isorobot Enterprise Management Software

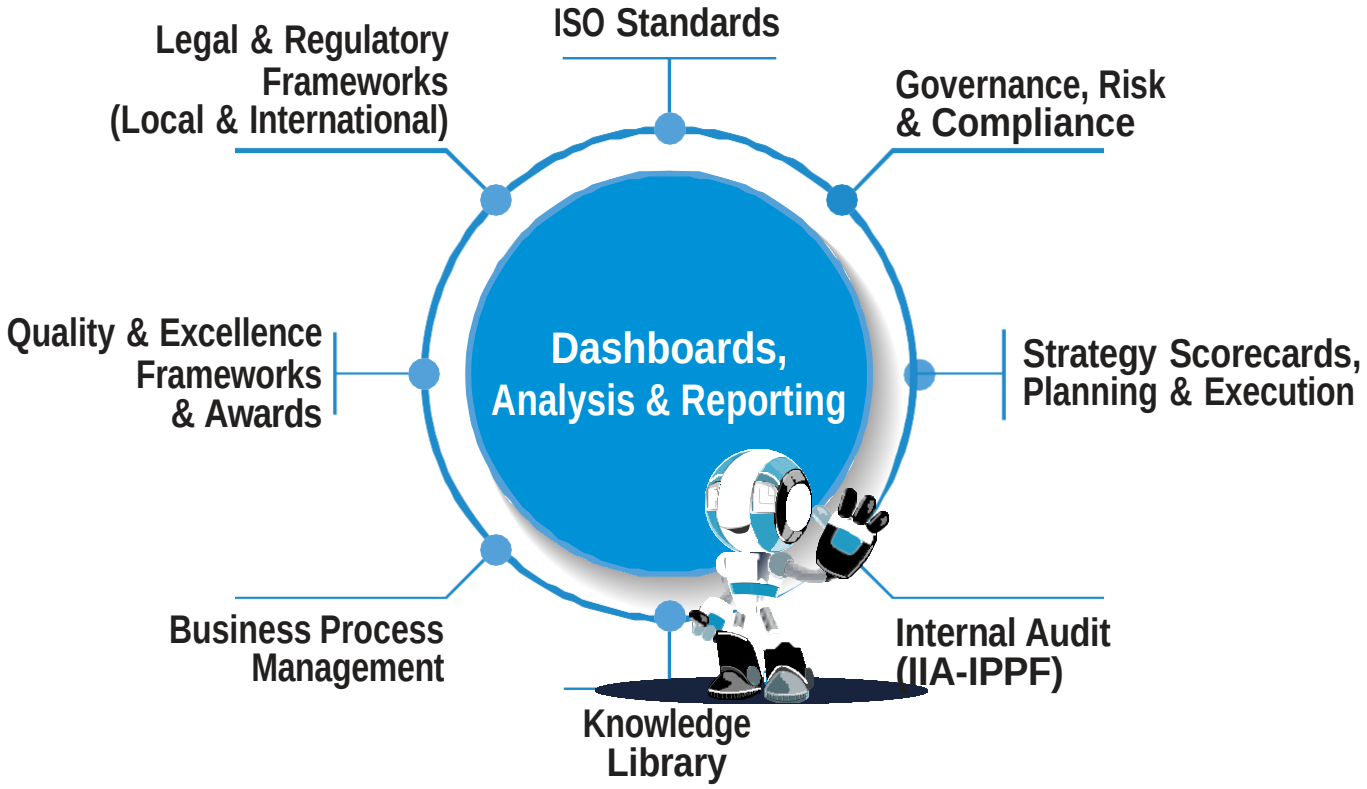
Service Definition Document

excelledia®

What is isorobot?

isorobot is a highly innovative platform which encompasses multiple ISO management systems, as well as various legal, regulatory, and business frameworks, all in a single platform.

The system helps you to define, capture, manage, maintain, integrate, monitor, measure and improve your existing business practices.



isorobot can be integrated with major ERP, CRM applications and other operational software solutions using its APIs

Key Features

- Secure, available On Cloud & On Premise
- Can hold any number of ISO Standards
- Hassle Free Document Management System
- Auto Approval Process
- Email Triggers
- Easy to integrate & customize all business Formats

- Business Impact Analysis
- Objective Setting & Business Scorecards
- Risk Management
- Preloaded Best Practices Library
- Paperless Audit Cycle & ROI Tracker
- Customer Satisfaction & Complaint Mgt.
- Standard and Enterprise Support
- Involvement of experts in development
- Information Lifecycle & Compliance Best Practices
- Integrated using ISO 30301 & ISO 19600
- Notifications Alerts Reminders Customized Dashboards

What it Can Assure?

