with a default Role. An example might be to provide two persons with the same Accounting Role, but removing from one of them the ability to sign cheques that are over $5000.

### User Grouping and Management

#### System User Groups

Users work together in Groups to communicate, collaborate in the development and management of Resources.

* + For flexibility quality reasons, Groups should be nestable to be capable of mapping of most organisation groups and (e.g., departments, classrooms, etc.)
  + To improve usability, Users must be able to be assigned RASCI inspired Roles within the group, rather than all being Members of the Group.
  + User Grouping, and associated User Group Role assignment,

#### Group Roles

Associated with User Groups are Roles specific to the Group Type.

* To improve the system’s usability quality, default Group Roles will probably mirror RASCI expectations.
* To improve the system’s recognisability quality, the role display name should be configurable to match users needs (e.g., “Department”, “Classroom”, etc.)

#### Group Role Applications, Invitations and Acceptances and Reminders

It is preferable that systems permit Roles within groups are Applied for, Invited to and Accepted, rather than unilaterally Assigned by a Group member with the appropriate Permissions to do so.

* For usability reasons, the system of invitations, acceptance or rejection should be automated.
* For security reasons, either only Permitted users should be permitted to invite other users, or Users can only invite users to equal or lower roles.  
  For example, Managers can invite Users to become Members, Members can invite other Users to become Members, but cannot invite them to become Managers of the Group.
* For security reasons, Invitations to Roles should not be open ended, and expire after a configurable time.
* For security reasons, Roles should not be open ended, and a reminder sent out to a Group manager a configurable amount of time before the role expires, so that they can decide what to do (extend the contract, or let it expire beforehand).
* For flexibility reasons Roles can be assigned to start in the future (e.g., aligning with an employment start date, or future school term sart).
* For security reasons, Permitted Users should be able to terminate a Role by moving forward the termination date.

Monitoring and Reporting

A key aspect of knowing whether a service is secure and fit for purpose is monitoring, alerting and reporting.

#### Monitoring

Monitoring is required for multiple purposes. Continual monitoring is required to develop a understanding of what is normal system and user behaviour. This in turn permits defining what to consider as abnormal system and user behaviour, and alert Maintenance Specialists to such conditions.

#### Report Management

It is a delivery error to push back reporting to the end: reports are arguably more important than user interfaces because they are often used to communicate with sponsors and governance stakeholders, who probably don’t even use the system.

* For usability reasons, it is common to integrate with 3rd party services that are specialised in reporting (e.g.: Microsoft BI) to deliver the desired reporting capabilities. Note that it is not recommended that systems develop their own integrated reporting solution, and it is not for systems to build provide the functionality to design and develop or edit the templates for new Reports.
* For security reasons, care must be used when integrating with 3rd party reporting systems: the data that is sent should not contain personal information – so is usually cleaned by replacing personal information with other text.

##### System Metric Reporting

* For maintainability reasons, reporting is required to develop reports on system characteristics: system availability, throughput and resource usage (and therefore cost) under normal and peak loads.

##### User Metric Reporting

* For funding purposes, reporting is required to report on evolving usage of the system. Hopefully the reports show that the number of users is increasing, they are accessing more information, and performing more operations per session.

Appendices

Appendix A - Document Information

### 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.

##### Term

: the meaning.

1. See ISO-25022, ISO-25012, ISO-25010 [↑](#footnote-ref-2)