Cradle

From concept to creation...

3SL

G-Cloud 13 - 3SL Cradle Cloud Software Services Definition

SG255/02 May 2022

https://www.threesl.com
salesdetails@threesl.com
support@threesl.com

Structured Software Systems Ltd (3SL)
Suite 2, 22a Duke Street
Barrow-in-Furness
Cumbria LA14 1HH, UK
Tel: +44 (0) 1229 838867
Fax: +44 (0) 1229 870096
Regd: 2153654 VAT: GB 473 2757 28

ISOQAR REGISTERED
UKAS PRODUCT CERTIFICATION
0026
Certificate Number 16926
ISO 9001

Contents

List of Figures

List of Tables

Product Description

Team collaboration tool for the full lifecycle definition, engineering and management of all your phased and agile projects, from unclassified (IL0) to OFFICIAL-SENSITIVE (IL3), that enables the:

- Capture, analysis and engineering of use cases, feature backlog, needs, goals, objectives, requirements, architecture and design models
- Tracing this data into a system, process, or product structure (SBS, PBS and CBS)
- Management of features with builds and releases and SCRUM iterations and/or phased developments
- Linking this data into UML, SysML, BPM, functional, architecture and EA models
- Definition of hierarchical risk register and linking to all this data
- Definition and execution of tests from module to integration and acceptance
- Publishing of contract-ready documents
- Supplier management
- Governance of the project, contractual relationships amongst its participants, and its deliverables

Different subsets of these capabilities are packaged into a range of Cradle software service offerings, all delivered from a choice of shared or dedicated SaaS hostings.

Service Summary

Table 1: Cradle Element

Cradle Service	
Hosting	UK-resident and/or UK-sovereign Unassured Cloud services (IL0) or Accredited Public Cloud services (OFFICIAL IL3)
Accessibility	PSN and Internet (IL0 only)
Contents	Cradle (web UIs and non-web UIs) and related desktop tools
Access	HTTPS secured: Remote desktop connection and/or Web browser connection
Data Exchange	Bidirectional to and from local desktop and network resources

1 Service Introduction

1.1 Objectives

The **3SL Cradle** service provides a configurable software solution for a wide variety of tasks in any and all of your product, service and enterprise architecture (EA) delivery projects.

For projects involvement the creation of physical products or infrastructure (such as roads, bridges, hospitals, railways, satellite systems), the **3SL Cradle** service can be used to capture needs and requirements for the project, to create physical or process architectures and designs for the project, to manage the implementation and build of the project, and/or to manage the testing and deployment of the project at all levels from unit through to integration testing and system acceptance.

For projects involving the creation of online software services, the **3SL Cradle** service can be used to capture needs and requirements for the service, to manage the feature backlog, the tasking of team members, the deployment iterations and sprints, and within each sprint, to manage the service design and architecture, the code modules, and the deployment and testing of the service at all levels from module, through integration and system acceptance.

For projects involving the creation of processes and organisation structures, the **3SL Cradle** service can be used to capture needs and requirements for the organisation, to support the Business Analysts (BAs) defining the enterprise architecture (EA), organisation breakdown structures (OBSs), roles and responsibilities and the process architecture, including the creation of process, functional, data and control models with notations including BPMN, SASD, PFDs, eFFBDs and IDEF. The **3SL Cradle** service can be used to manage the new process deployment and the monitoring of the effectiveness of this deployment.

For all types of project, the **3SL Cradle** service is particularly helpful when there are several organisations involved, and especially when these organisations are in a customer-supplier hierarchy, potentially of many levels. The service is particularly useful to capture, manage and assess the KPIs of the Service Level Agreements (SLAs) and Operating Agreements (OAs) that you create between these sets of cooperating parties.

1.2 Service Features

The **3SL Cradle** service is created from 3SL's requirements management and systems engineering tool "Cradle". The principal technical features of the service are:

1. Software as a Service (SaaS) from UK-based servers accredited from IL0 to IL3 that are accessible over public Internet (IL0) or PSN (IL3) and other HMG networks upon request
2. Your data is fully isolated in UK-resident private storage accessible only to the customer and only by the customer through the SaaS application
3. The SaaS environment is managed for you by 3SL:
   a) User management of access to the environment (you control and manage all access

to your data inside your databases)

b) Database management of your data, archiving, restoration and so on

c) Database backups to meet agreed KPIs in a Service Level Agreement (SLA)

d) Server snapshots

e) Resilient infrastructure

f) Governance processes to ensure the integrity and information assurance of the SaaS environment to protect you and your data

4. Applicable to any stage in all:

   a) Systems engineering processes
   b) Application lifecycle development processes
   c) Application lifecycle management processes
   d) Business analysis projects
   e) Business process modelling projects
   f) Requirements management processes
   g) Systems engineering processes

   for all product, service and enterprise architecture / business analysis projects

5. Simple on-boarding of your project process and data, guided and assisted by 3SL
6. Unlimited databases and data volumes, scaling to accommodate your projects' needs
7. Accredited environments from IL0 through IL3 (OFFICIAL - SENSITIVE) - RMADS in place with annual ITHCs (IT Health Checks) and fully assured ATO (authority to operate)
8. Delivering an integrated software tool to capture, analyse, engineer, check, manage, publish, review, baseline and evolve data for all stages in your project lifecycles, including goals, needs, epics, user stories, features, objectives, requirements, models, tests, builds, release items, defect items, verifications, acceptance items, processes and procedures
9. Accepts, manages, and provides traceability to/from any number of versions of any number of source documents and the user-defined information in the databases
10. Publishes any number of issues of any number of user-defined, production-quality, project documents with automatic traceability between the database and the contents of these document issues
11. Range of supporting consultancy and training services
12. Full range of off-boarding services, guided and assisted by 3SL

1.3 Service Benefits

The principal benefits from the **3SL Cradle** service are:

1. Complete integration of all functionality for the complete lifecycle (or some subset of this, depending on the Cradle service chosen) that is equivalent to combining multiple tools (such as JIRA®, Confluence®, Polarion®, DOORS® Enterprise Architect®,

Archimate® and QualityCenter®), eliminating tool interfaces, multiple databases and training needs, removing duplicative functionality and reducing cost

2. Coordinates work by any number of users and groups
3. Manages any volume of any types of information and documents
4. Ensures nothing is missed with end-to-end traceability
5. Prevents scope creep with end-to-end coverage analyses
6. Proves closure of issues and defects
7. Provides stakeholders controlled access to their parts of the project data
8. Eliminates quality problems, using automated, user-defined, content, conformance and consistency checks
9. Eliminates omissions and unwarranted insertions, by using bi-directional, uniquely transitive, traceability
10. Automatically generates consistent, production-quality, documentation in your format
11. Easily reuses and shares information between projects, teams and stakeholders
12. Automatically generates management information, KPIs, and dashboards
13. Automates release management from sprints, iterations, phases and quality reviews

1.4 Service Elements

The **3SL Cradle** service comprises:

1. Licences of the 3SL requirements management and systems engineering tool “Cradle”
2. A ***Cloud Hosting*** delivery platform, your choice of:
    - An ***Unassured Cloud*** using shared hosting or
    - An ***Assured Public Cloud*** such a 3SL-standard architecture that have been approved to manage information up to OFFICIAL-SENSITIVE, IL3 by having been CLAS certified based on a risk management documentation set (RMADS), threat analysis according to IS1 and IS2, architecture assessment, penetration test and IT Health Check (ITHC)

    from a range of alternative UK-based and/or UK-sovereign PaaS (Platform as a Service) providers, including:

    - Amazon Web Services (AWS)
    - FCDO Services (formerly FCOS)
    - OVH
3. A database design (***schema***) optimised for one or more of:
    - Agile collaboration, including sprints / iterations, needs, goals, features, epics, user stories, verifications, acceptance, builds and releases
    - Agile software development, including sprints / iterations, needs, goals, features, epics, user stories, models (analysis, process, architecture and design), verification, acceptance and releases
    - Agile software management, including sprints / iterations, needs, goals, features, epics, user stories, verifications, acceptance and releases

- Application lifecycle development including needs, goals, objectives, user and system requirements, models (analysis, process, architecture and design), tests, releases, issues and defects
- Application lifecycle management, including needs, goals, objectives, user and system requirements, tests, releases, issues and defects
- Business analysis, including needs, goals, objectives, user and system requirements, and process, procedure and task descriptions
- Business process modelling, including needs, goals, objectives, user and system requirements, models (analysis and process), and process, procedure and task descriptions
- Requirements management, including needs, goals, objectives, user and system requirements (functional and non-functional), verifications and acceptance
- Systems engineering, including needs, goals, objectives, user and system requirements (functional and non-functional), models (analysis, process, architecture and design), verifications and acceptance
- Traceability
- Document publishing
- Issue tracking
- Defect tracking
- Risk management, with all risks linked into the product/service description, requirements and test data
- User Acceptance Tests (UATs), acceptance criteria, validations, verifications, test cases, test plans, test runs and test results. Cradle fully supports test execution, helping to automate your testing processes

Please note the schema will be dependent on the **3SL Cradle** service element chosen.

4. Unlimited technical support from our UK-based, security-cleared, support team
5. A range of optional training and consultancy services

2 Cradle

2.1 Summary

Cradle provides features to create and manage all types of data, at all levels, throughout a product, service or enterprise development. By managing data in one place, Cradle can provide traceability across the entire lifecycle in one tool. Without Cradle, you must assemble multiple tools, typically from different vendors, and try to assemble them into a working ***toolchain***:

- That can exchange data bidirectionally
- That manages the many duplications of data across tools that are needed for each tool to have an accurate representation of its part of the over project traceability
- In which your actions in one tool automatically causes other tools to perform whatever

corresponding actions may be necessary to maintain consistency of all tools' views of the project data

and even then you will still not have the full traceability that Cradle can provide.

Cradle is multi-user, multi-project, distributed, open and extensible. It links to your existing desktop tools to create a tailored environment to suit your process.

Cradle has built-in issue, risk, test and interface management. It supports comparative trade studies. It has a built-in configuration management and control system. It bidirectionally links a ***Work Breakdown Structure*** (WBS) and progress reporting to your project planning tool. Cradle removes the need for you to connect risk, CM or change tracking tools to your:

- Systems engineering
- Requirements management
- Agile process
- Application lifecycle development
- Business analysis
- Business process modelling

Cradle provides everything you need, integrated and ready to use.

Cradle has customisable, hierarchical, access control facilities and integrates with your authentication, access control and security mechanisms including firewalls, LDAP and SSL. Cradle is CLAS accredited within HMG.

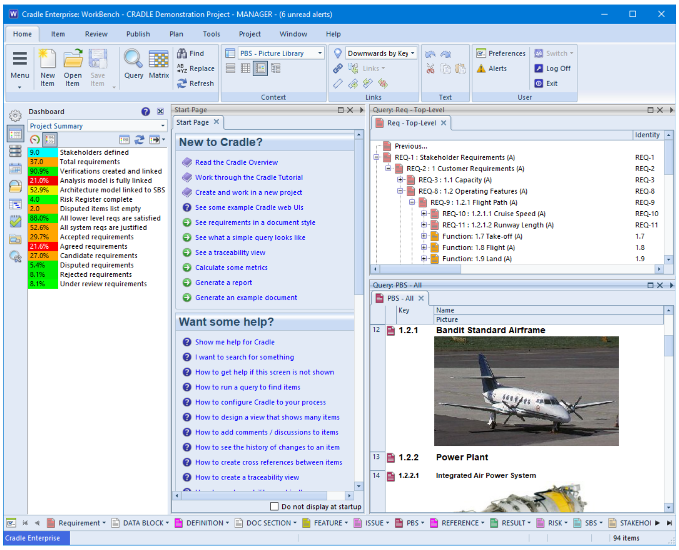
Cradle provides user-definable views of project data, tailored to each stakeholder group. With customisable navigation, review and entry tools and tailored web UIs, Cradle shows each user the data that they want to see, in the way that they want to see it.

Projects use user-defined, arbitrarily extensible databases, linked to external files, URL resources and data in external repositories. Each database is configuration controlled, with change histories, baselines, versions and variants, managed by configurable change requests and change tasks, and using user-defined workflows.

2.2 Capabilities

The **3SL Cradle** service is a multi-user, collaborative environment to:

- Capture and manage any number of types of information
- Track multiple versions of any number of source documents
- Create traceability links between information
- Track changes to information & links
- Publish to user-defined views and documents
- Track multiple versions of all published documents and the database information items that have been published inside them
- Maintain the project ***risk register***
- Manage information with built-in CM
- Manage WBSs and users' task lists
- Provide management metrics, dashboards, KPIs and earned value / burn down charts



9.0	Stakeholders defined
37.0	Total requirements
90.9%	Verifications created and linked
21.0%	Analysis model is fully linked
52.9%	Architecture model linked to SBS
4.0	Risk Register complete
2.0	Disputed items list empty
88.0%	All lower level reqs are satisfied
52.6%	All system reqs are justified
29.7%	Accepted requirements
21.6%	Agreed requirements
27.0%	Candidate requirements
5.4%	Disputed requirements
8.1%	Rejected requirements
8.1%	Under review requirements

New to Cradle?

- Read the Cradle Overview
- Work through the Cradle Tutorial
- Create and work in a new project
- See some example Cradle web UIs
- See requirements in a document style
- See what a simple query looks like
- See a traceability view
- Calculate some metrics
- Generate a report
- Generate an example document

Want some help?

