Iress Software
Xplan

Technical Reference Guide

V 1.5
Nov 2023

1. Summary

The purpose of this document is to provide technical information that communicates details of the Iress Xplan software as deployed in the Iress Cloud Platform (ICP).

This document offers current and prospective clients with technical information regarding the Iress Xplan software and is also a technical reference for Iress client-facing, product and technology teams.

1.1 Document Information

Version	Date	Contributors	Notes
1.0	20 May 2020	Andrew Todd Emily Chen Luke Deller	Initial version
1.1	8 July 2021	Jeremy Epstein	Updating to mention auto scaling
1.2	20 July 2022	Priya Kandababu	Added HA testing
1.3	19 Jan 2023	Sumit Sharma	Updated Backup management and restoration
1.4	6 Feb 2023	Luke Deller	Updated Backup management and restoration
1.5	8 Nov 2023	Rodney Marsh	Expanded to cover Secure SDLC & CI/CD

Table of contents

1.2 Background

Xplan is a complete and comprehensive financial planning and wealth management software for advice practices of any size — from the smallest IFA to the most extensive networks. Xplan supports provisioning all types of advice, from simple through to sophisticated needs.

The software enables management of the entire advice process from discovery, current position, goal-setting, analysis, strategy development, production recommendations, advice documentation through to implementation and ongoing review— accessing powerful modelling tools and product information. Manage a client's portfolio, review strategies against objectives and truly bring people and their financial life into the process with an online portal and secure two-way messaging.

With centralised storage of all client data and documentation, the software has full workflow management capability and comprehensive reporting for business management.

Xplan is hosted, web-based software and ISO/ IEC 27001 security certified, ensuring data is secure. Its comprehensive functionality enables the operation of a front, middle and back-office on a single platform. With extensive training and user support available, Xplan is reliable and cost-effective software for advice and wealth management businesses.

2. Product summary

2.1 Overview

This section provides details of the capabilities of the Iress Xplan software. Specifically:

a. An overview of the core functionality provided

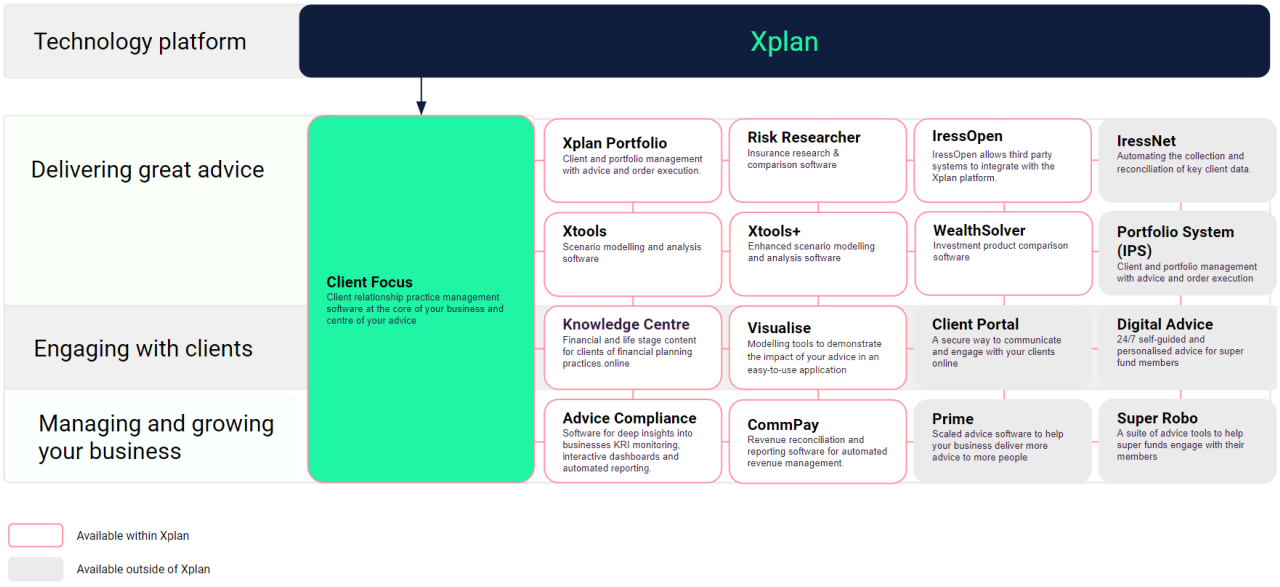
b. High-level architecture overview

c. Integrations and APIs

d. Key non-functional capabilities

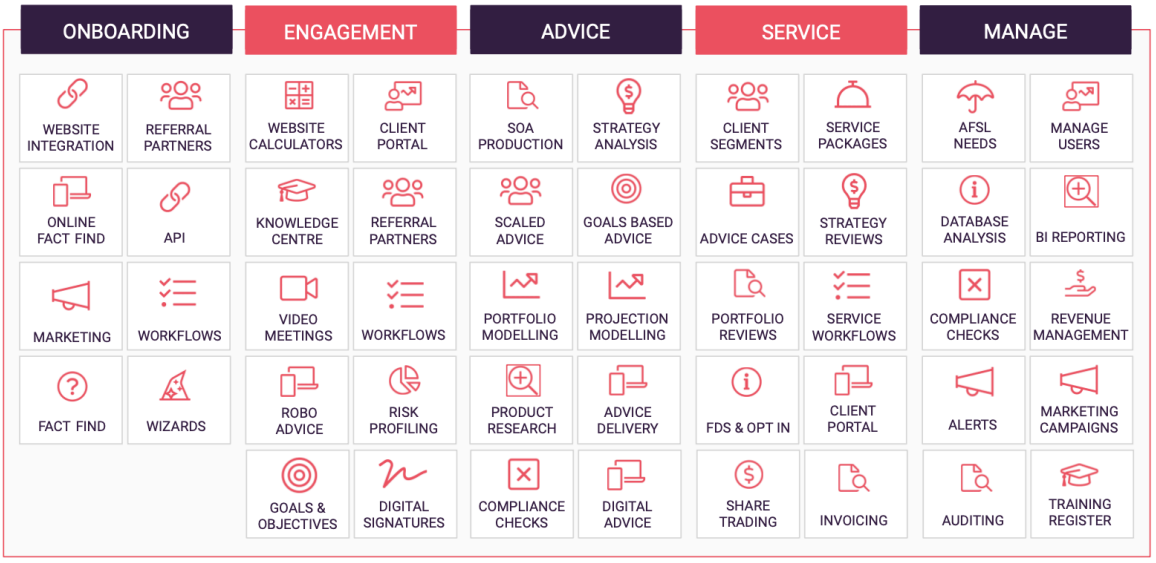
2.2 Product suite

The Xplan solution comprises a series of functional modules. These are selected and deployed based on client requirements.



A high-level view of the Xplan product suite

2.3 Functional overview



A high-level overview of the key functional capabilities of the Xplan product

a. **Client data & information**: Providing an effective and powerful client database and relationship management system for an advice business.

b. **The spectrum of advice & advice involvement**: Xplan supports the delivery of all types of personal advice—from clients with simple needs requiring single-issue advice to those with complex needs requiring comprehensive advice—and variation in the degree of adviser involvement—from client self-directed, to adviser guided and full-service advice.

c. **Strategy development & modelling**: Critical to the discovery and analysis process are the Xtools calculators and Xtools+ modelling tools. These intuitive, robust and illustrative tools help identify client needs, model scenarios and compare and assess strategy options.

d. **Research & comparisons**: Research and comparisons form the basis of sound financial recommendations and advice. Xplan offers a depth of information to enable purposeful analysis and considered recommendations.

e. **Advice recommendations, documentation & execution**: At the 'pointy' end of the advice process, integration and the re-use of data already captured, is a fundamental driver of efficiency. The Xmerge and eApplications functions allow for stored data to pass directly into advice document templates and application forms.

f. **Portfolio management**: Provides a complete, simplified view of portfolios. Manage and monitor portfolio positions with Xplan Portfolio.

g. **Strategy monitoring, goal tracking, reviews & reports**: These capabilities support the building and management of an ongoing service offering. Help ensure clients are on track to achieve their goals.

h. **Client engagement & experience**: With increased importance on client engagement, you can provide your clients with the flexibility and convenience of viewing their live, consolidated investment and insurance portfolio, (including other personal information) online.

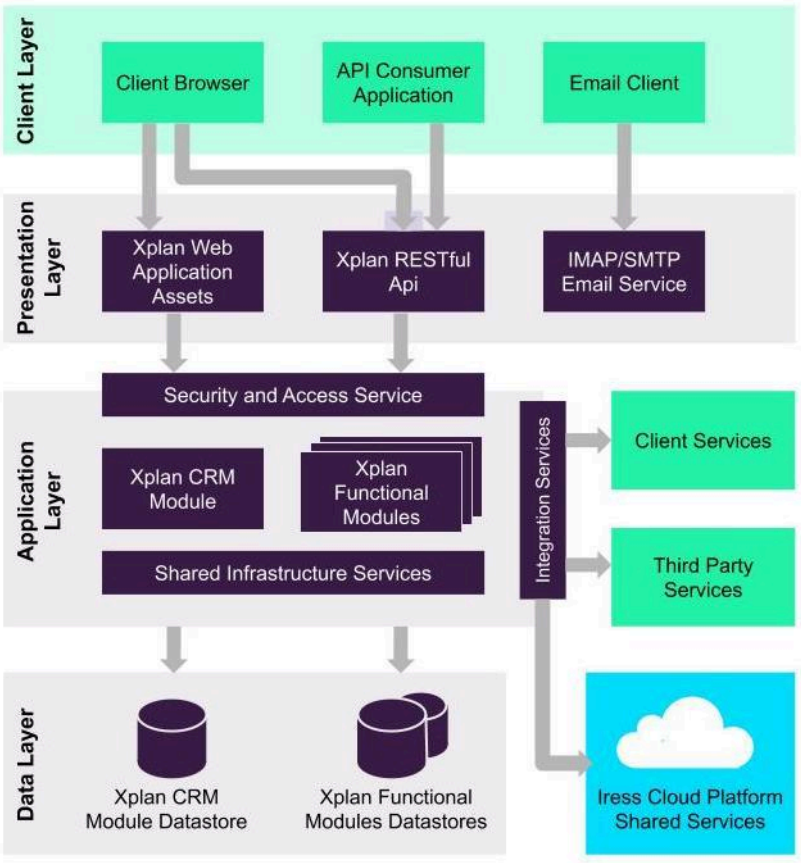
i. **Compliance and risk management**: Make the responsibility of satisfying compliance requirements and managing risk easier using Xplan's in-built features and functions. Streamline the process and reduce the hassle when dealing with compliance.