This tool enable the organization to manage the following

System Functionality Requirements

Application is of SaaS type and it will be hosted in AWS cloud. It will fulfil all the required processes as set out in section 2 Appendix 1 as well as following the security and audit tail process and reporting.

Full technical details are provided in our separate Technical Proposal document. This includes our:

- Application Architecture Diagram
- Network Diagram
- Hardware Requirements

We can host the application on all well-known cloud providers like Amazon Cloud Services (AWS), Microsoft Azure, Google Cloud etc. and also own a private datacentre. High available and Normal implementation can be provided based upon the requirement. Our system can be configured on Unix based OS's like RHEL, CentOS, Ubuntu etc and it supports MySQL and MSSQL database.

➢ Web Interface

Our system is fully compatible with and operates on all modern web browsers including Google Chrome, Firefox, Safari Edge and Internet Explorer. For the best experience and optimum security, we always recommend using the latest stable release but would not discontinue support for any versions that you are currently using during the life of the contract.

A responsive design makes use of flexible layouts, flexible images and cascading style sheet media queries including a responsive web design for all mobile devices e.g. phones, tablets.

Our system offers an easy, consistent and intuitive interface and functionality for users and administrators.

This includes all interfaces, including where users add or access data (e.g. reports and dashboards).

Sample screen shots are shown below and also throughout our separate Technical Proposal document which we have included to ensure clarity of the screenshots:

isorobot has readily discoverable features with
simple and user-friendly navigation and function selection.

The system has a multi-window mode, allowing users to view multiple windows simultaneously. This delivers a significant boost in terms of both productivity and convenience.

It enables the user to tile all open windows side- by-side and offers a high degree of personalisation and configuration at the user interface level, without the need to change the underlying schema or source code.

Our system allows the user to configure their screens according to their individual needs and preferences and it remembers individual users' choices.

isorobot is compatible with all common operating systems and browsers, including updates and new- versions to ensure compatibility.

It does not require the installation of any special software or plug-ins on the end-users' computers.

➢ Integration

isorobot is compatible with and is proven to work with Single Sign On technologies.

We always strive to provide the very best user experience but one that is also safe and secure.

As such, our system supports authenticated logon that is integrated with the Windows security model. Single Sign On with two factor authentication will be used so that users do not need to re-key the password or use password managers or browser add-ons.

We confirm that our application will support directory integration, as outlined above.

We can integrate authentication for end-users with Microsoft Azure Active Directory.

With Azure AD, signing certificates can be used with applications that use SAML 2.0, WS- Federation, or OpenID Connect Protocols as well as Password Single Sign On.

With Microsoft Azure AD Application Proxy, we can provide access to applications located inside your private network securely from anywhere and on any device. After you have installed an application proxy connector within your environment, it can be easily configured with Azure AD.

We can also add any application that already exists in your organisation, or any third-party application from a vendor who is not already part of the Azure AD gallery.

Depending on your license agreement, the following capabilities are available:

- Self-service integration of any application that supports Security Assertion Markup Language (SAML) 2.0 identity providers (SP-initiated or IdP-initiated)
- Self-service integration of any web application that has an HTML-based sign-in page using password-based SSO
- Self-service connection of applications that use the System for Cross-Domain Identity Management (SCIM) protocol for user provisioning

Ability to add links to any application in the Office 365 app launcher or the Azure AD access panel.

a. Security and audit trail process and reporting

All our offices across the globe are ISO 27001:2013 Certified and we follow best practice in relation to ISO 22301:2019 Business Continuity Management System to ensure internal and external business continuity.

An Information Security Incident Response Plan is available as part of our well established ISMS. It is tested at regular intervals to ensure the efficiency of the processes. Our Incident Register is regularly reviewed at set intervals.

Our Information Security Policy is approved and signed by the CEO and is regularly updated as part of our internal review system. It is communicated to all relevant internal and external stakeholders.

Independent external audits are carried out once a year. Internal Audits and Management Review Meetings are carried out twice a year. We use a sophisticated digital platform (Isorobot) to ensure the effective implementation of all our compliance requirements. Internal and external audit findings and Management Review Meeting minutes are captured in Isorobot. The related ISMS policies, procedures and forms (workflows) are also available within Isorobot. Interactive dashboards, analysis and reporting provides us with real time monitoring of the information security management system.