- Show me help for Cradle
- I want to search for something
- How to get help if this screen is not shown
- How to run a query to find items
- How to configure Cradle to your process
- How to design a view that shows many items
- How to add comments / discussions to items
- How to see the history of changes to an item
- How to create cross references between items
- How to create a traceability view

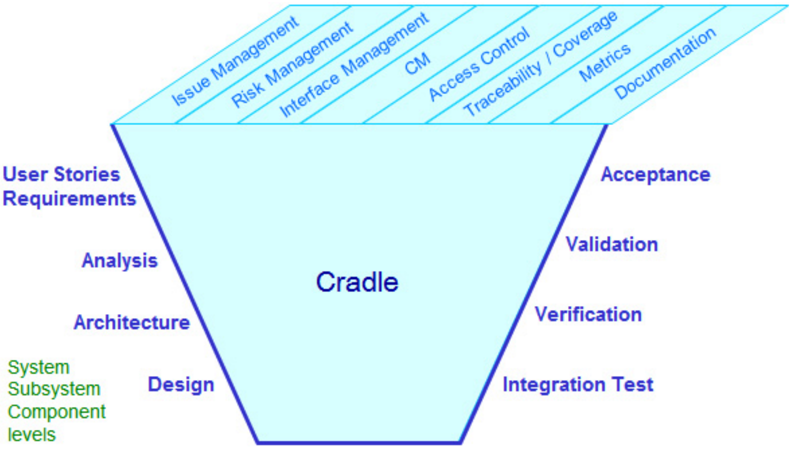
□ Do not display at startup

	Identity
Previous...	
REQ-1 : Stakeholder Requirements (A)	REQ-1
REQ-2 : 1 Customer Requirements (A)	REQ-2
REQ-3 : 1.1 Capacity (A)	REQ-3
REQ-8 : 1.2 Operating Features (A)	REQ-8
REQ-9 : 1.2.1 Flight Path (A)	REQ-9
REQ-10 : 1.2.1.1 Cruise Speed (A)	REQ-10
REQ-11 : 1.2.1.2 Runway Length (A)	REQ-11
Function: 1.7 Take-off (A)	1.7
Function: 1.8 Flight (A)	1.8
Function: 1.9 Land (A)	1.9

	Key	Name Picture
12	1.2.1	Bandit Standard Airframe
13	1.2.2	Power Plant
14	1.2.2.1	Integrated Air Power System

2.3 Key Features

- Supports a full lifecycle at system of systems, system, subsystem and lower levels
- Fully user-definable and user-extensible
- User-defined information, such as epics, user stories, requirements, sprints, risks, features, tests & validations
- Scales to millions of information items
- Full traceability of data with full version management



- Traceability and coverage analyses, with indirect, transitive, cross-lifecycle traceability
- Unlimited user-definable views of data including tables, trees, documents, matrices, pivot tables, diagrams and graphs
- Built-in change tracking and formal configuration management (CM), with user-defined workflows, formal reviews, change control (CC), version management, and baselines
- User-defined access controls (to attribute level), team hierarchies and truly multi-user information locking to prevent conflicting updates
- Collaboration including comments, discussions and user-defined alerts
- User-definable UI, including process-related ***phase hierarchies*** through which users can operate Cradle separately from its as-supplied UI, and start pages (optionally graphical) of convenient short-cuts, both with user-defined content that can be customised for

each user and stakeholder group

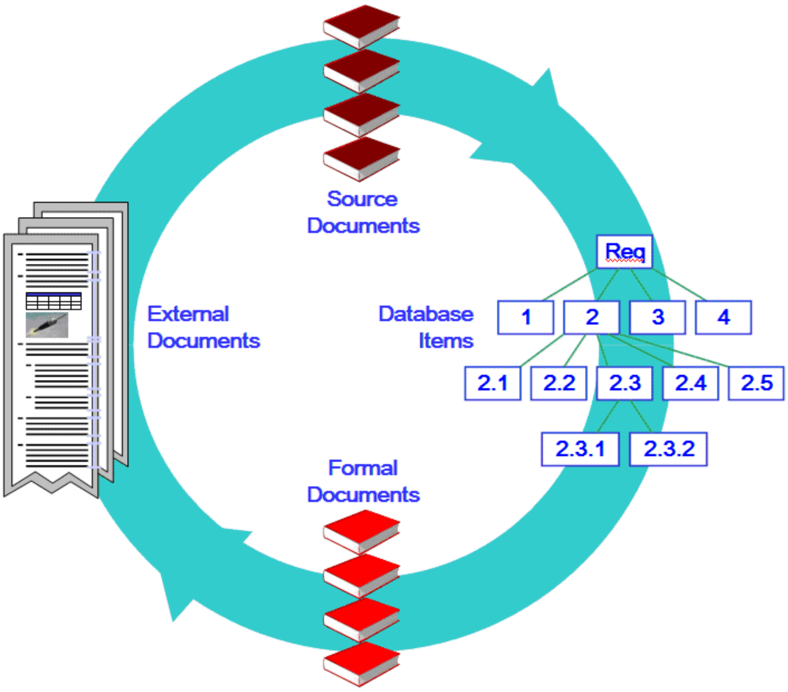
2.4 Applications and Uses

You can use Cradle to:

- Manage data for all of your project phases
- Capture data from external documents or tools and track changes to these sources
- Build new sets of requirements, user stories, SBS, WBS, PBS, functions, architecture components, tests or verifications and link them to the source data and each other
- Check the quality of text statements and data structures
- Create analysis, process, architecture and design models
- Check the quality and consistency of the models and their traceability to non-model data
- Prove information integrity with traceability and coverage analyses
- Raise customers' confidence with proof that your work satisfies its source data, complies fully with its constraints, and will meet their needs
- Generate full project documentation and track data in all issues of project documentation
- Track your progress with metrics, dashboards and KPIs and link your WBS and actual progress to project planning tools

You can create any number of projects, each with a schema and a database of any number of items of any number of user-defined types. Each item contains any number of attributes, each with up to 1 TByte of any type of data, held in Cradle, or referenced in files, URLs or other tools. Attributes can be of any of over 30 data types provided by 3SL, including user-defined calculations. You can also define your own data types if needed.

All items can be linked with user-defined types of cross reference. Links have attributes to justify, parametise or explain them. Links are direct and indirect, for full lifecycle traceability, impact and coverage analyses.



External documents can be loaded into hierarchies of items. Every requirement, regulation or other item in Cradle is linked to any document from which it was loaded. Changes in new document versions are found automatically and the database updated. You can prove the integrity of your source data to customers with a full range of coverage analyses of their documents.

Items can be linear, hierarchical and in many-to-many relationships. Item can be split, merged and reordered. All information can be shared and reused across all such structures. You can easily support product ranges, models, variants and builds in your Cradle databases.

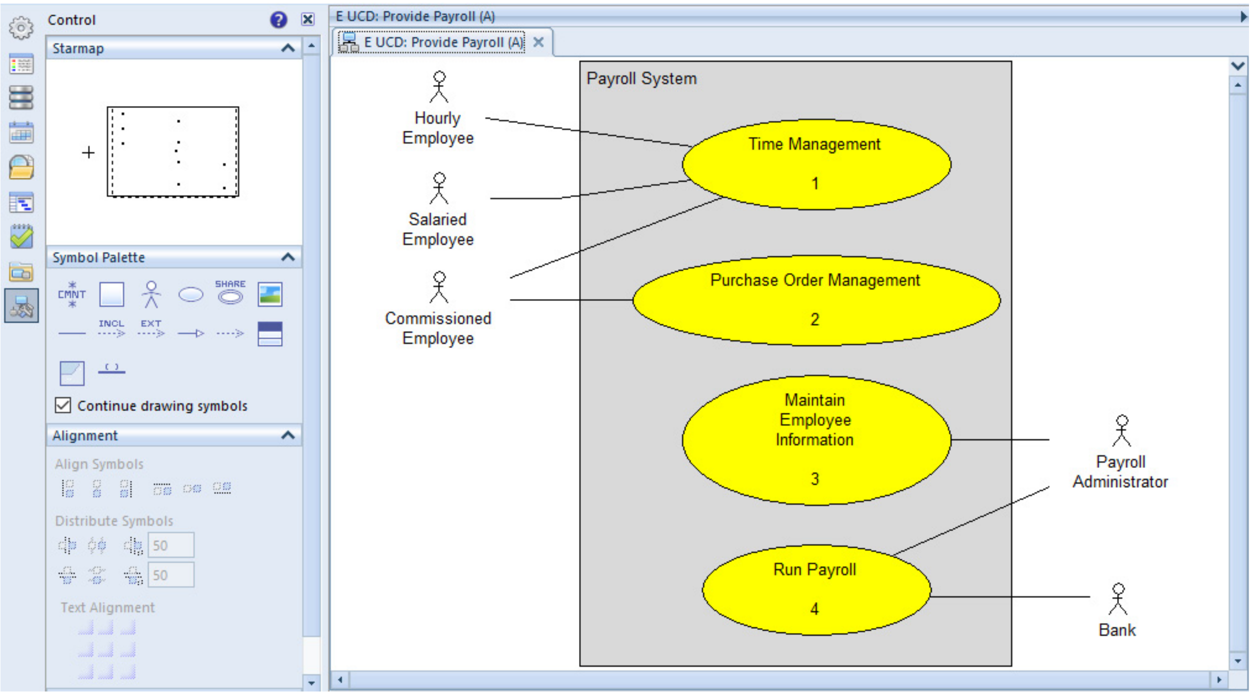
You can create any number of analysis, process, architecture and design models in SysML, UML, eFFBD, SASD, IDEF, ADARTS, BPMN and other notations. Each model can contain any number of diagrams and supporting descriptions (specifications and data definitions). You can use notations from different methodologies in the same model wherever you decide that this will assist the primary purpose of any model, to communicate clearly and effectively.

Automatic syntax checking is applied to model elements. Each model can be checked for consistency and completeness.

Models can refer to each other, allowing libraries of reusable models. Consistency checks across models allow each use of a model in a project to be verified against that model's external interface in the library.

Models can optionally be grouped into hierarchies or into graphs, for example to:

- Represent separate stages in an evolutionary process
- Contrast alternative processes, for example ***as-is-now***, ***as-proposed***, ***as-designed***, ***as-implemented*** and so on
- Explore design alternatives
- Show decomposition through levels from system-of-systems, system, subsystem, equipment to component

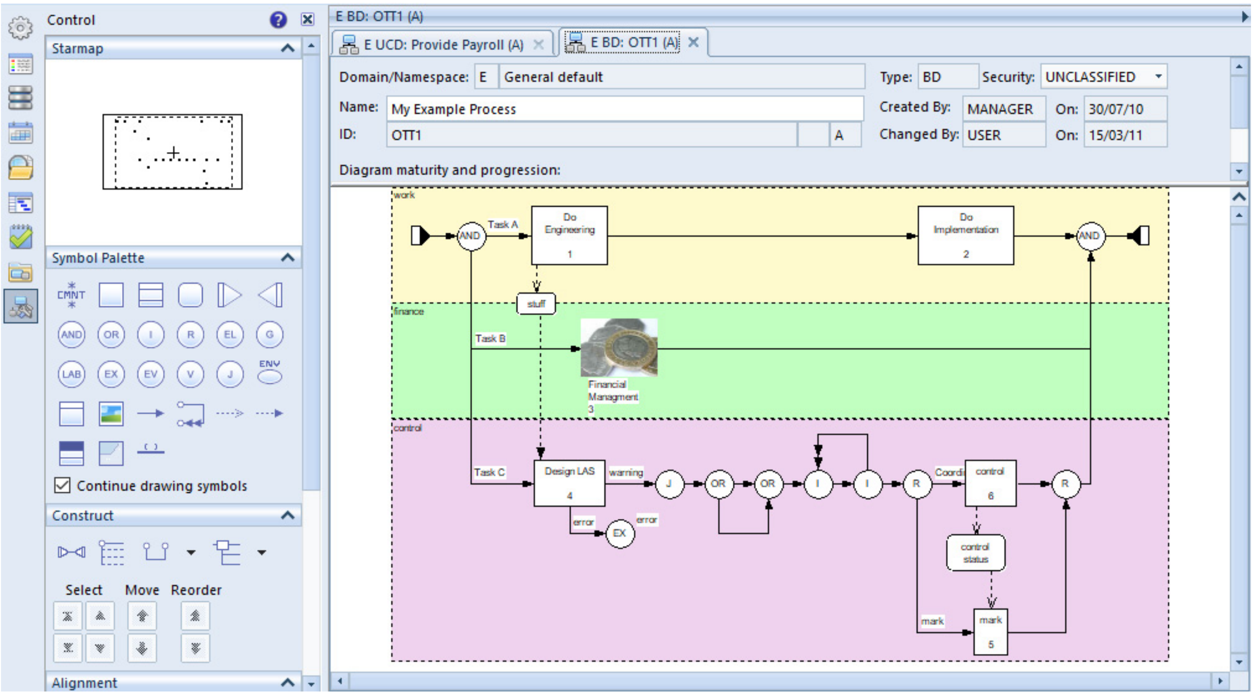


- Show evolution of the system from sprint to sprint, iteration to iteration, or release to release

Every diagram, specification and data definition in every model can be linked to non-model information, including user stories, requirements, SBS, features, risks, test cases and all other information. You can show these links graphically as item and containment symbols in any of a model's diagrams.

You can create models to describe process, logical and physical architectures. Process architectures are an essential business analysis tool. Logical architecture models describe physical components and logical connections. Any diagram symbol can be replaced by some embedded graphics, to make diagrams easier to understand.

Physical architectures describe the same physical components and physical connections. Cradle supports any number of physical architectures for each logical architecture so that performance, resilience, reliability and FMECA analyses can be applied.