j. **Practice management**: Effectively manage your practice including, client reviews, activities, workflow, documents, client service delivery and staff management.

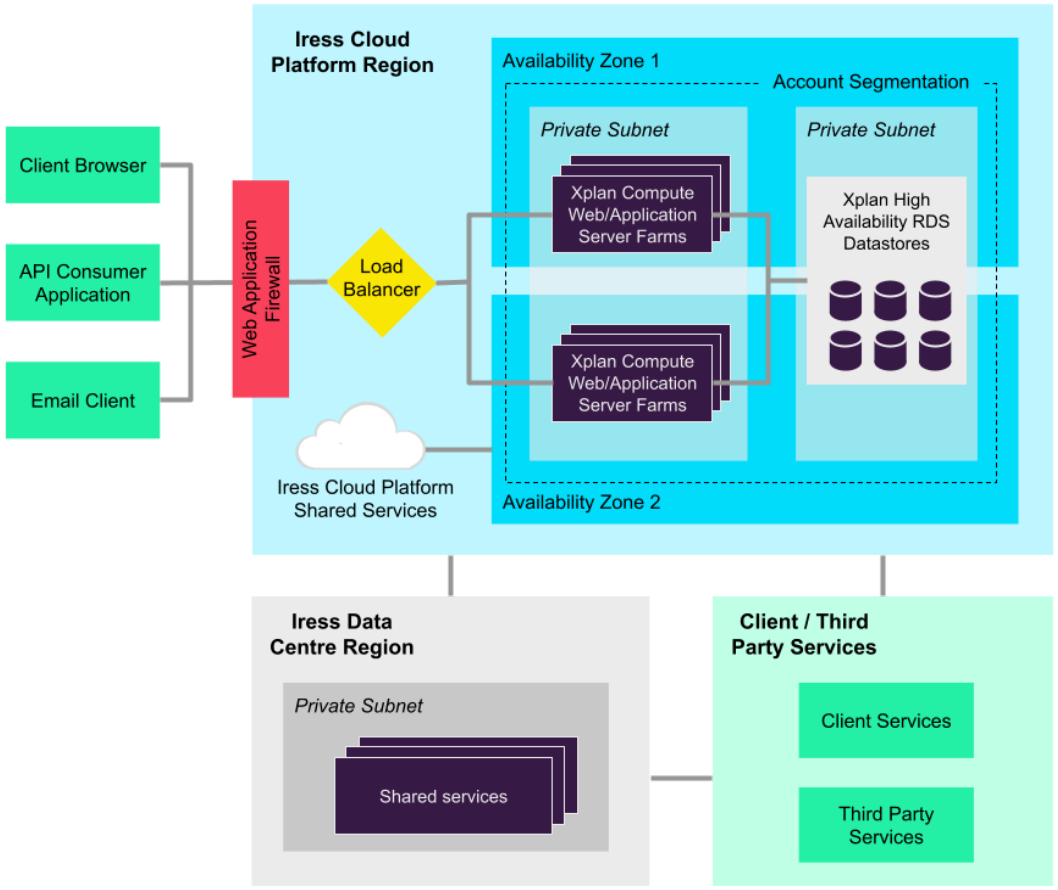
2.4 Software release details

Release notes are available on the Iress Community, click here for details (requires login).

2.5 Software design and architecture



A high-level logical overview of the Xplan architecture



Both the Iress Cloud Platform (ICP) and the Iress Data Centre (IDC) host the Xplan solution

a. Xplan is a web-based software application hosted within the Iress Cloud Platform (ICP) and the Iress Data Centre (IDC).

b. The application is container-based running on the Amazon ECS service. Deployment of the solution is via multiple instances running across availability zones delivering high availability and resilience.

c. The Xplan database is deployed as a highly-available datastore using the Amazon RDS service.

d. The Xplan solution connects to Iress Shared Services and other software in the Iress Data Centre via the AWS direct connect service.