Risk Management is practiced using the best practices of ISO 31000:2018. The Risk Management Policies, Procedures are managed using Isorobot. Our risk management workflow uses a 5x5 Risk Matrix. Our risk management process identifies all the major information assets handled by Excelledia with an asset criticality assessment. As a result of the risk management process the Statement of Applicability (SoA) is produced based on the applicable controls from the list of 114 controls as required by the ISO 27001:2013 standard.

The application will be configured with HA (high availability) to ensure zero down time with two load balanced web servers and two database servers both of which are located in the UK.

isorobot is GDPR compliant as well as compliant with the internationally recognised best practices of ISO 27001 Information Security, ISO 19600 Compliance, ISO 27014 Information Security Governance and ISO 22301 Business Continuity Management Systems. This ensures the highest possible standards of security and business continuity.

Backup Policy. We follow the '3-2-1 backup' rule. Which means the data is stored in three different locations, via the live server hard disk, a backup server located in a region other than the live server and the AWS S3 cloud storage. We have four weeks' retention period for daily backups, the 3-month retention period for weekly backups, the 1-year retention period for monthly backup and 3-year retention period for yearly backup. We will agree your retention period requirements with you on appointment and in mutual agreement.

b. Hosting

SaaS solution and associated database will be regularly audited for security purposes to the ISO 27001:2013 Standard.

c. Evidence of security certification

d. All our offices across the globe are ISO 27001:2013 Certified and we follow best practice in relation to ISO 22301:2019 Business Continuity Management System to ensure internal and external business continuity. All certificates can be provide under request.

e. Cient-side requirements

Our application is completely web based and only requires internet and browser to access.

f. Database copy

Client can take backup of the database and store it in their environment.

g. Data centres

SaaS solution will be hosted in AWS cloud. AWS got in data centres within European Economic Area (EEA) jurisdiction. Application will be hosted European Economic Area (EEA) jurisdiction only.

h. Access controls

Access control policies like MFA (Multi factor authentication), IAM (Identity Access management), roles and policies will be in place to protect client data.

Secure Log retention is achieved by leveraging an audit trail: a digital record of server activity including data entry and user access activity. Audits will regularly be performed on applications and devices across your environment while simultaneously helping ensure the safety of your system by comparing issues to a list of known threats.

Our Security Log analyses user data histories from a central management console. Visual features facilitate easy interpretation of what users have access to what data, including when they accessed which resources. In terms of retention, this tool typically stores events for 30 days, although this can be varied and extended depending on

your requirements.

Number of events stored (and then reported on) depends on your own storage space limitations.

Logs can be retained to meet compliance log retention standardsand these logs are used to identify potential threats, focusing on user access and activity logs to catch additional risk factors, and implementing an overall strategy around security log monitoring to better identify and alert security issues.

Minimum log retention for a period of 6 months is available and can be reviewed in the case of breaches.

An admin approval process will be followed each time new accounts are created and access to your data from a secure device is made possible with HTTPS secure access.

We have a process for the immediate removal of access to data for all staff leaving the organisation who no longer require access.

Administrative facility for control of user accounts and user access privileges and roles

Role-based access control (RBAC) is an access control method is implemented.

Under this model, every employee is assigned a role. Every role has a collection of permissions and restrictions. An employee can access objects and execute operations only if their role in the system has the relevant permissions, can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices.

All resources, including the roots, organizational units, accounts, and policies in an organisation are owned by an administer account. Permissions to create or access a resource are governed by permissions policies.

The security protocols outlined above for access by the Contracting Authority's staff also apply to our own staff in Excelledia.

We have a process for the immediate removal of access to data for all staff leaving Excelledia or who no longer require access.

We also have a long established and trusted team and follow best practice in relation to all of our employee policies and procedures.

i. Suitability for client technical environment

Full technical details are provided in our separate Technical Proposal document. This includes our:

- Application Architecture Diagram
- Network Diagram
- Hardware Requirement

Support Service Levels

We have separately provided a copy of our proposed SLA which outlines our proposed service management facility.

This includes response and resolution times which are as follows and are also outlined in our SLA:

Severity Level 1. Occurrence is potentially damaging to end user supplied data; gives incorrect results without warning; prevents user from using any functionality that would normally be available and requires immediate action due to unavailability of a workaround known to the user.

Maximum response time Two (2) hours

Maximum resolution time
Not to exceed twenty-four (24) hours

Severity Level 2. Occurrence is not potentially damaging to end user supplied data; gives incorrect results but warns user, and does not prevent user from using any functionality that would normally be available; No workaround available.