E BD: OTT1 (A)

E UCD: Provide Payroll (A) | E BD: OTT1 (A)

Domain/Namespace: E General default

Type: BD

Security: UNCLASSIFIED

Name: My Example Process

Created By: MANAGER On: 30/07/10

ID: OTT1 A

Changed By: USER On: 15/03/11

Diagram maturity and progression:

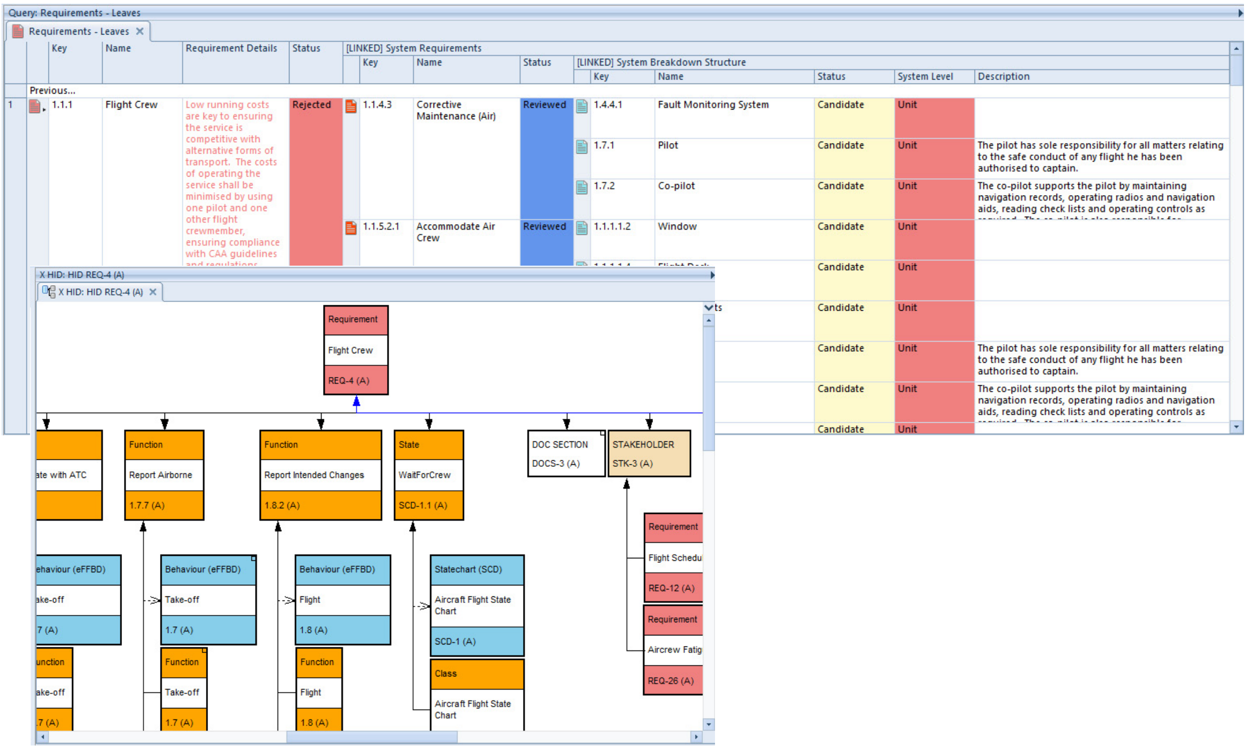
Cradle tracks all edits to every epic, user story, sprint, release, feature, requirement, test case, verification and all other information that you want it to hold. Edits can be reversed selectively or by group. Change logs are immediately available.

All information can be checked for quality using user-defined rules that analyse text, model consistency and item structures. Model check rules can be customised.

You can control all work with team hierarchies, roles and access controls. Items are reviewed with discussions, user-defined workflows and built-in CM, with baselines, full version control and formal change management.

You can generate reports and documents including URD, SRD, RTM, PVM, IRS, SDS or SSDS in any desired format and with full traceability across any number of sets of information and full traceability of which items were published in each document issue.

You define how information is viewed and reported in any number of ***views***, and shown as nested tables, trees, matrices, pivot tables, and as diagrams. You can create ***custom web UIs*** for stakeholder groups in which each web UI has any style and appearance, presents just the data appropriate to that group and provides the functionality that the group needs. Cradle can provide any number of these custom web UIs simultaneously.



Query: Requirements - Leaves

Requirements - Leaves

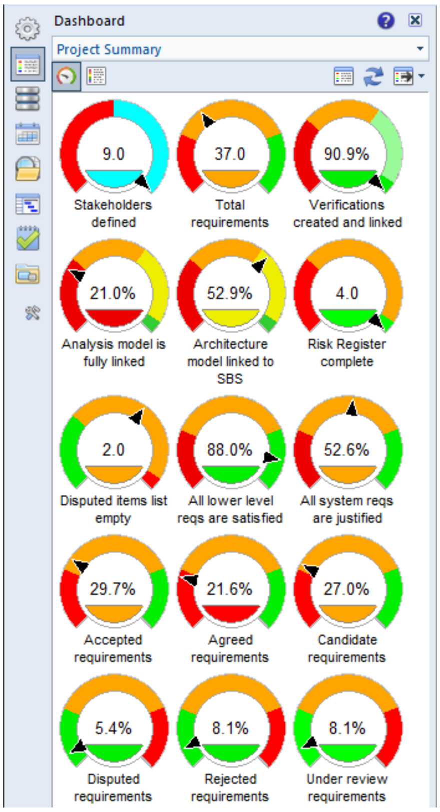
	Key	Name	Requirement Details	Status	[LINKED] System Requirements Key	Name	Status	[LINKED] System Breakdown Structure Key	Name	Status	System Level	Description
	Previous...											
1	1.1.1	Flight Crew	Low running costs are key to ensuring the service is competitive with alternative forms of transport. The costs of operating the service shall be minimised by using one pilot and one other flight crewmember, ensuring compliance with CAA guidelines and regulations	Rejected	1.1.4.3	Corrective Maintenance (Air)	Reviewed	1.4.4.1	Fault Monitoring System	Candidate	Unit	
								1.7.1	Pilot	Candidate	Unit	The pilot has sole responsibility for all matters relating to the safe conduct of any flight he has been authorised to captain.
								1.7.2	Co-pilot	Candidate	Unit	The co-pilot supports the pilot by maintaining navigation records, operating radios and navigation aids, reading check lists and operating controls as
					1.1.5.2.1	Accommodate Air Crew	Reviewed	1.1.1.1.2	Window	Candidate	Unit	
								1.1.1.1.4	Flight Deck	Candidate	Unit	
										Candidate	Unit	
										Candidate	Unit	The pilot has sole responsibility for all matters relating to the safe conduct of any flight he has been authorised to captain.
										Candidate	Unit	The co-pilot supports the pilot by maintaining navigation records, operating radios and navigation aids, reading check lists and operating controls as
										Candidate	Unit	

You can manage the progression of your projects with:

- ***Metrics***, user-defined calculations of items' values
- ***Key Performance Indicators*** (KPIs), results of metric calculations with colour-coded display bands shown as a table or dials
- Bi-directional links to Microsoft Project, including task lists and actual progress reporting between the WBS in Cradle and the project schedule

Cradle is open. It supports many I/O formats (such as CSV, TSV, XML, ReqIF, Cradle and Cradle-XML), has many interface mechanisms to link to other tools including API, RESTful WSI, DDE and user-defined commands, and has bi-directional interfaces to Office, including Word, Excel, PowerPoint, Visio and Project.

Cradle is simple to customise and use. You do not need to write code or scripts to tailor it. After every change to your schema, Cradle will automatically update collections of queries, views, forms and other definitions that make you productive immediately.



2.5 Management

Cradle is simple to manage and administer. The **3SL Cradle** service can have any number of databases. You have full control over the access to, and content of, each of these databases.

All administration is through simple point-and-click UIs to:

- Manage data and user policies (such as password aging and automatic lock-outs)
- Manage user accounts
- Manage the database structure (***schema***)
- Run data and cross reference integrity checks
- Analyse the quality of the data being entered, against criteria that you define

Real-time management information is available to monitor:

- User logins
- Login failures
- User lock-outs
- Licence usage
- Licence denials

This information can be graphed, automatically if you wish, to produce day-by-day, weekly or monthly summaries of the usage of the Cradle system.

Further logs exist to track each access to Cradle and to confirm the security and integrity of these connection attempts. You can optionally limit the remote locations (hosts or IP addresses) from which access can occur, and the remote users who can gain access. These controls apply to both web-based and non web-based users.

Cradle will automatically share licences between all connected users. You can apply controls to ensure that idle users do not consume licences that should be available to others, and to optionally limit which licences are available to each user.

With assistance from 3SL, you can configure single-sign-on, such that access to your **3SL Cradle** service does not require a username or password, such details being taken from the users' host environment. This mechanism is not permitted in OFFICIAL - IL3 environments.

3 The Cradle Service

The service will deliver the latest version of Cradle, and a range of other applications, directly to users' desktops. The Cradle tools and Cradle web UIs will appear in windows on end users' computers, just like any other application that users run locally. But Cradle, and the databases that it is linked to, are all running on a remote server inside the Cradle service hosted by a third-party PaaS provider that you have agreed with 3SL.

So, in summary, the service is:

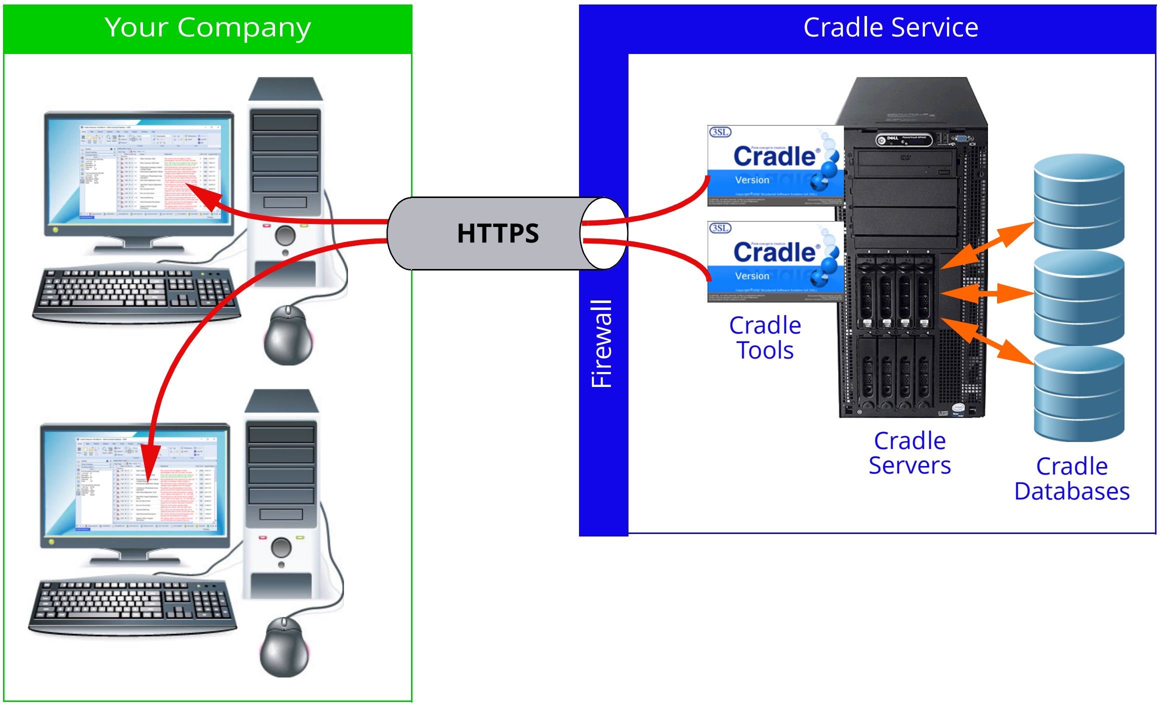


Figure 1: Summary of the Cradle Service

You will use a Cradle system installed on a set of servers that are ***dedicated*** to you. These servers will be hosted in the UK. If you wish, the associated hosting company can be chosen so as to be UK sovereign. The servers will be grouped in a ***Virtual Private Cloud*** (VPC) that will be built by 3SL, see "Service Architecture" on page 20. These servers will be exclusive to you, and any of your customers, suppliers or partners that you want to have access.

The servers will be managed for you by 3SL.

The servers will not be part of any existing tenancy that you may already have with the chosen PaaS provider. This is to ensure that 3SL does not ever need to have access to any of your existing PaaS resources. 3SL does not want to ever have any such access.

3SL will ensure the resilience of the service, using the underlying resilience provided by the Paas provider. This means that you can be assured that the service will always be available, as defined by the SLA (see "Service Level Agreement" on page 51). 3SL will ensure the integrity of your databases, taking regular backups and snapshots. 3SL will restore database backups if you should ever need them, subject to the backup policy agreed in the SLA.

The service includes other pieces of software, such as desktop applications from Microsoft Office, a web browser, a PDF file viewer, and basic text editing tools. These applications will help you to work with the data in your Cradle databases.

Your users will have access to their local and network drives and printers from the service. This means that your users can load information from their local computer or network into Cradle. It also means that any reports, documents or other information produced by Cradle can be easily saved to users' local computer and network drives. If you use the Cradle ***alert*** mechanism in your projects, these alerts can produce e-mails that your users will receive through your corporate e-mail system, in the same way as any other e-mails from the Internet. This will also apply to Cradle users from any of your suppliers and partners who have been given access to the Cradle service. They will receive notification e-mails directly through their organisations' mail systems, in the same way as any other e-mails that they receive from the Internet.

The service includes all of the licensing for Cradle and the third party software and includes all of the licensing and charges for the RDP redirection software (SALs - "Subscriber Access Licences") and the host servers in the VPC. The service is actively managed by 3SL. All of the licensing costs are included in the single per user, per month, charge.

3.1 Lead Users

You will nominate one or more ***lead users*** to 3SL. These are the people who will represent your organisation to 3SL and from whom 3SL will take instructions. The instructions relate to users, locations and databases.

A lead user can send instructions to 3SL to add or remove other lead users. If 3SL is in any doubt, we will seek confirmation from a suitable authority in your organisation, typically someone who has authorised an order or payment to 3SL.

3.2 Users

Your lead users will maintain a list of the people who are to be able to access the service and will send this list of users to 3SL. For each person, 3SL needs to know:

1. The person's gender, so we can send polite e-mails to them
2. Their first or given name
3. Their surname or family name
4. Their e-mail address
5. The location from where they will access the service, see "Locations" on page 17

3SL will safeguard this personal information in the same way that we safeguard all personal data in our possession. You can access our privacy policy here. We are fully compliant with all UK data protection regulations and the EU's GDPR.

3SL will use this information to create a ***service login account*** for each person in your list. These are Windows® login accounts that provide access to the Cradle service. They are ***not*** login accounts for any of your Cradle databases.