2.6 Integration design and interface points

a. A developer-focused Xplan API enables the creation of external client solutions through integration with a RESTful API. The Xplan API co-exists adjacent to the Xplan website.

b. The Xplan API provides access to Xplan data and functional capabilities. Access is provided, but not limited to:

- client data
- investment information

- user/adviser data
- single sign-on (SSO)
- in-force production data
- calculations
- research
- marketing and leads management between applications

c. The Xplan API accepts access through HTTP Basic Authentication and OAuth 2.0. With HTTP Basic Authentication, any connecting application requires access to a valid Xplan account username and password for the authentication. Client HTTP client libraries must provide support for Basic authentication.

d. The Xplan API's OAuth 2.0 mechanism enables external application request authorisation to an Xplan users' data resources without requiring their password.

e. The Xplan External Data Interface (EDAI) allows read and write access using either JSON-RPC or XML-RPC and supports functions such as an asynchronous search.

f. The Xplan Synchronous Integration Services (SIS) permits configuration of software hooks into the application that triggers specific web services. This service is a powerful capability that facilitates many integration possibilities with various enterprise applications.

2.7 Key non-functional capabilities

a. Resilience and recovery

- Xplan leverages the resilience, reliability, security and governance provided by the ICP. Backups and shared services are centralised, automated and monitored within the ICP.
- The software also has several fault-tolerant and self-healing measures architectured into the software design and deployment architecture.
- If a processing node experiences an unrecoverable fault, it is detected, and a new instance gets launched to replace it automatically. The new node automatically receives web traffic from the faulty node.
- Xplan batch nodes are configured to auto-scale and auto-heal. The job queue takes advantage of this and will restart (with a max limit) any failed background tasks.

b. High availability

- The Xplan application is replicated and distributed over multiple fault-tolerant and geographically disperse availability zones (AZ)[1]. Application load balancers (ALB's) route traffic based on the availability of infrastructure.
- Each Xplan site gets provisioned with several web servers running active-active across different availability zones.
- The data tier gets deployed within an RDS cluster, leveraging the multi-AZ feature to ensure availability across multiple geographically dispersed locations.

c. Scalability

[1] Availability zones are geographically separate groups of one or more physical data centres.

- Software instances automatically scale horizontally based on client need, allowing additional nodes to process web traffic requests or report processing.
- Predicted volumes and client non-functional requirements drive the configuration of an initial deployment into the ICP. Monitoring of load and capacity is in place, ensuring the Xplan solution gets scaled appropriately to meet capacity demands.

3. Software delivery

3.1 Overview

This section provides details on some core aspects of the delivery approach for the Xplan software solution. Specifically:

a. Approach to source code and binary management

b. Approach to software delivery

c. Engineering practices and controls

d. Approach to software deployment

e. Approach to managing third-party dependencies

3.2 Source and binary code management

a. Iress uses source code management to provide versioning of source code, integrated and interactive peer reviews of code change as well as provide a secure repository for the code.

b. Iress uses an artifact management repository to store binary artifacts. Storage of software binaries in the repository occurs upon completion of a successful build.

c. Access to binary artifacts is secured and protected by the artifact management repository.

d. Iress' identity management and multi-factor authentication system integrates and protects access to the source code and artifact management repositories.

e. The source code management platform is configured with several technical guardrails to ensure an appropriate level of diligence concerning code change, such as the authenticity of commits, enforced peer review and defined code owners.

3.3 Approach to software delivery

a. The Iress Delivery Framework (IDF) has been developed for teams at Iress to work more collaboratively and consistently, and focus on building the right solutions in the best way possible within defined constraints. It utilises user feedback and measurements and includes the following components:

- Definition of product goals. Client outcomes are the focal point for how teams work together to solve problems.
- Opportunity exploration. Opportunities are evaluated using a variety of research methods and selected based on alignment with strategic objectives and product goals.
- Solution discovery exploration. A series of discovery sessions are held with experts across Iress to generate a solution hypothesis and a high-level delivery path.

- Design validation and inception. Once a solution hypothesis is evaluated and selected for development, our cross-functional product engineering teams further design and refine the solution, decomposing it into smaller increments that can be released independently and iteratively, and validated with users.
- Software engineering (where required). Once a solution hypothesis is evaluated and selected for development, our cross-functional product engineering teams further design and refine the solution, decomposing it into smaller increments that can be released independently and iteratively, and validated with users. Product engineering teams sequence the work into iterations and continuously build, release and validate new product increments with clients and users.
- Release. Automated processes ensure a consistent, scalable and repeatable to software releases.
- Launch and runtime management. Our software is continually measured and monitored against success goals and performance measures. Data is collected and combined with client & user feedback to inform further changes and future product investment.
- Continuous improvement. The Iress engineering team follows a continuous improvement process that is data driven looking for opportunities to improve efficiencies and fine tune the operation and performance of their solutions.

b. The IDF defines a consistent approach to sourcing, planning, and executing software and solution delivery. The IDF has four principles that drive activity and mechanisms to deliver work effectively. These are:
   - Broad collaboration
   - Include experts and stakeholders
   - Ensure constant validation of the work required
   - Continuously define and measure success.