Maximum response time Four (4) hours

Maximum resolution time
Not to exceed three (3) days. Workaround interim solution within Forty-eight (48) hours

Severity Level 3. Occurrence has a reasonable, secure, user-friendly and automated workaround that is not potentially damaging to end user supplied data; and does not compromise stability or introduce errors in other parts of the software.

Maximum response time Next working day

Maximum resolution time
Written response within one week giving detail of the proposed resolution schedule.

Severity Level 4. The problem has been investigated and classified as a minor enhancement with no business impact – such as when a change is needed in the User manual.

Maximum response time Five (5) days

Maximum resolution time
Written response within one month giving details of the proposed resolution schedule.

Severity Level E. Enhancement Request. Maximum response time
Thirty (30) days

Maximum resolution time
Enhancement requests will be reviewed on a monthly basis by Excelledia

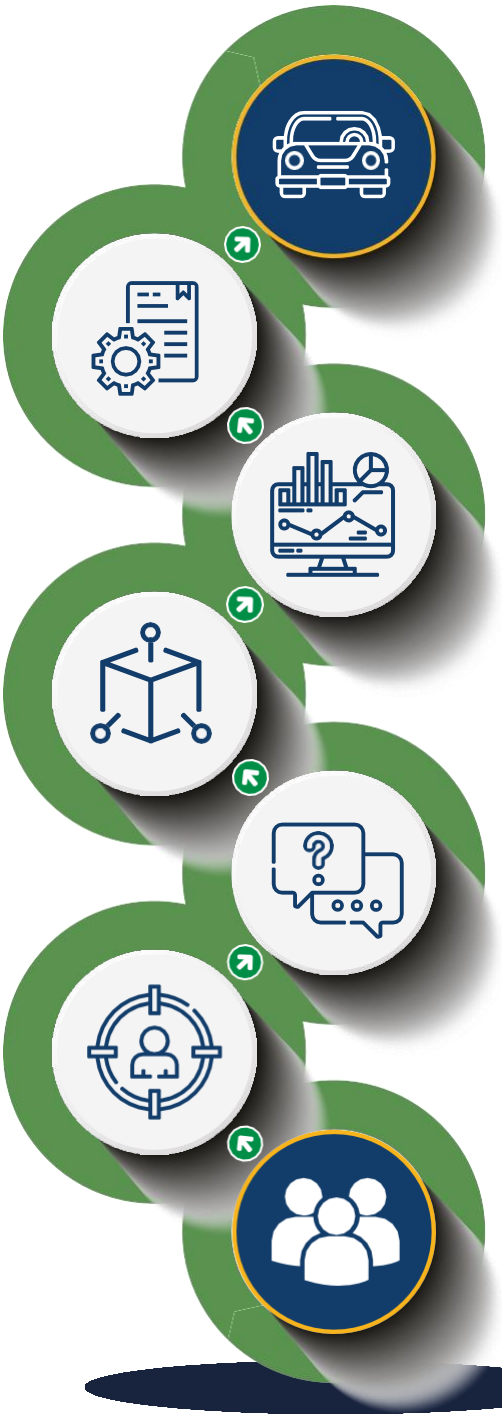
a. **Proposed Service Levels**

The Severity Levels categorization, description, Response Time, and Resolution Times shall be as set forth below:

Severity Level	**Problem Definition**	**Maximum Response Time**	**Maximum Resolution Time**
1	Occurrence is potentially damaging to end user supplied data; gives incorrect results without warning; prevents user from using any functionality that would normally be available and requires immediate action due to unavailability of a workaround known to the user.	Three (3) hours	Not to exceed **twenty-four (24) hours**.
2	Occurrence is not potentially damaging to end user supplied data; gives incorrect results but warns user, and does not prevent user from using any functionality that would normally be available; No workaround available.	Five (5) hours	Not to exceed **three (3) days**. **Workaround** interim solution within **Forty-eight (48) hours**.
3	Occurrence has a reasonable, secure, user-friendly and automated workaround that is not potentially damaging to end user supplied data; and does not compromise stability or introduce errors in other parts of the software.	Next working day	Written response within **one week** giving detail of the proposed resolution schedule.
4	The problem has been investigated and classified as a minor enhancement with no business impact – such as when a change is needed in the User manual.	Five (5) days	Written response within **one month** giving detail of the proposed resolution schedule.
E	Enhancement Request	Thirty (30) days	Enhancement requests will be reviewed on a monthly basis by Excelledia.

Business Process Analysis Methodology

Excelledia adopts the proven methodology to determine the core business processes and document them to arrive at the function points.