Each of your Cradle databases will have its own set of ***Cradle login accounts*** (called ***user profiles*** in Cradle). 3SL will have ***no*** access to the Cradle usernames and passwords in your Cradle databases. You will decide what usernames and passwords will exist in each of your Cradle databases and who will be able to use them.

This creates a clear distinction:

- ***3SL*** will create and maintain users' service login accounts to the Cradle service
- ***You*** create and maintain Cradle login accounts in your Cradle databases

This means that 3SL cannot reset or recover any Cradle logins or passwords.

3.3 Locations

The Cradle service will be hosted on a collection of servers, some of which are exposed to the Internet. Access to these servers will be limited by a ***firewall*** maintained by 3SL.

You must tell 3SL which of your operating ***locations*** may access the Cradle service. You may also include the locations of any of its partners and suppliers who are also to have access to your Cradle service.

Each of these permitted locations must be specified by:

- A name, that you and 3SL will use to communicate with each other
- A range of IP addresses, called a ***CIDR***. 3SL will query any CIDRs with a block size of 64 or more addresses, for example a CIDR such as: `1.2.3.4/26`

You can change these locations from time to time as it wishes.

3.4 Databases

You can have any number of Cradle databases in the Cradle service and can, of course, use these databases in any way that it wishes. These databases, and the information inside them, are private to you and are ***not accessible by 3SL***.

At any time, your lead users can instruct 3SL to create Cradle databases, or delete them, or to restore them from a backup.

The initial deployment of the Cradle service will include sufficient disk space for 500 GBytes of Cradle databases and their backups.

If 3SL determines that your Cradle databases are growing to a point where it would be prudent to add additional disk space to the Cradle service, 3SL will contact you and, with your agreement to any additional charges that may apply, add the extra disk space to the Cradle service.

3.5 Software Provided

The Cradle service includes:

1. The latest version of Cradle
2. The Microsoft Office tools:
   - Word 2016
   - Excel® 2016
   - PowerPoint® 2016

   Office tools, such as Visio® and Project can be provided for an additional fee
3. Web browser, Firefox® latest release. This is only provided to display Cradle's online help and Cradle output generated in HTML. The browser will not have access to the Internet from within the Cradle service.

4. Adobe Acrobat Reader®, latest release
5. Basic text editing tools:
   - NotePad
   - WordPad

3SL will keep these applications updated by applying fixes and security patches when their authors make them available. 3SL will ensure that Cradle is always up to date.

3.6 Backups

The Cradle service includes backups, whose purpose is to allow entire Cradle databases to be returned to their condition at a specific date and time. These backups are not intended to allow the recovery of individual database items or cross references.

We recommend using the ***change history***, ***formal review***, ***baseline***, ***configuration log*** and ***workflow*** mechanisms in Cradle's Configuration Management System (CMS) to ensure that you will have a full record of all changes and actions in your databases over time.

3.6.1 Contents of Backups

The Cradle service includes full backups of all Cradle databases. This means that:

1. The entire database is backed-up as a single entity, and can be restored as a single entity
2. Users' **Personal** scope definitions and the **System** scope definitions are not part of the backups. All other definitions (**User**, **Team**, **User Type**, **Project** and **Automatic** scope) ***are*** included in the backups.

3SL will also arrange daily backups of the Cradle administration and configuration files. These backups will include the **Personal** and **System** scope definitions.

3.6.2 Recovery Point Objective

The recovery point objective (RPO) for all Cradle databases in all subscriptions is 8 hours.

This means that it is not possible to restore one of your databases to its content at any time of your choosing, only to restore that database to its content at a fixed time in the past, which could be up to 8 hours ago.

If necessary, the RPO can be changed after discussion between you and 3SL.

3.6.3 Backup Times

Automated backups of all Cradle databases in all subscriptions will occur daily at 05:00 UTC, 13:00 UTC and 21:00 UTC. You may specify different backup times.

3.6.4 Backup Retention Policy

The backup retention policy specifies how long 3SL will keep each backup of each database:

Table 2: Backup Retention Policy

Retention Period	Backups That are Kept
1 week	05:00, 13:00 and 21:00 backups from each day
Further 2 weeks	21:00 backups from each day
Further 1 month	21:00 backups from Friday of each week
Further 6 months	21:00 backups from last Friday of each month

Backups are deleted as specified by this policy. Deleted backups cannot be recovered.

An alternative way to view this policy is to consider the backups that exist at a point in time. As an example, consider the backups that would exist at the end of 21st September 2022:

Table 3: Retained Backups Example

June 2022

M	T	W	T	F	S	S
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
				21:00		
27	28	29	30			

July 2022

M	T	W	T	F	S	S
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
				21:00		

August 2022

M	T	W	T	F	S	S
1	2	3	4	5	6	7
				21:00		
8	9	10	11	12	13	14
				21:00		
15	16	17	18	19	20	21
				21:00		
22	23	24	25	26	27	28
				21:00		
29	30	31				

September 2022

M	T	W	T	F	S	S
			1	2	3	4
			21:00	21:00	21:00	21:00
5	6	7	8	9	10	11
21:00	21:00	21:00	21:00	21:00	21:00	21:00
12	13	14	15	16	17	18
21:00	21:00	21:00	05:00 13:00 21:00	05:00 13:00 21:00	05:00 13:00 21:00	05:00 13:00 21:00
19	20	21	22	23	24	25
05:00 13:00 21:00	05:00 13:00 21:00	05:00 13:00 21:00				
26	27	28	29	30		

3.6.5 Recovery Time Objective

The recovery time objective (RTO) for any backup of any database is 4 hours.

This means that 3SL will make every effort to restore a backup of any database within the RTO from receiving an instruction from you.

3.7 Cradle Upgrades and Updates

3SL will tell you when a new version of Cradle has been released, and you can decide when it should be installed. The installation will occur in an appropriate maintenance period, see "Maintenance Periods" on page 20.

3.8 Daily Server Restarts

By default, the Cradle Database Server (CDS) will be restarted daily. Your Cradle service will not be available during this service outage:

- The CDS will be stopped at: 23:00 UTC
- The CDS will be started at: 23:05 UTC

This is to allow the demonstration databases **DEMO** and **SYSM** to be reset to their default, as-supplied, content, removing any changes that new users may have made to these databases as part of their introduction to Cradle.

You may change the time of this daily restart, or tell 3SL not to do these restarts at all.

3.9 Maintenance Periods

Your Cradle service will include regular periods for 3SL to install operating system and application updates and fixes. Your Cradle service will not be available:

- From: 15:00 UTC on 3rd Monday in each month
- Until: 17:00 UTC on the same day

These maintenance periods are timed to be after Microsoft releases its security updates.

3SL may not need every one of these maintenance periods.

3SL will notify your lead users in the week before a maintenance period to advise if the maintenance period will occur. **By default, the maintenance period will not occur.** 3SL will send notifications to your lead users ***if, and only if,*** the maintenance period ***will*** occur.

You may postpone or cancel such maintenance periods.

4 Service Architecture

The architecture for your Cradle service is based on 3SL's standard architecture. The general characteristics of the architecture and its use cases are considered first, followed by the details of the architecture.

4.1 Access Vectors

1. The Cradle SaaS service will be housed in a VPC (Virtual Private Cloud) to allow all access to, and by, the VPC to be controlled
2. There is nothing in the Cradle SaaS service that, of itself, attempts external access, not even the VPC's server VMs' (virtual machines) operating systems (so, no internal actors)
3. The Cradle SaaS service cannot look outside its VPC (there is no vector) and so could not access the IT systems of you, or any partner or supplier that has been given access, even if a malicious actor inside the Cradle SaaS tried to get access
4. The Cradle SaaS service will be accessed by you and any of your suppliers and partners. They may initiate connection to the Cradle SaaS service which, if allowed, will create bi-directional communications between the Cradle SaaS service and that user.

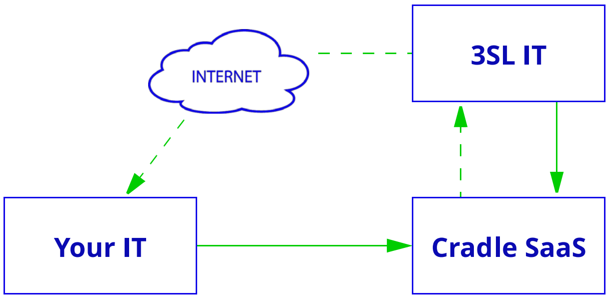


Figure 2: Access Vectors

4.2 Use Cases

4.2.1 Ordinary Cradle Users

The most common use case in which users will use Cradle. The steps will be:

1. A user opens a HTTPS URL in a web browser. This shows a login dialog.
2. The user logs-in to a service login account (see "Users" on page 16), to show a web page containing icons for applications including Cradle and Office. Each icon is a shortcut to a RDP file to serve that application using RemoteApp. There is no remote desktop.
3. The user clicks an icon to start an application, a Windows authentication may be needed
4. The application starts, such as Cradle WorkBench
5. The user logs-in to a Cradle database using a Cradle login account created by you
6. By default, the application will have access to the filesystems and printers:
   a) Local to the user's desktop/laptop
   b) Accessible in your LAN / WAN from the user's desktop/laptop

These forms of access are essential as it is the means by which users can:

- Load data into Cradle from documents, spreadsheets and other tools' output data
- Have wider access to reports, matrices, graphs, diagrams, metrics, dashboards and documents that are published from Cradle

4.2.2 E-Mail Notifications

Cradle has databases containing your sets of ***items***, connected by your ***links***, both with ***workflows*** that you have defined. Events can occur in these workflows, such as items being edited or links being created or changed. If you wish, these events can be notified by ***alerts***. If so, you can choose that these alerts are delivered by e-mail.

In this case, Cradle will create an e-mail, with a format and content optionally controlled by you, and send this e-mail via a relay inside the Cradle SaaS architecture, to the 3SL mail server at `mail.threesl.com`. In turn, the 3SL mail server will relay the e-mail to your organisation's mail servers which will receive it from address `noreply@threesl.com` addressed to the publicly-known e-mail addresses of all of the intended recipients working in the Cradle database, that is, a set of addresses each of the form: `aaa.bbb@you.gov.uk`

The e-mails sent by Cradle and relayed (twice) by Cradle and 3SL, will be received over the public Internet by your organisation in exactly the same manner that your receive all e-mails over the public internet. There will be no use of PSN or any other Government network.

The receipt of these e-mails by your mail server from the 3SL mail server, all sent to public e-mail addresses, is the only vector by which the Cradle SaaS architecture can initiate any contact to you, or your organisation.

This use case is optional. It is a matter for you whether it is used, or not.

4.2.3 Cradle Web Users

Cradle provides web-only UIs in which users can interact with Cradle databases using a web browser instead of a Cradle tool. You can create your own, custom, web UIs if you choose a Cradle service that includes this Web Access capability.

You may prefer that some of your users, potentially including your suppliers and partners, should access the information in your Cradle database(s) using these custom web UIs.

These users will connect to the Cradle SaaS subscription from a web browser over a HTTPS connection. They will not authenticate to the Windows SaaS environment. They will only authenticate directly with Cradle. The steps will be:

1. A user opens a URL in a web browser to show your custom web UI with a login dialog
2. The user logs-in to a Cradle database using a Cradle login account created by you

There is no ability for such a web user to provide Cradle with access to the user's local or network resources through this web connection.

4.3 SaaS Architecture

The service architecture to support all of the use cases in the previous section is:

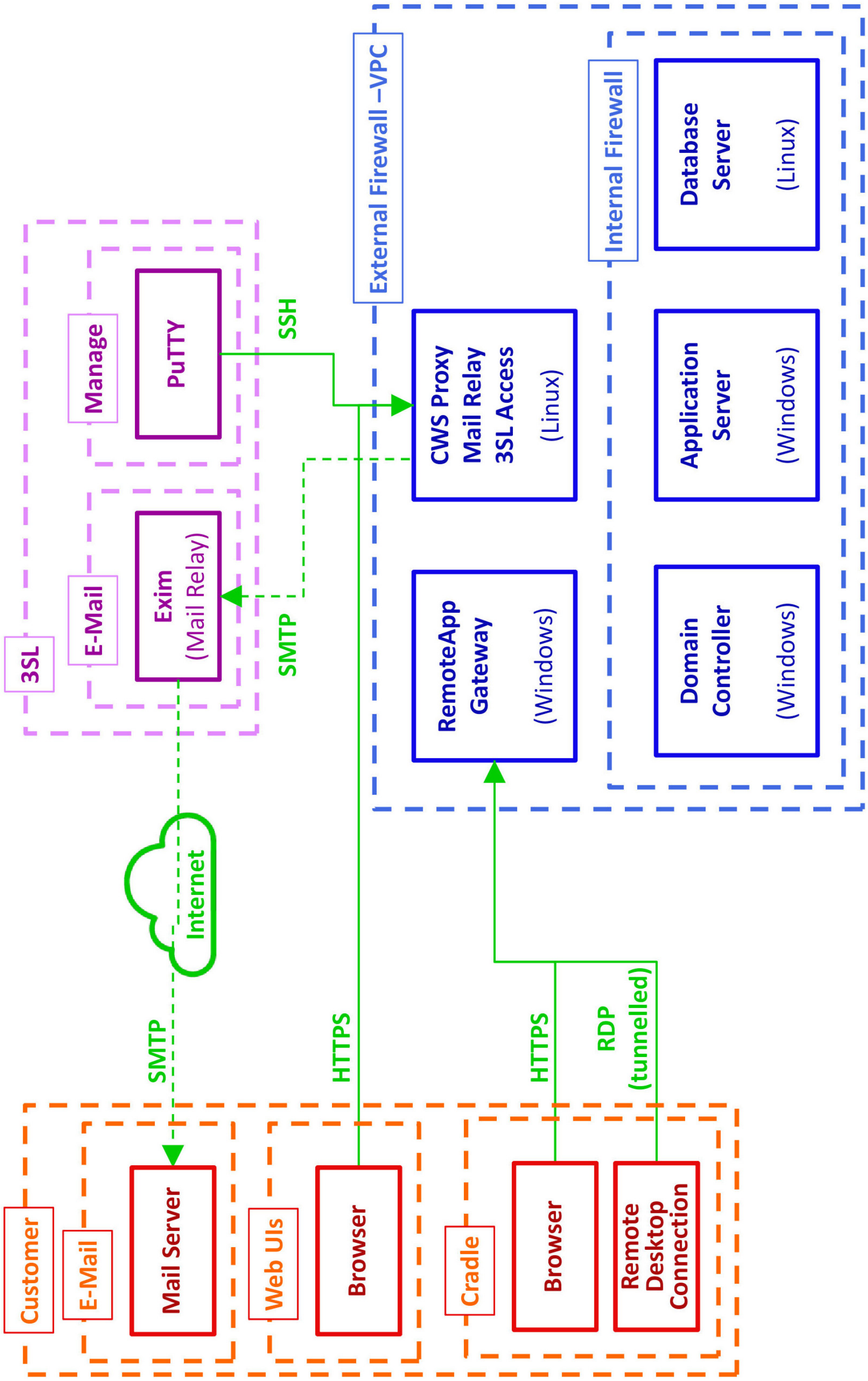
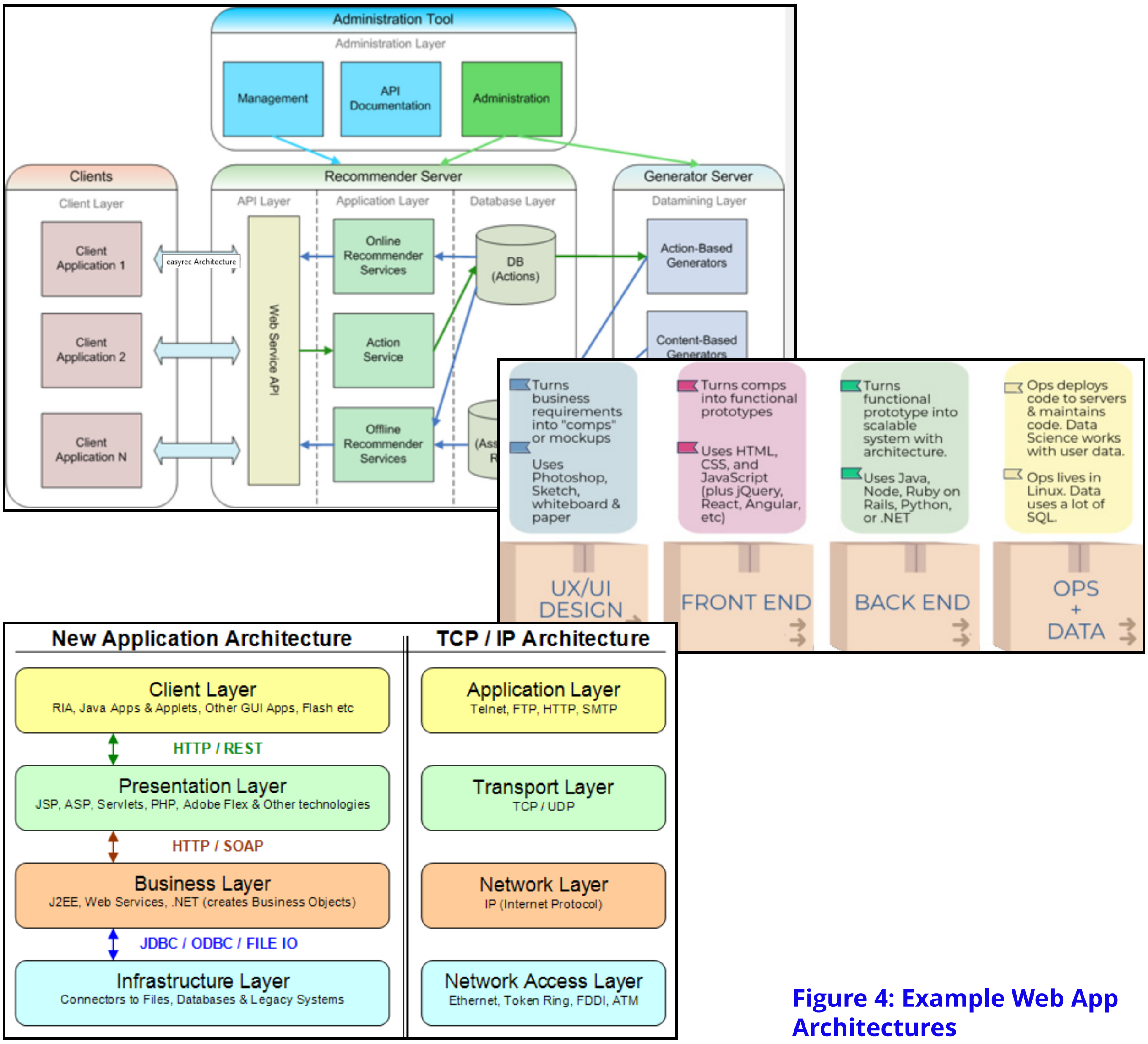


Figure 3: Cradle Service Architecture

4.4 Web Architecture

Cradle databases can be accessed from web browsers connected to the Cradle Web Server (CWS) over HTTP or HTTPS. 3SL provides some example web UIs. Customers can define their own ***custom web UIs*** and control which users can use the web UIs and the IP address ranges from where the web UIs can be used. You can use this facility to build its own web UIs.

There are many ways to build web applications, often using layers of software called a ***web stack*** or an ***application stack***. The layers may reflect a design approach (such as services, RESTful WSIs, SOAP and others), a specific web UI toolkit (such as Angular, Bootstrap, Electron and others), or an implementation language or environment (such as PHP, Javascript, C#, .NET, Java and others). For example:



Turns business requirements into "comps" or mockups

Uses Photoshop, Sketch, whiteboard & paper

Turns comps into functional prototypes

Uses HTML, CSS, and JavaScript (plus jQuery, React, Angular, etc)

Turns functional prototype into scalable system with architecture.

Uses Java, Node, Ruby on Rails, Python, or .NET

Ops deploys code to servers & maintains code. Data Science works with user data.

Ops lives in Linux. Data uses a lot of SQL.

New Application Architecture	TCP / IP Architecture
Client Layer RIA, Java Apps & Applets, Other GUI Apps, Flash etc	Application Layer Telnet, FTP, HTTP, SMTP
HTTP / REST	
Presentation Layer JSP, ASP, Servlets, PHP, Adobe Flex & Other technologies	Transport Layer TCP / UDP
HTTP / SOAP	
Business Layer J2EE, Web Services, .NET (creates Business Objects)	Network Layer IP (Internet Protocol)
JDBC / ODBC / FILE IO	
Infrastructure Layer Connectors to Files, Databases & Legacy Systems	Network Access Layer Ethernet, Token Ring, FDDI, ATM

Figure 4: Example Web App Architectures

The Cradle web architecture is very different:

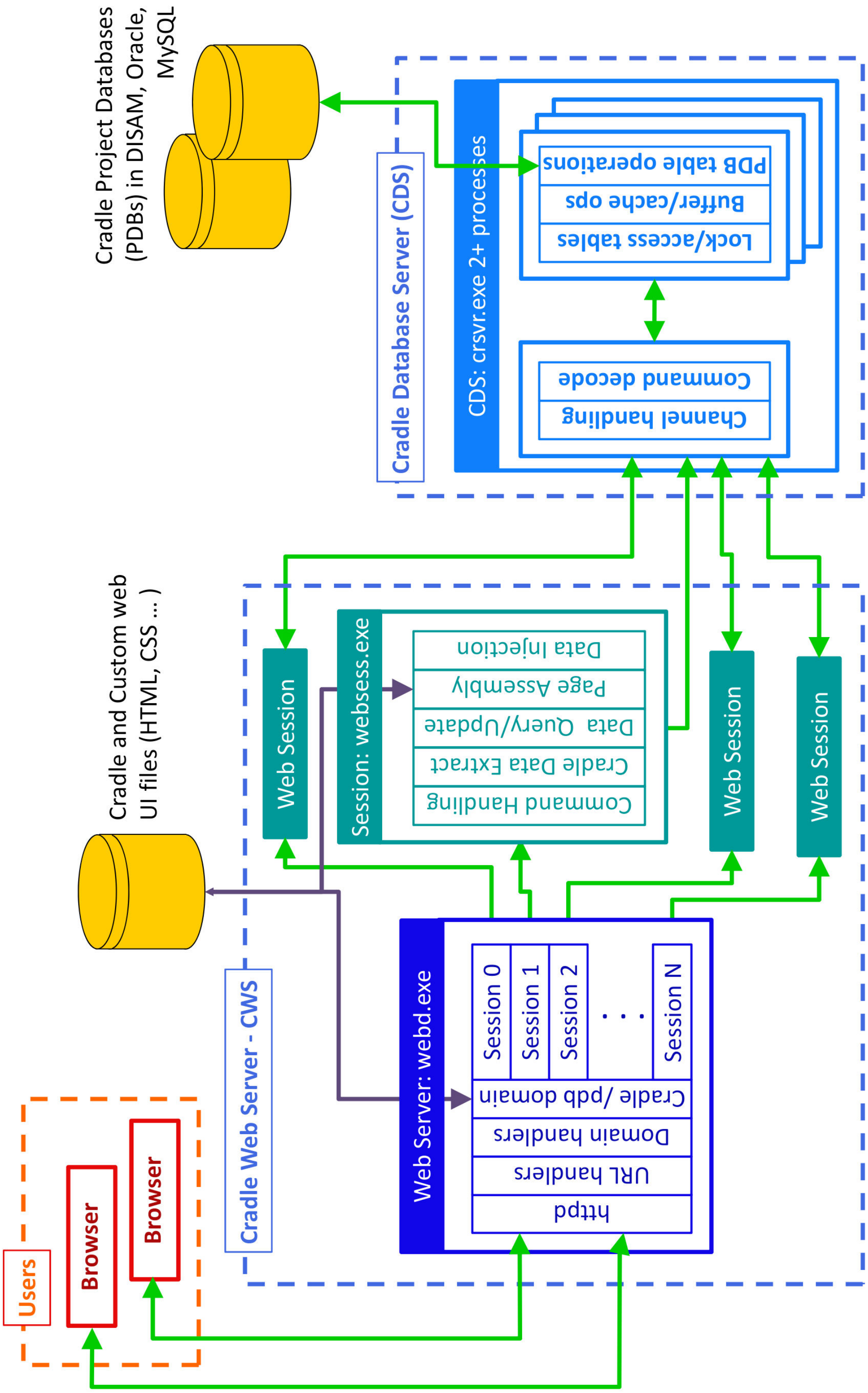


Figure 5: Cradle Web App Architecture

- It is not general purpose, it can only interact with the Cradle Database Server (CDS)
- The majority of it is written by 3SL

- The majority of it is written in C, so it is deployed as compiled binary code
- There is no direct coupling between the web UI and the database back-end

The Cradle web application architecture brings several benefits:

1. **Most code in each layer of a Cradle architecture web UI is Cradle-focused 3SL code**
   You have no need to write or understand code at each layer. In other architectures, you must understand, correctly configure, manage, and identify and then mitigate risks for, complex application brokers and/or web servers, and/or service managers.
2. **The 3SL codebase in each layer of the Cradle architecture is small and fully used**
   In other architectures, you will only use small parts of large packages of third party code (such as Nginx, Apache, Tomcat, AngularJS, Docker). This exposes you to increased risk from indirect effects of errors in pieces of code that are irrelevant to you.
3. **Most of the code in the Cradle web architecture is compiled**
   In other architectures, malicious actors can easily compromise any of the code in these large and complex third party packages using only a simple text editor. Such hacks are unlikely to be detected. In contrast, it is virtually impossible to hack the binary code in the Cradle web architecture and very obvious if it is attempted.

These differences can be pictured:

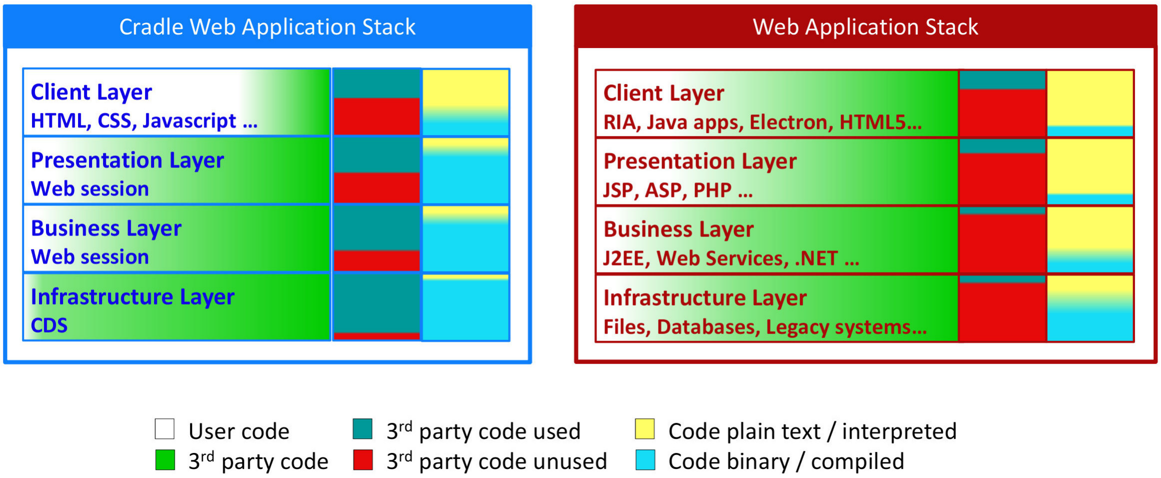


Figure 6: Cradle vs Typical Web Applications

The Cradle web application architecture makes Cradle web UIs inherently immune to a wide range of attack vectors that affect web UIs built with typical architectures. Vectors such as ***code injection*** and ***cross-site scripting*** are impossible. This mitigates or eliminates a wide range of the risks described in “OWASP Top 10 Web UI Risks” on page 37.