3.4 Technical engineering practices and controls

a. Build
   - By using continuous integration principles and quality tooling, the software build processes automate the compilation of the codebase and execute various types of testing, including unit, integration, and smoke testing processes. The build process automatically creates and delivers the build assets to a central source for the artifacts to later be picked up by automated deployment tooling.

b. Reviews
   - Technical code reviews occur utilising a “pull request” mechanism within the source code repository. The result is that every code change requires at least two engineers to review the code changes, ensuring the code is fit for purpose and follows the required practices and policies.

c. Validation and testing approach
   - Each code commit has numerous validations applied. Unit and smoke testing help prevent any code that may pollute the codebase or cause production issues upon release.
   - After code changes are committed to the repository, there are several levels of automated integration testing that get executed before the binary code being accessible for production deployment.

- Execution of static code analysis occurs when code is committed to the repository. The code analysis provides several reports on the quality of the code committed such as technical quality indicators and security indicators.
- Execution of manual exploratory testing occurs on any development that may affect critical aspects of the application or key deliverables for initiatives in progress.
- Iress utilises the concept of a Test Pyramid to guide the approach to testing.
- Numerous guidelines are in place that together provide a view on the effectiveness and validity of the work done. These guidelines apply to the following:
    - (A) Functional review
    - (B) Adherence to unit testing coverage policy
    - (C) Impact analysis
    - (D) Quality gates (includes various test types)
    - (E) Software performance
    - (F) Software security
    - (G) Test criteria validation
    - (H) Regression testing
    - (I) Product manager review
    - (J) Release notes
    - (K) User guides
    - (L) Operational support guides
    - (M) Non-critical defects
    - (N) Client feedback
- A feature toggle strategy is used to develop and continuously integrate features into production releases throughout development. The features are only enabled for end-users after they have been through our validation and testing approach defined above.

3.5 Deployment

a. All Xplan sites operating within the ICP utilise the “auto-upgrade” facility enabling subscribed clients to receive ongoing enhancements and changes on a fast, regular basis.
    - The auto-upgrade capability supports and promotes a continuous deployment approach. With this approach, clients can quickly and easily benefit from improvements, defect fixes or other remediation work.

b. The code branching strategy ensures that the release branch is in a clean and releasable state.

c. Every change in the release branch goes through extensive automated tests. These tests are driven by continuous integration tooling and provide the quality assurance gates

d. Release candidate artifacts get automatically created and deployed to canary sites for further pre-release testing.

e. A final manual gate enables promotion of the software to production and executes the "auto-upgrade" process for the subscribed sites.

f. Within the ICP, Xplan infrastructure, tooling and related components are managed using Infrastructure as code (IaC) and Configuration as code. Automated testing of infrastructure, deployment verification and post-deployment health checks occur as part of the deployment pipelines.

g. Monitoring of production software health occurs by using inbuilt health checks.

h. Deployments of new releases follow a canary approach, where upgrades take place on a limited cohort of Xplan sites, monitored for a period of time and if no issues are detected, deployments are expanded to cover all eligible targets.

i. In case of an issue, deployments will be halted and a new patched version of Xplan will be released and deployed. Depending on the severity and impact of the issue, the version of Xplan with the defect may be “denylisted” in which case it will not be a viable target for upgrade.

3.6 Management of open source and third-party libraries

a. Xplan makes use of both open-source and commercial software libraries.

b. Restrictions on the use of third party libraries are in place.

c. Any libraries used are subject to several control activities.

- Penetration testing
- Automated and manual testing
- Version updates (with consideration given to preventing breaking changes)
- Where any library or open-source software upgrade introduces a breaking change, the implementation of the library or open-source software upgrade is incorporated as part of functional roadmap delivery.

d. Access to external libraries gets proxied via Iress’ package management platform to ensure there is appropriate allowlisting and denylisting of packages.

e. The package management platform and source code repository provide data related to the security profile of open source libraries, enabling proactive management of any security issues.

f. Xplan requires the use of only supported browsers and does not require the use of any legacy browsers or operating systems.

4. Security controls and data management

4.1 Overview

This section provides details on security controls and data management in the context of the software solution. Specifically:

a. Approach to user management

b. Authorisation and access control leveraged

c. Authentication approach

d. Use of encryption

e. Security verification approach

f. Auditing and Logging

4.2 User management

a. Iress does not manage user accounts within Xplan. The Xplan web interface and REST APIs provide facilities that enable clients to create and manage user accounts.

b. Iress supplies initial site administrator credentials. Clients use these credentials to set up site administrator accounts.