Follow visual design phase

Document Processes

AS-IS and to be process documentation and identification of Gaps

Interface Analysis

Analyzing the touch points with external systems and entities (If applicable)

AS-IS Modeling

Identify existing services, challenges, redundant processes, opportunities for improvement gaps, strategic disconnects if any.

Interview

Interviews with champions and nominated stakeholders to solicit ideas, identify requirements, verify facts, figures, engage end users.

Focus Group

Nominate champions from different user groups such as users, management reps, department heads etc

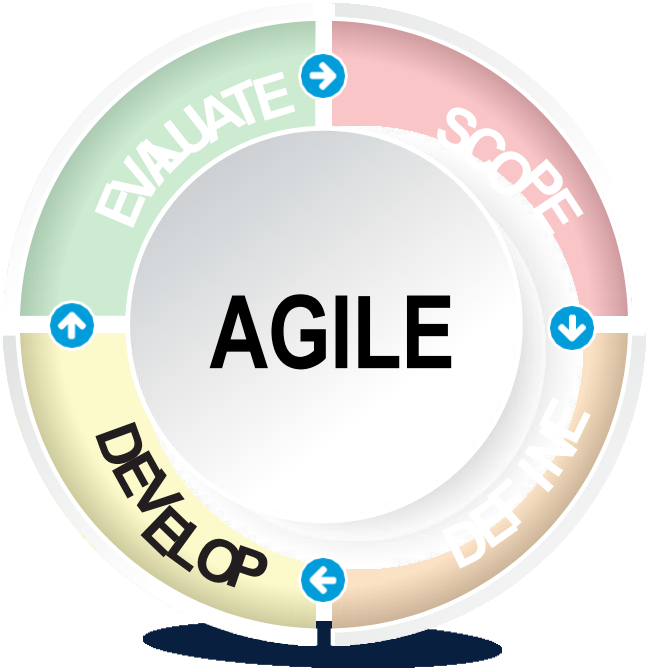
User Groups Profiling

Identify the user groups behavior patterns and goals.

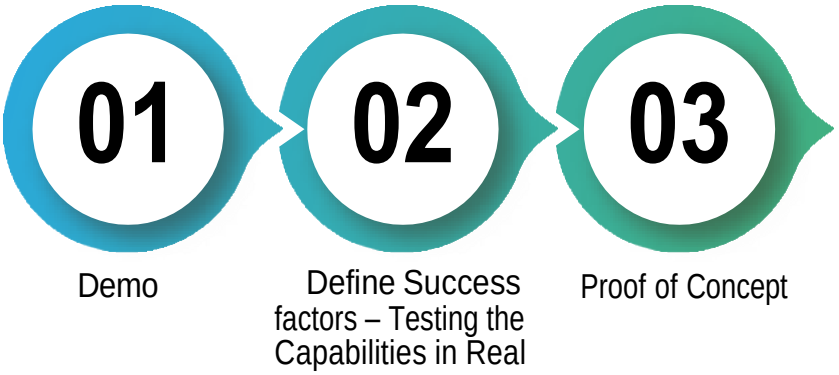
excelledia®

Project Approach

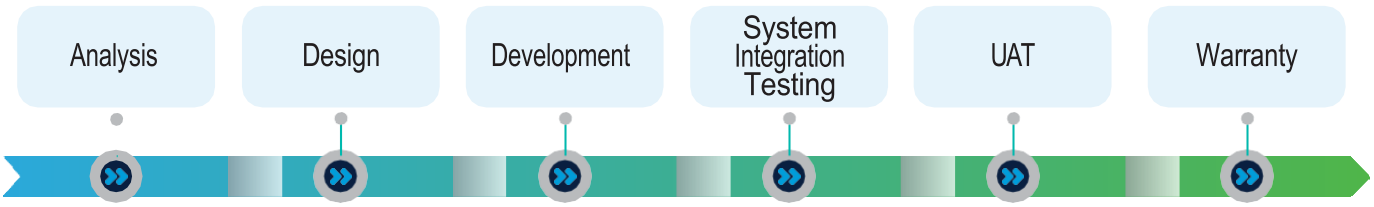
- Fast product releases and ability to gauge customer reaction and alter accordingly
- Focusing on Business value, allowing the client to determine the priority of features, the team understands what's most important to the client's business, and can deliver features in the most valuable order
- Incorporating continuous integration and daily testing into the development process, allowing the development team to address issues while they're still fresh
- Keeping customers involved and engaged throughout projects
- Agile methodology virtually eliminate the chances of absolute project failure



Prior to Awarding the Project



isorobot Project Management Methodology



excelledia®