As a simple example, SQL code injection is impossible in a Cradle web UI since:

- Cradle never executes anything entered by a user into any UI, web or otherwise
- Everything entered into a Cradle web UI is used solely and strictly as data values
- Cradle does not use SQL, nor does it directly use a RDBMS

5 Information Assurance

5.1 General

3SL has partnered with Cloud Hosting providers including FCO Services, UK Cloud, UK Fast, Amazon Web Services (AWS) and OVH to ensure that 3SL's Cloud Software products are compliant with all information assurance requirements for unclassified data (Unassured Cloud services, formerly known as IL0), and for data that is classified OFFICIAL and OFFICIAL SENSITIVE (Accredited Public Cloud services, formerly known as IL3).

Unclassified data can be provided from cloud services over PSN and the Internet. OFFICIAL data that warrants assurance corresponding to IL3 can be provided from cloud services over PSN. All such services can have Pan Government Accreditation (PGA) for the underlying Cloud Hosting and full accreditation for the Cradle Cloud Software.

All our Cloud Hosting providers' datacentres are highly resilient Tier 3 and are UK-resident, UK-sovereign, or both.

3SL will manage all servers that provide the **3SL Cradle** service and ensure that all security patches to Windows, Office and the other applications are installed no later than 1 week after they become available.

5.2 Technology Code of Practice

The Technology Code of Practice is a set of criteria to help government design, build and buy technology and, as such, is directly relevant to all SaaS services provided through the Digital Marketplace. It is used as a cross-government agreed standard in the spend controls process. The Technology Code of Practice is part of the Transformation Strategy 2017-2020 and the Local Digital Declaration.

Following the Technology Code of Practice is intended to help you to introduce or update technology so that it:

- Meets user needs, based on research with your users
- Is easier to share across government
- Is easy to maintain
- Scales for future use
- Is less dependent on single third-party suppliers
- Provides better value for money

There are 12 elements to the Technology Code of Practice. The **Cradle SaaS** service is **Compliant** with 7 of the 12 elements. The remaining 5 elements are rated **Not Applicable**.

There are no non-compliances. The details are:

Table 4: Code of Practice Compliance

#	Details	
1	Name	**Define user needs**
	Summary	Understand your users and their needs. Develop knowledge of your users and what that means for your technology project or programme.
	Cradle SaaS	**Compliant** The needs are for your users and, at your option, selected suppliers and partners, to have access to information in Cradle using a choice of non-web UIs and custom web-based UIs in a manner that provides acceptable performance and control for all users, whilst being consistent with all other Governmental constraints (as detailed in the tables in this section.
2	Name	**Make things accessible and inclusive**
	Summary	Make sure your technology, infrastructure and systems are accessible and inclusive for all users.
	Cradle SaaS	**Compliant** The UIs in all Cradle software, including 3SL-supplied Cradle web UIs, are section 508 (and hence WCAG 2.1) compliant and, as such, can be crawled by assistance technology so as, for example, to be rendered in audio for visually impaired users. You can ensure similar capability in any custom web UIs that you may choose to create.
3	Name	**Be open and use open source**
	Summary	Publish your code and use open source software to improve transparency, flexibility and accountability.
	Cradle SaaS	**Not Applicable** Cradle is 3SL's commercial product and contains 3SL intellectual property. 3SL complies with all licence requirements for any and all open source software that is included in Cradle, for example in relation to statements of inclusion of open source software and mandatory re-distribution of that open source software. All open source software used in Cradle (such as Tcl, Tk and regex libraries) do not have any restrictions on their use in commercial products and most do not make any demands of 3SL for disclosure or redistribution of original and/or modified source files.
4	Name	**Make use of open standards**
	Summary	Build technology that uses open standards to ensure your technology works and communicates with other technology, and can easily be upgraded and expanded.
	Cradle SaaS	**Not Applicable** Cradle is 3SL's commercial product that contains 3SL intellectual property. Cradle supports a range of open standards where this is helpful for users, for example for import, export and data encoding and formatting standards such as CSV, TSV, RTF, XML, HTML, ReqIF and JSON.
5	Name	**Use cloud first**
	Summary	Consider using public cloud solutions first as stated in the Cloud First policy.
	Cradle SaaS	**Compliant** The Cradle SaaS service is delivered using your choice of public or assured cloud PaaS platforms from your choice of the UK-resident and/or UK-sovereign PaaS providers that 3SL can provide.

Table 4: Code of Practice Compliance (continued)

#	Details	
6	Name	**Make things secure**
	Summary	Keep systems and data safe with the appropriate level of security.
	Cradle SaaS	**Compliant** The Cradle SaaS service may hold information up to OFFICIAL - SENSITIVE. The Cradle SaaS service has been implemented to be compliant with the NCSC Cloud Security principles, see “NCSC Cloud Security Principles” on page 31 and, in particular for the Technology Code of Practice: 1. **Data encryption** All data in transit and at rest is encrypted 2. **Single sign-on** No, as would create an unwise link between your internal authentication (if any) and an external, third party, authentication system - the Cradle SaaS server managed by 3SL. You may wish to develop a centralised authentication system that will be referenced by individual SaaS systems. As such, 3SL confirms that we have a long-term goal to migrate SaaS systems towards SAML and external authentication mechanisms. 3. **Two-factor authentication (2FA)** Not considered necessary. Note that two authentication stages are needed to access your data through Cradle tools. 4. **Fine-grained access control** Under your sole control within Cradle itself. This can control which user(s) have NA, RO or RW access to each attribute in each item and to each link between items. 5. **Usage monitoring and alerts** The Cradle SaaS service maintains logs of logins, both to Windows and to Cradle itself. Cradle itself maintains logs of all changes to every item and link, to every CM-related action, and to all baselines and formal change operations. 6. **Timely patching** 3SL will apply patches to the PaaS (such as Windows and Linux operating systems) and SaaS elements (such as Cradle and Microsoft Office) during regular maintenance updates whose timing and frequency will be agreed with you.
7	Name	**Make privacy integral**
	Summary	Make sure users rights are protected by integrating privacy as an essential part of your system.
	Cradle SaaS	**Compliant** The Cradle SaaS service will not hold any personal data. In the unlikely event that you decide that the Cradle SaaS service is to hold information that is personal to identifiable individuals, then you can use the access control mechanisms in the Cradle software to ensure that access to this information is limited to appropriate users. Such controls are solely within your control since only you will have administrative access into your Cradle database(s) in the Cradle SaaS service.
8	Name	**Share, reuse and collaborate**
	Summary	Avoid duplicating effort and unnecessary costs by collaborating across government and sharing and reusing technology, data, and services.
	Cradle SaaS	**Not Applicable** You can collaborate with any other Government department or agency or external entity to which you grant access to your Cradle SaaS service, or if they grant access to you to their Cradle SaaS service. Common processes, templates, techniques, approaches and other meta data can be easily shared and reused. You can share data if you wish by export/import.

Table 4: Code of Practice Compliance (continued)

#	Details	
9	Name	**Integrate and adapt technology**
	Summary	Your technology should work with existing technologies, processes and infrastructure in your organisation, and adapt to future demands.
	Cradle SaaS	**Not Applicable** You cannot integrate with any existing technology, process or infrastructure as its objective is to use Cradle as SaaS and there are no Cradle SaaS services that you can access that will meet your security requirements, see the “NCSC Cloud Security Principles” on page 31.
10	Name	**Make better use of data**
	Summary	Use data more effectively by improving your technology, infrastructure and processes.
	Cradle SaaS	**Compliant** We would expect that the Cradle SaaS service will hold information vital to your future plans and facilities. The Cradle SaaS service has been implemented to be compliant with the NCSC Cloud Security principles, see “NCSC Cloud Security Principles” on page 31 and, in particular for the Technology Code of Practice: 1. **Save time and money, by reusing open data that is already available** Any relevant data can be included inside your Cradle databases. 2. **Make sure infrastructure and services contain consistent information** Cradle allows information to be linked to ensure traceability, coverage and consistency. By linking, Cradle allows information to be defined once and used many times, thereby guaranteeing consistency. 3. **Give your users a more consistent experience when using government services online, which builds trust** You can provide users with a customised experience using Cradle’s mechanisms for: • Start pages • Phase hierarchy • Custom web UIs 4. **Minimise data collection and duplication** Duplicative information can be found and removed. Information can be reused by linking to it from all places where it is to be referenced. 5. **Make datasets interoperable which will increase opportunities for data use** All information in Cradle can be exported in any desired format, including CSV, TSV, RTF, XML, HTML, ReqIF and JSON helping it to be shared with others who need to use it.
11	Name	**Define your purchasing strategy**
	Summary	Your purchasing strategy must show you’ve considered commercial and technology aspects, and contractual limitations.
	Cradle SaaS	**Compliant** The Cradle SaaS service would be reviewed through your control procedures so as to ensure its procurement meets all of your local and wider Governmental purchasing requirements and is as cost effective for your organisation as possible. The Cradle SaaS service: • Will bring long term financial savings by reduced in-house IT costs • Is a contract that has been disaggregated from other agreements • Has a clearly defined contract exit, the off-boarding process provided by 3SL • Helps with the transition to the cloud by being SaaS • Has a short contract term determined by you, probably annual, with a streamlined renewal process • Is clearly defined in 3SL’s SaaS user documentation so you have a clear understanding of the service deployment, operation, maintenance and termination

Table 4: Code of Practice Compliance (continued)

#	Details	
12	Name	**Meet the Service Standard**
	Summary	If you're building a service as part of your technology project or programme you will also need to meet the Service Standard.
	Cradle SaaS	**Not Applicable** In your consideration of Cradle, you are not building a service. Your consideration is rather to potentially purchase the Cradle SaaS service from 3SL and to use it to assist in the progression of your product and/or service and/or EA / BA activities.

5.3 NCSC Cloud Security Principles

There are 14 NCSC Cloud Security Principles. The Cradle SaaS service is **Compliant** with all 14 principles. There are no **Not Applicable** principles and no non-compliances. The details of the compliances are:

Table 5: NCSC Principle Compliance

#	Details	
1	Name	**Data in transit protection**
	Summary	User data transiting networks should be adequately protected against tampering and eavesdropping.
	Cradle SaaS	**Compliant** All data is sent encrypted through HTTPS. All data is sent over the public Internet or PSN. Depending on how many locations you want to have access, and whether these locations' IP addresses are subject to change, it may be decided to place the service into a VPN to which users must first connect before they can access the service over HTTPS.
2	Name	**Asset protection and resilience**
	Summary	User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.
	Cradle SaaS	**Compliant** All data will be held and processed in a UK-resident data centre of whichever PaaS provider you prefer from the range that 3SL offers. These data centres are already accepted as providing acceptable security by UK Government departments / agencies. All data at rest will be held in encrypted drives that are exclusive to the Cradle SaaS service. If you terminate the service, you will remove appropriate data from the service with 3SL's assistance and then all data backups and server snapshots in the service will be destroyed.

Table 5: NCSC Principle Compliance (continued)

#	Details	
3	Name	**Separation between users**
	Summary	A malicious or compromised user of the service should not be able to affect the service or data of another.
	Cradle SaaS	**Compliant** The Cradle SaaS service is delivered from a dedicated VPC (virtual private cloud) in your choice of PaaS. The implementation of VPCs is such that your VPC cannot be accessed by any user of other Cradle SaaS services. As such, all users of the Cradle SaaS service are separated from all other users of all other cloud services. The Cradle SaaS is only accessible from specific locations (IPs/CIDRs) through a firewall that is external to the VPC and is managed by 3SL. All users of the Cradle SaaS must authenticate to the service, to either or both of: • A Windows domain managed by 3SL • A set of Cradle login accounts for each of a set of Cradle databases, all managed by you The ability of a malicious or compromised user who has accessed the Cradle SaaS service from an approved location and who has authenticated successfully, is subject to the access controls that you implement in your Cradle databases. It is impossible for a malicious or compromised member of 3SL to access the contents of any of your Cradle databases unless you have chosen to give 3SL access. In such cases, this access is subject to the access controls that you implement in your Cradle databases.
4	Name	**Governance framework**
	Summary	The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.
	Cradle SaaS	**Compliant** The Cradle SaaS service is provided using the procedures described in “Security Governance Framework” on page 48. 3SL asserts that this is an acceptable framework as it meets the NCSC guidance by providing: 1. **A clearly identified person who is responsible for the security of the cloud service.** This is 3SL’s Director: Mark Walker 2. **A documented framework for security governance, with policies governing key aspects of information security relevant to the service.** These policies are described in “Security Governance Framework” on page 48 3. **That security and information security are part of the service provider’s financial and operational risk reporting mechanisms.** The security and integrity of 3SL’s SaaS services appears in 3SL’s corporate risk register that is reviewed as required by 3SL’s ISO9001 processes and corrective action taken as necessary with all possible speed. 4. **Processes to identify and ensure compliance with applicable legal and regulatory requirements.** 3SL receives legal advice monthly from specialist third parties.