4.3 Authorisation and access controls

a. A combination of controls applies to data access and functionality within Xplan:

- User "capabilities" that get set on the user account.
- Group membership drives data visibility and access.

b. "User access levels" simplify the management of user capabilities by allowing sets of capabilities to be defined.

4.4 Authentication

a. The default authentication mechanism is username and password

b. Passwords get stored as PBKDF2/SHA256 hashes. Enforcement of minimum password strength is supported, along with temporary account lockout to protect against brute force password guessing attacks.

c. Multi-factor authentication is supported, where the site administrator can enable and of the following MFA methods:

- Soft token compatible with the OATH standard (such as Google Authenticator)
- SMS
- Email

d. Single-Sign-On (SSO) is available to delegate authentication to a corporate identity provider, using the SAML2 "Web SSO profile" standard.

e. Xplan does not generally use system accounts, however user entities can be set up as system or service accounts. These users, the same as all users, are controlled by capabilities, and can have the ability to login into Xplan front end removed.

4.5 Encryption

a. Encryption at rest applies for all data delivered through the use of RDS encryption for the database, AWS S3 encryption for documents, and AWS EBS encryption for file systems attached to compute resources which may hold temporary files.

b. Encryption in transit exists for all traffic across the Internet, primarily through the use of TLS / HTTPS. Additionally, client data transmitted within our internal network in the Iress Cloud Platform is also encrypted in transit. This includes traffic behind load balancers to web servers, traffic between services, and database access.

c. Where appropriate, Transport Layer Security (TLS) 1.2+ with Perfect Forward Secrecy (PFS) has been implemented. Our implementation of TLS enforces the use of strong ciphers and key-lengths where supported by the browser.

4.6 Software security validation

a. Iress executes an annual external security testing regime, performed by an independent security testing specialist. Additionally, Iress undertakes internal security testing using internal security engineers. Product engineering teams are assigned any findings from internal or external penetration testing to remediate in alignment with Iress policy.

b. Security and compliance validation is embedded in every stage of the lifecycle of components, systems and infrastructure. To ensure our applications are secure by default, all our components follow the standards as defined by the OWASP Application Security Verification Standard (ASVS v4.0.3). We also employ Static, Dynamic & Interactive Application Security Testing (SAST, DAST & IAST) tools at build, deploy and runtime to perform comprehensive security testing and monitoring.

4.7 Auditing and logging

a. Application, access and security logs get stored in Iress cloud platform with a 30 day retention policy. A policy of least-privilege access is applied.

b. Xplan produces infrastructure metrics and other life cycle events. This data gets directed to a central observability platform that enables continuous monitoring and automated alerting.

c. The automated deployment approach ensures all traceability of changes to the current system. Application and infrastructure assets get codified, and versioned artefacts maintained and audited.

4.8 Artifact security validation

a. Binary software images are scanned for security vulnerabilities before they are released.

4.9 Runtime environment security

a. All ICP hosts which run the software are hardened.

b. All ICP hosts have a security agent installed to enable runtime security and vulnerability scanning.

c. All ICP hosts are replaced with updated server images at least weekly.

5. Operational and runtime management

5.1 Overview

This section provides details on the operational and runtime management of the software solution. Specifically:

a. Approach to logging and monitoring

b. Alerting capability

c. Operational management needs

d. Provisioning and deployment approach

e. Maintenance and change windows

f. Backup management and restoration

g. Disaster recovery

5.2 Logging and monitoring

a. Xplan generates various operational logs and sends these to the ICP with a retention period of 30 days. These logs enable and aid in the troubleshooting of the Xplan software solution.

5.3 Alerting

a. Xplan uses several automated mechanisms to monitor the health of the software, including from outside the Iress network. Alerts are raised to engineering teams within Iress to act upon where necessary.

b. Infrastructure metrics like CPU usage, memory, network usage are gathered and monitored. Proactive alerting is implemented at predefined thresholds. Further, alerts are raised to the relevant product engineering teams within Iress to act upon if necessary.

c. Each Xplan site has myriad health checks run against it, including a range of internal and external connectivity checks, the checks include categories such as:

- Key modules and services are running without issue, including Commpay, IPS etc
- Key components and services are running without issue, e.g. DB
- Connections to third party apps and services are running without issue
- Connections to Iress systems (e.g. licensing and billing systems) running without issue
- Checks on user sessions, job queues etc.

5.4 Operational support

a. Iress operates a front-line service desk. The hours that the service desk operates varies depending on region and relevant support contracts.

b. A runtime operations team monitors the application and environment from 7am - 7pm in each region. This team is also the escalation point for the front-line service team.

5.5 Provisioning and deployment

a. Xplan infrastructure provisioning utilises an infrastructure and configuration as code approach. As a result, all infrastructure and system configuration is delivered from source code through automated deployment pipelines and the deployment of each environment is consistent, repeatable and scalable.