Table 5: NCSC Principle Compliance (continued)

#	Details	
5	Name	**Operational security**
	Summary	The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.
	Cradle SaaS	**Compliant** The Cradle SaaS service will be managed by 3SL as described in “Security Governance Framework” on page 48. These ensure a well managed service, and specifically: 1. **Configuration and change management** The details of, and timing of, all changes to the Cradle SaaS service will be agreed with you. All changes will be tested and approved by 3SL before the service is released back to you. Changes will be software upgrades and changes to the users, locations and databases in the service. Testing of all such changes is very simple and back-outs are equally straightforward, typically to restore what existed before the change. 2. **Vulnerability management** 3SL will become aware of all security issues identified in any components of the Cradle SaaS service by e-mail alerts from their respective authors. These will be vulnerabilities in operating systems and application software. 3SL will mitigate / remove all such vulnerabilities as changed, see above. 3. **Protective monitoring** 3SL will monitor all attempted accesses to the Cradle SaaS service, particularly those that failed either at the external firewall or Windows service account authentication. 3SL will also monitor login failures to the Cradle software in the service. All such attacks on the service will be reported to you. 4. **Incident management** 3SL can restore the Cradle SaaS service to a working condition from all types of failure: • PaaS failures • VM failures • Firewall failures • Windows / Linux operating system crashes or other failures • Cradle or third party software failures • Cradle database corruption • Unintended loss of data by user error The RPO (recovery point objective) and RTO (recovery time objective) will be agreed with you for all such failures, see “Service Level Agreement” on page 51
6	Name	**Personnel security**
	Summary	Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.
	Cradle SaaS	**Compliant** 3SL personnel and the PaaS provider personnel will have no access to your data in the Cradle SaaS service. The only people who will have access to your data in the Cradle SaaS service will be those people to whom you grant access by: • The provision of a Cradle login account in one or more of your Cradle databases • Configuring the Cradle login accounts with the skills, privileges and team membership needed to allow access to appropriate items and links in these database(s)

Table 5: NCSC Principle Compliance (continued)

#	Details	
7	Name	**Secure development**
	Summary	Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.
	Cradle SaaS	**Compliant** You can have confidence in the security of the development of the Cradle SaaS service and the software deployed within it: 1. **New and evolving threats are reviewed and the service improved in line with them.** 3SL is aware of new and changing threats to the technologies in the Cradle SaaS service and will update these technologies as necessary. An example is when 3SL upgraded from SSL and TLS 1.0 based secure connections to TLS 1.2 and later. 2. **Development is carried out in line with industry good practice regarding secure design, coding, testing and deployment** 3SL designs and develops Cradle using industry good practice and in a way that ensures the integrity of the Cradle software. Further details are available in the 3SL white paper "Information Assurance", 3SL document number RA003. 3. **Configuration management processes are in place to ensure the integrity of the solution through development, testing and deployment.** See 2 above. All 3SL development is controlled by a professional grade development process and configuration controlled source code repository - Subversion.
8	Name	**Supply chain security**
	Summary	The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.
	Cradle SaaS	**Compliant** Other than the PaaS provider, 3SL does not use any third parties to deliver the Cradle SaaS service to you. Therefore there is no supply chain whose security principles need to be managed.
9	Name	**Secure user management**
	Summary	Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.
	Cradle SaaS	**Compliant** 3SL identifies lead users as the persons who may instruct 3SL to administer the Cradle SaaS service, see "Lead Users" on page 16 1. **Authentication of users to management interfaces and support channels** a) **You are aware of all of the mechanisms by which the service provider would accept management or support requests from you (telephone phone, web portal, e-mail etc.)** The lead users, see "Lead Users" on page 16 b) **Only authorised individuals from your organisation can use those mechanisms to affect your use of the service (Principle 10 can help you consider the strength of user identification and authentication in each of these mechanisms)** The lead users, see "Lead Users" on page 16

Table 5: NCSC Principle Compliance (continued)

#	Details	
		2. **Separation and access control within management interfaces** a) **have confidence that other users cannot access, modify or otherwise affect your service management** 3SL will only respond to lead users. If 3SL is unsure of a user's authority, 3SL will only accept the authority of someone who has demonstrated they have financial authority as well as technical authority. For example, users who are named on a customer Purchase Order (PO). b) **manage the risks of privileged access using a system such as the 'principle of least privilege'** You have sole control of the privileges and roles of Cradle user profiles (login accounts) in Cradle databases and therefore it is only you who can control which items and links in the database are accessible to any given user. c) **understand how management interfaces are protected (see Principle 11) and what functionality they expose** All management interfaces to the Cradle SaaS service are managed by 3SL. 3SL will only respond to lead users. You have sole control of the privileges and roles of all Cradle users and therefore it is only you who can control which Cradle users are able to perform administration in Cradle database.
10	Name	**Identity and authentication**
	Summary	All access to service interfaces should be constrained to authenticated and authorised individuals.
	Cradle SaaS	**Compliant** All access to the Cradle SaaS service is constrained by access being: 1. Only permitted from IPs / CIDRs that you have specified to 3SL 2. Only permitted using usernames and passwords to Windows logins that have been created by 3SL acting on instructions from you 3. Only permitted by second Cradle usernames and passwords to Cradle database logins
11	Name	**External interface protection**
	Summary	All external or less trusted interfaces of the service should be identified and appropriately defended.
	Cradle SaaS	**Compliant** There are no separate interfaces to the Cradle SaaS service. All identity and authentication is as specified for element **10** above.
12	Name	**Secure service administration**
	Summary	Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.
	Cradle SaaS	**Compliant** Only 3SL can administer the Cradle SaaS service as only 3SL can access the service through the administrative interfaces, such as: 1. The PaaS infrastructure that provides access to the VMs inside the VPC and to the external firewall (the security groups in AWS and the firewall rules in OVH) 2. PuTTY terminal / shell access over SSH. Authentication is based on certificates in password-protected `.ppk` files which supplement the IP/CIDR access restrictions 3. Access to Windows desktops on the windows servers - the Domain Controller, the Application Server and the RemoteApp Gateway

Table 5: NCSC Principle Compliance (continued)

# Details

4. User accounts that have administrative rights. Only 3SL has access to administrative privileges in the VMs.

Even so, since 3SL does not have administrative access into any Cradle database, only you have access to the Cradle login accounts that have full Cradle administrative rights, such as the user **MANAGER**.

3SL recommends that you create and use a user **MGR** in each database. This account has all Cradle privileges except **ACCESS_BYPASS** so accidental deletion of data is far less likely.

The Cradle SaaS service is managed using a model that does not exist within the NCSC principles. The service is managed using login accounts specific to 3SL from any authorised external IP/CIDR which gives access to an administrative environment (such as a Windows desktop and Linux shell and `sudo` rights) that are not available to you or any other user. Once into this administrative environment, 3SL users can gain the additional administrative rights that they need, typically by assuming other administrative user identities, such as Linux `sudo`.

With reference to the NCSC principles:

1. **End user devices used for management of services are incredibly valuable targets to an attacker, so it's vital that you protect them. We recommend you build upon our End User Devices Security Guidance but go further to protect the integrity of those devices.**
   This does not apply to the Cradle SaaS service since it is the 3SL logins that are special, combined with the administration environment that only these logins can use and the elevated administrative accounts that are accessed once inside the administration environment.
2. **In particular, administrators should:**
   a) **Have separate user accounts for administration and normal user activities. They should not use their administration accounts for normal business activities. This reduces the exposure of privileged accounts and reduces their risk of compromise.**
   This is the approach used in the Cradle SaaS environment, all logins are to unprivileged accounts

   b) **Not be able to browse the internet or open their external e-mail in the same processing context as they manage systems. To do so would mean that a successful spear-phishing or watering-hole attack against an administrator would yield access to their system in the same context that the administrator can perform their privileged duties.**
   This is the approach used in the Cradle SaaS environment.
   From within the VPC it is not possible to connect to anything outside the VPC. So no user, you or 3SL, can use a web browser or e-mail or connect to any external host.

   c) **Be strongly authenticated before being able to carry out any service management functions.**
   This is the approach used in the Cradle SaaS environment.
   Authentication is by originating IP / CIDR and username/password and keypair to access an account from where a further username/password provides access to an administrative environment.

Table 5: NCSC Principle Compliance (continued)

#	Details	
13	Name	**Audit information for users**
	Summary	You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.
	Cradle SaaS	**Compliant** The Cradle SaaS service provides a wide range of logging that allows 3SL to detect any malicious activity directed to the service from outside. These logs include: • All accesses to the Cradle SaaS environment are logged by the PaaS environment • All attempted Windows logins to the Cradle SaaS environment are logged by Windows • All launch of applications over RDP is logged by RDP services • All starts of Cradle tools, including connections from web browsers to the Cradle Web Server, are logged by the Cradle Database Server • All attempted logins to Cradle, either Cradle tools or custom web UIs, are logged • If you wish, all user actions, including all interactions with items and links, can be logged using the External Command Interface • If you wish, every edit and change to the links to/from each item can be logged in that item’s change history • If you wish, all actions related to items workflows can be logged • If you wish, all CM-related actions and events can be logged, including all reviews of items and links • If you wish, all changes to baselined information can be formalised using Change Request (CHR) items and Change Task (CHT) items whose evolution can be logged
14	Name	**Secure use of the service**
	Summary	The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.
	Cradle SaaS	**Compliant** 3SL is responsible for the overall CIA (confidentiality, integrity and availability) of the Cradle SaaS service. You are responsible for all legitimate, authorised, user actions inside all Cradle databases.

5.4 OWASP Top 10 Web UI Risks

The Open Web Application Security Project (OWASP) is an international group interested in web application security. More details are in their website here. The “OWASP Top 10” is a list of what they consider the most critical security concerns for web application security.

Cradle has a capability where the Cradle Web Server (CWS) can serve any number of user-defined ***custom web UI*** to different groups of users. Users can create their own web UI to add to, or replace, the example web UIs provided by 3SL. Custom web UIs may or may not be relevant to you.

The Cradle SaaS service is **Compliant** with 8 of the 10 risks in the OWASP Top 10 risk list and

Mostly Compliant with the remaining 2 risks, as shown in 3SL's assessment of Cradle's web UI capability against the list:

Table 6: OWASP Top 10 Compliance

#	Details	
1	Name	**Injection**
	Summary	Injection attacks happen when untrusted data is sent to a code interpreter through a form input or some other data submission to a web application. For example, an attacker could enter SQL database code into a form that expects a plain text username. If that form input is not properly secured, this would result in that SQL code being executed. This is known as an SQL injection attack. Injection attacks can be prevented by validating and/or sanitising user-submitted data. (Validation means rejecting suspicious-looking data, while sanitisation refers to cleaning up the suspicious-looking parts of the data.) In addition, a database admin can set controls to minimize the amount of information an injection attack can expose.
	Cradle SaaS	**Compliant** Cradle has measurers to prevent injection of untrusted data at the client level, web server level and at the web application level. Injection of such data would have no effect as there is no processing of input data that could be compromised by such injections. **An application is vulnerable to this attack when:** • **User-supplied data is not validated, filtered, or sanitised by the application.** **Not vulnerable**. Cradle has measurers to prevent injection of untrusted data at the client level, web server level and at the web application level. Data Injection ineffective as there is no data processing that could be compromised, for example, no command driven RDBMS, whether SQL or other. • **Dynamic queries or non-parametised calls without context aware escaping are used directly in the interpreter.** **Not vulnerable**. Cradle does not allow non-parametised calls. Input fields' contents are always escaped and being checked for input that could be used for injection. • **Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records.** **Not vulnerable**. There is no command-driven RDBMS, SQL or other, and no user input is used to control or specify actions in Cradle databases. • **Hostile data is directly used or concatenated, such that the SQL or command contains both structure and hostile data in dynamic queries, commands, or stored procedures.** **Not vulnerable**. There is no command-driven RDBMS, SQL or other, and no user input is used to control or specify actions in Cradle databases.
2	Name	**Broken Authentication**
	Summary	Vulnerabilities in authentication (login) systems can give attackers access to user accounts and even the ability to compromise an entire system using an admin account. For example, an attacker can take a list containing thousands of known username/password combinations obtained during a data breach and use a script to try all those combinations on a login system to see if there are any that work. Some strategies to mitigate authentication vulnerabilities are 2-factor authentication (2FA) and limiting or delaying repeated login attempts using rate limiting.

Table 6: OWASP Top 10 Compliance (continued)

#	Details	
	Cradle SaaS	**Mostly Compliant** Cradle's username/password authentication has many security capabilities: • Limit of 3 consecutive failed login attempts • Ability to ensure strong passwords (length, content, regex pattern) • Prevent password repetition (password cycles) • Enforce password ageing We provide new random session IDs linked to the connecting client. These session IDs are invalidated after logout, idle, and absolute timeouts **Confirmation of the user's identity, authentication, and session management are critical to protect against authentication-related attacks.** **There may be authentication weaknesses if the application:** • **Permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords.** **Not vulnerable**. Impossible, limit on number of failed logins. • **Permits brute force or other automated attacks.** **Not vulnerable**. Impossible, limit on number of failed logins. • **Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin".** **Not vulnerable** as Cradle can enforce strong passwords, password cycles and ageing. • **Uses weak or ineffective credential recovery and forgot password processes, such as "knowledge-based answers", which cannot be made safe.** **Not vulnerable**. No passwords are stored at an application level. Every available mechanism to prevent web browsers remembering usernames and passwords has been used. There is no 'forgot password' recovery mechanism. There is no 'password hints' mechanism. • **Uses plain text, encrypted, or weakly hashed passwords (see A3:2017-Sensitive Data Exposure).** **Vulnerable** as web UIs are zero thickness (no local processing) usernames and passwords are sent in plain text. Hence HTTPS is used by the Cradle SaaS, not the end result is that the Cradle SaaS is **not vulnerable** in this respect. • **Has missing or ineffective multi-factor authentication.** **Vulnerable** - We do not provide multi-factor authentication. 3SL has a long-term goal to migrate SaaS systems towards SAML and external authentication mechanisms. • **Exposes Session IDs in the URL (e.g., URL rewriting).** Cradle exposes session ID in its URLs, but **not vulnerable** to URL rewriting as source IP and session ID are checked on every call to ensure message is from the same client connection as that originally used to initialise the session. • **Does not rotate Session IDs after successful login.** **Not vulnerable**. All session IDs are regenerated when first logged in, and not reused. • **Does not properly invalidate Session IDs. User sessions or authentication tokens (particularly single sign-on (SSO) tokens) aren't properly invalidated during logout or a period of inactivity.** **Not vulnerable**. All session IDs are invalidated when the user session is closed, both by logout and by inactivity.