5.6 Maintenance and change windows

a. The auto-upgrade capability can upgrade an Xplan site on a weekday between 10pm and 5am and any time on the weekend. The process of upgrading an Xplan site may result in limited downtime.

b. All clients are on auto-upgrade with the majority on a weekly schedule. By exception, there may be an agreement between Iress and selected clients to determine the upgrade frequency for sites not on the weekly schedule program.

c. Downtime that cannot be scheduled during the preferred change window is communicated to customers either through their direct account managers or through the Iress Community page depending on severity and impact.

5.7 Backup management and restoration

a. The Xplan software utilises the ICP automated backup and retention capability.

   Backup frequency and retention period as per our backup policy:
   RDS backups for Production Instances
   - Daily - retain for 35 Days
   - Monthly - retain for 12 months
   - Bi-Annually for 7 Years

   After 7 years the RDS snapshot is deleted (a process which is managed by the AWS Backup service)

   Additionally there are backups supporting restoration to any point in time within the last 7 days, up to a latest restorable time of 5 minutes from the current time.

b. Restoring from backup has the following timing:
   - Recovery Time Objective (RTO): The backup restoration process will begin within 72 hours of customer request, and may take several hours (depending on the size of the database)
   - Recovery Point Objective (RPO): 5 minutes

c. General restoration testing is performed at least annually, and specifically on customer request with results documented.

d. Backup monitoring is enabled and configured as part of AWS Backup. Alerts from the backup are monitored and investigated as necessary.

5.8 Disaster recovery

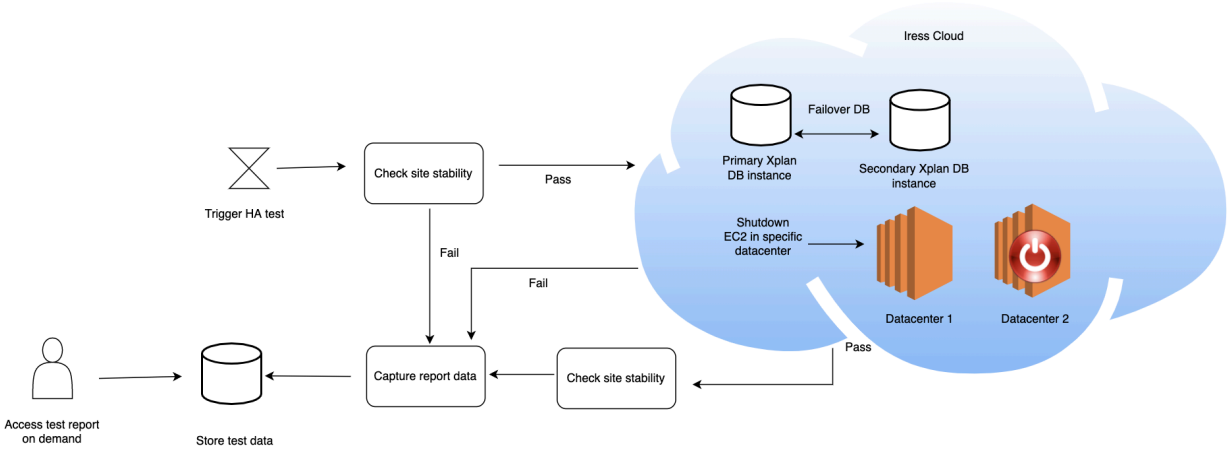
a. Enabled through the ICP, multiple availability zones use an active-active configuration behind load balancers ensuring there is no single point of failure in the application layer.

b. Automation of infrastructure and deployment enables responsive environment and Xplan site provisioning in the case of a complete disaster. Once restored, a database restoration is applied, the site is fully operational.

5.9 Testing high availability

a. The goal of testing high availability is to validate the resilience of the Xplan software and the underlying infrastructure environment. Testing is performed across the web, application and data tiers.

Automated testing process



a. The diagram above illustrates the flow of automated testing steps. The validations utilise in-built status information and include software health checks. Pre and post-check validations are used to confirm the software is operating as expected when software instances are “turned off” in the services in an availability zone. Once the above tests are complete, data are captured, reviewed and analysed for issues or improvement opportunities.

Testing scenarios

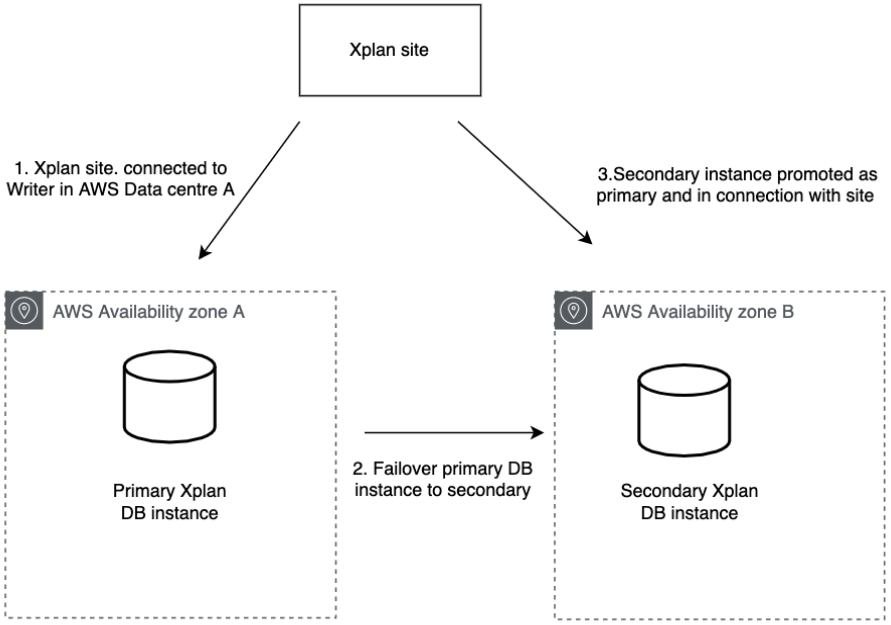
a. The following table summarises the test scenarios, expected data loss and the current status. Testing scenarios focus on services operating at different technical tiers. Additional information for each scenario follows the table.

Scenario	Expected data loss	Status
Database Ensure resilience exists when the “current live” database is made unavailable.	No	Available
Application services Ensure that application services continue to operate	No	Available

when individual services are made unavailable. The individual services include EC2 instances and containerised services within a specific availability zone.		
Application services Ensure that application services continue to operate when a complete failure of an availability zone occurs.	No	Test design and automated execution in planning.

Database

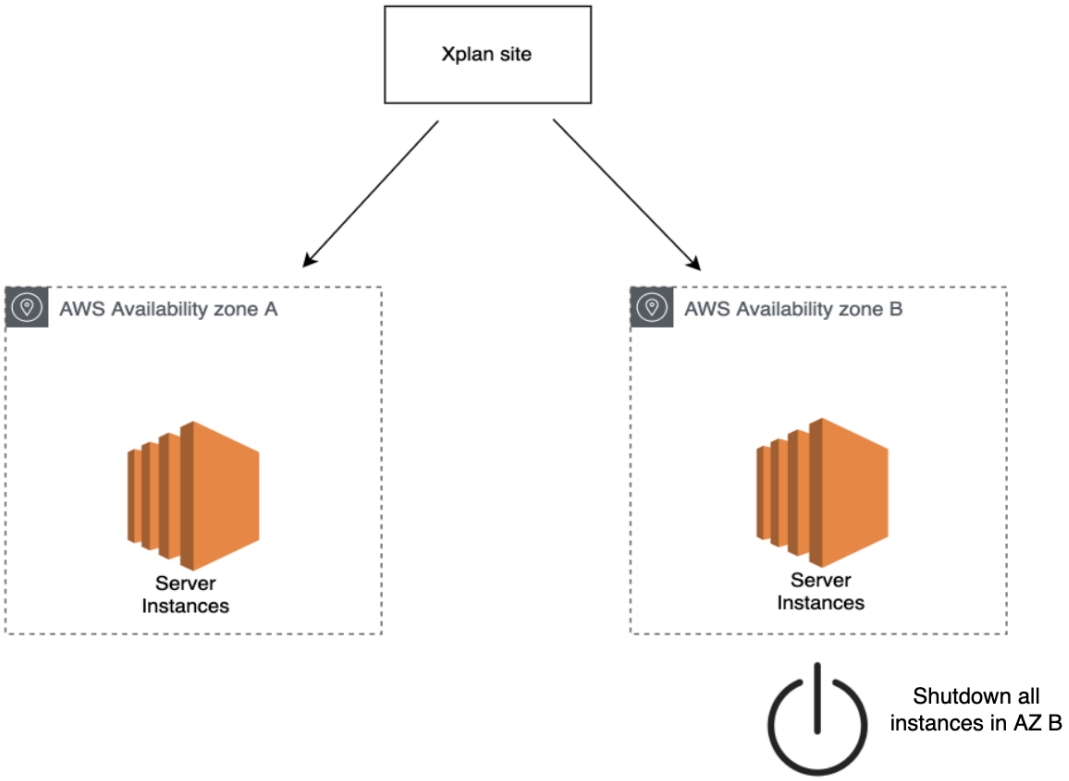
A. The Xplan database is hosted within the ICP and configured in a "multi-availability zone" mode for high availability across two availability zones. The test scenario will failover the writer instance (primary) and the reader instance (secondary) is promoted as a writer.



6. Application services

Test scenario: Shut down EC2 instances

A. Servers in one availability zone are shut down. Confirmation that the site is not affected by a service loss in a specific zone is validated, while automatic scaling ensures Xplan users are served effectively.



7. Supporting infrastructure

a. Xplan requires IDC access. It also requires some standard AWS functionality as an underlying component of the ICP.