Table 6: OWASP Top 10 Compliance (continued)

#	Details	
3	Name	**Sensitive Data Exposure**
	Summary	If web applications don't protect sensitive data such as financial information and passwords, attackers can gain access to that data and sell or utilize it for nefarious purposes. One popular method for stealing sensitive information is using a man-in-the-middle attack. Data exposure risk can be minimized by encrypting all sensitive data as well as disabling the caching* of any sensitive information. Additionally, web application developers should take care to ensure that they are not unnecessarily storing any sensitive data. *Caching is the practice of temporarily storing data for re-use. For example, web browsers will often cache web pages so that if a user revisits those pages within a fixed time span, the browser does not have to fetch the pages from the web.
	Cradle SaaS	**Mostly Compliant** **The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information and business secrets require extra protection, particularly if that data falls under privacy laws, e.g. EU's General Data Protection Regulation (GDPR), or regulations, e.g. financial data protection such as PCI Data Security Standard (PCI DSS). For all such data:** • **Is any data transmitted in clear text? This concerns protocols such as HTTP, SMTP, and FTP. External internet traffic is especially dangerous. Verify all internal traffic e.g. between load balancers, web servers, or back-end systems.** **Vulnerable** as Cradle web UIs do not encrypt any data. Hence the Cradle SaaS uses HTTPS connections and Cradle web UIs are therefore **mot vulnerable**. • **Is sensitive data stored in clear text, including backups?** **Not vulnerable** as data is not stored on the same server as that which serves the web UIs, there is a firewall between the two servers, there is no user access to the server that stores the data, and the data is encrypted on the server where it is stored. • **Are any old or weak cryptographic algorithms used either by default or in older code?** **Not vulnerable** as HTTPS will negotiate the latest cryptographic algorithm supported by the browser and the Cradle Web Server. The CWS supports the latest ciphers. • **Are default cryptographic keys in use, weak cryptographic keys generated or re-used, or is proper key management or rotation missing?** **Not vulnerable** as HTTPS will negotiate the latest cryptographic algorithms and use new keys for each connection to the CWS. • **Is encryption not enforced, e.g. are any user agent (browser) security directives or headers missing?** **Not vulnerable** as HTTPS is enforced by the CWS which, in the Cradle SaaS service, has been configured to not support HTTP. • **Does the user agent (e.g. app, mail client) not verify if the received server certificate is valid?** **Not vulnerable** as the CWS needs a valid certificate to start. The certificate used by the Cradle SaaS service is 3SL's company certificate that is fully validated and verified.

Table 6: OWASP Top 10 Compliance (continued)

#	Details	
4	Name	**XML External Entities (XEE)**
	Summary	This is an attack against a web application that parses XML* input. This input can reference an external entity, attempting to exploit a vulnerability in the parser. An 'external entity' in this context refers to a storage unit, such as a hard drive. An XML parser can be duped into sending data to an unauthorized external entity, which can pass sensitive data directly to an attacker. The best ways to prevent XEE attacks are to have web applications accept a less complex type of data, such as JSON**, or at the very least to patch XML parsers and disable the use of external entities in an XML application. *XML or Extensible Markup Language is a markup language intended to be both human-readable and machine-readable. Due to its complexity and security vulnerabilities, it is now being phased out of use in many web applications. **JavaScript Object Notation (JSON) is a simple, human-readable notation often used to transmit data over the internet. Although it was originally created for JavaScript, JSON is language-agnostic and can be interpreted by many different programming languages.
	Cradle SaaS	**Compliant** **Applications and in particular XML-based web services or downstream integrations might be vulnerable to attack if:** • **The application accepts XML directly or XML uploads, especially from untrusted sources, or inserts untrusted data into XML documents, which is then parsed by an XML processor.** **Not vulnerable**. Cradle does not accept XML directly to be interpreted. Cradle web UIs and the CWS have functions to stop code injection wherever an opportunity to inject code may have existed. • **Any of the XML processors in the application or SOAP based web services has document type definitions (DTDs) enabled. As the exact mechanism for disabling DTD processing varies by processor, it is good practice to consult a reference such as the OWASP Cheat Sheet 'XXE Prevention'.** **Not vulnerable**. Cradle does not use XML, nor SOAP, and does not process DTDs in any form, anywhere. • **If your application uses SAML for identity processing within federated security or single sign on (SSO) purposes. SAML uses XML for identity assertions, and may be vulnerable.** **Not vulnerable**. Cradle does not use SAML. • **If the application uses SOAP prior to version 1.2, it is likely susceptible to XXE attacks if XML entities are being passed to the SOAP framework.** **Not vulnerable**. Cradle does not use SOAP. • **Being vulnerable to XXE attacks likely means that the application is vulnerable to denial of service attacks including the Billion Laughs attack.** **Not vulnerable**, for the reasons listed above.

Table 6: OWASP Top 10 Compliance (continued)

#	Details	
5	Name	**Broken Access Control**
	Summary	Access control refers a system that controls access to information or functionality. Broken access controls allow attackers to bypass authorization and perform tasks as though they were privileged users such as administrators. For example a web application could allow a user to change which account they are logged in as simply by changing part of a URL, without any other verification. Access controls can be secured by ensuring that a web application uses authorization tokens* and sets tight controls on them. *Many services issue authorization tokens when users log in. Every privileged request that a user makes will require that the authorization token be present. This is a secure way to ensure that the user is who they say they are, without having to constantly enter their login credentials.
	Cradle SaaS	**Compliant** **Access control enforces policy such that users cannot act outside of their intended roles and permissions. Failures typically lead to unauthorized information disclosure, modification or destruction of all data, or performing a business function outside of the limits of the user. Common access control vulnerabilities include:** • **Bypassing access control checks by modifying the URL, internal application state, or the HTML page, or simply using a custom API attack tool.** **Not vulnerable**. The accessibilty of information and ability to perform operations on information is not determined by, nor controlled, by any part of the web UI. No form of API attack can be launched from a web UI. For connections to Cradle through its API, the accessibility of information and ability to perform operations on information is not determined by, nor controlled, by any part of the API. Hence no actions by a web UI or an application written with the API can influence accessibility of, and ability to perform and save operations to, any items of information or links between items. • **Allowing the primary key to be changed to another users record, permitting viewing or editing someone else's account.** **Not vulnerable**. There is no ability to access primary keys of any information or user records from a web UI or any other part of Cradle. This functionality does not exist anywhere in the product. • **Elevation of privilege. Acting as a user without being logged in, or acting as an admin when logged in as a user.** **Not vulnerable**. It is impossible to access any information in, or perform operations on, links or cross references in a Cradle database without having logged-in successfully and obtained a valid session ID. • **Metadata manipulation, such as replaying or tampering with a JSON Web Token (JWT) access control token or a cookie or hidden field manipulated to elevate privileges, or abusing JWT invalidation.** **Not vulnerable**. It is impossible to access any information in, or perform operations on, links or cross references in a Cradle database using any web construct such as JWT, cookies or indeed anything other than Cradle identifiers - such as PDUIDs - which can only be obtained after having logged-in successfully and obtained a session ID.

Table 6: OWASP Top 10 Compliance (continued)

#	Details	
		• **CORS misconfiguration allows unauthorized API access.** **Not vulnerable**. CORS exploits are impossible for Cradle web UIs since only one connection per login per database is allowed and each such connection has a session ID hence CORS is ineffective as it cannot introduce session IDs into other connections. • **Force browsing to authenticated pages as an unauthenticated user or to privileged pages as a standard user. Accessing API with missing access controls for POST, PUT and DELETE.** **Not vulnerable**. Cradle web UIs' access controls are indirectly associated with POST, PUT and DELETE, but they are directly linked to users' accounts. The architecture of Cradle web UIs is completely different to typical web apps. See "Web Architecture" on page 24.
6	Name	**Security Misconfiguration**
	Summary	Security misconfiguration is the most common vulnerability on the list, and is often the result of using default configurations or displaying excessively verbose errors. For instance, an application could show a user overly-descriptive errors which may reveal vulnerabilities in the application. This can be mitigated by removing any unused features in the code and ensuring that error messages are more general.
	Cradle SaaS	**Compliant** **The application might be vulnerable if it is:** • **Missing appropriate security hardening across any part of the application stack, or improperly configured permissions on cloud services.** **Not vulnerable**, out of the box we provide a secure system without any need of configuration. Additional configuration can allow for a more secure system that can only allow the web server to only allow connections from trusted hosts. There is no application stack and no reliance on third party services, including HTTPS, which we control in the Cradle Web Server (CWS). • **Unnecessary features are enabled or installed (e.g. unnecessary ports, services, pages, accounts, or privileges).** **Not vulnerable**. Unlike other web UIs, there are no additional services, pages, ports or any other components in a Cradle web UI. See "Web Architecture" on page 24. • **Default accounts and their passwords still enabled and unchanged.** **Not vulnerable**. There are no default accounts for a Cradle web UI. The accounts are one and the same as those in the underlying Cradle database that have all been created by, and are all managed by, you. • **Error handling reveals stack traces or other overly informative error messages to users.** **Not vulnerable**, no information provided in any error output would reveal anything damaging as there is no application logic in a Cradle web UI due to the fundamentally different architecture. See "Web Architecture" on page 24. • **In upgraded systems, new security features are disabled or insecurely configured.** **Not vulnerable**, no security features are disabled in any Cradle web UI, but this is mainly inapplicable since Cradle web UIs do not use any third party application stack. All libraries, such as OpenSSL, are fully updated.

Table 6: OWASP Top 10 Compliance (continued)

#	Details	
		• **The security settings in the application servers, application frameworks (e.g. Struts, Spring, ASP.NET), libraries, databases, etc. not set to secure values.** **Not vulnerable** and not applicable as there is no application logic in a Cradle web UI due to the fundamentally different architecture. See “Web Architecture” on page 24 and hence no use is made of any application stack. • **The server does not send security headers or directives or they are not set to secure values.** **Not vulnerable**, the Cradle Web Server (CWS) does not send security headers in its exchanges with users’ web browsers. • **The software is out of date or vulnerable (see A9:2017-Using Components with Known Vulnerabilities).** **Not vulnerable** and not applicable. The CWS uses limited third party software, all of which is up to date. No application stacks (or equivalent) are used in any Cradle web UI. See “Web Architecture” on page 24.
7	Name	**Cross-Site Scripting**
	Summary	Cross-site scripting vulnerabilities occur when web applications allow users to add custom code into a URL path or onto a website that will be seen by other users. This vulnerability can be exploited to run malicious JavaScript code on a victim’s browser. For example, an attacker could send an email to a victim that appears to be from a trusted bank, with a link to that bank’s website. This link could have some malicious JavaScript code tagged onto the end of the URL. If the bank’s site is not properly protected against cross-site scripting, then that malicious code will be run in the victim’s web browser when they click on the link. Mitigation strategies for cross-site scripting include escaping untrusted HTTP requests as well as validating and/or sanitising user-generated content. Using modern web development frameworks like ReactJS and Ruby on Rails also provides some built-in cross-site scripting protection.
	Cradle SaaS	**Compliant** **There are three forms of XSS, usually targeting users' browsers:** • **Reflected XSS: The application or API includes unvalidated and unescaped user input as part of HTML output. A successful attack can allow the attacker to execute arbitrary HTML and JavaScript in the victim's browser. Typically the user will need to interact with a malicious link that points to an attacker controlled page, such as malicious watering hole websites, advertisements, or similar** **Not vulnerable**. Cradle web UIs and the CWS have functions to stop code injection wherever an opportunity to inject code may have existed. There is no opportunity for a web UI to execute code. • **Stored XSS: The application or API stores unsanitised user input that is viewed at a later time by another user or an administrator. Stored XSS is often considered a high or critical risk.** **Not vulnerable**. Cradle web UIs cannot store unsanitised user input. Even if they did, unsanitised user input cannot ever be executed. See “Web Architecture” on page 24. • **DOM XSS: JavaScript frameworks, single-page applications, and APIs that dynamically include attacker-controllable data to a page are vulnerable to DOM XSS. Ideally, the application would not send attacker-controllable data to unsafe JavaScript APIs.** **Not vulnerable**. Cradle web UIs never execute user input, whether Javascript or otherwise.

Table 6: OWASP Top 10 Compliance (continued)

#	Details	
8	Name	**Insecure Deserialisation**
	Summary	This threat targets the many web applications which frequently serialise and deserialise data. Serialization means taking objects from the application code and converting them into a format that can be used for another purpose, such as storing the data to disk or streaming it. Deserialisation is just the opposite: converting serialized data back into objects the application can use. Serialization is sort of like packing furniture away into boxes before a move, and deserialisation is like unpacking the boxes and assembling the furniture after the move. An insecure deserialisation attack is like having the movers tamper with the contents of the boxes before they are unpacked. An insecure deserialisation exploit is the result of deserialising data from untrusted sources, and can result in serious consequences like DDoS attacks and remote code execution attacks. While steps can be taken to try and catch attackers, such as monitoring deserialisation and implementing type checks, the only sure way to protect against insecure deserialisation attacks is to prohibit the deserialisation of data from untrusted sources.
	Cradle SaaS	**Compliant** **Applications and APIs will be vulnerable if they deserialise hostile or tampered objects supplied by an attacker.** **This can result in two primary types of attacks:** • **Object and data structure related attacks where the attacker modifies application logic or achieves arbitrary remote code execution if there are classes available to the application that can change behaviour during or after deserialisation.** **Not vulnerable**. Cradle web UIs do not serialise or deserialise and do not execute anything entered by a user or stored in a database. • **Typical data tampering attacks, such as access-control-related attacks, where existing data structures are used but the content is changed.** **Not vulnerable**. Cradle web UIs do not serialise or deserialise and do not execute anything entered by a user or stored in a database. **Serialization may be used in applications for:** • **Remote- and inter-process communication (RPC/IPC)** **Not vulnerable**. This is used between Cradle clients and CDS helper processes, for example for remote query execution, but this is invisible to users, web UIs and everything else that is accessible by or visible to, users. • **Wire protocols, web services, message brokers** **Not vulnerable**. Not used in this context by Cradle. • **Caching/Persistence** **Not vulnerable**. Not used in this context by Cradle. • **Databases, cache servers, file systems** **Not vulnerable**. Not used in this context by Cradle. • **HTTP cookies, HTML form parameters, API authentication tokens** **Not vulnerable**. Not used in this context by Cradle.

Table 6: OWASP Top 10 Compliance (continued)

#	Details	
9	Name	**Using Components With Known Vulnerabilities**
	Summary	Many modern web developers use components such as libraries and frameworks in their web applications. These components are pieces of software that help developers avoid redundant work and provide needed functionality; common example include front-end frameworks like React and smaller libraries that used to add share icons or a/b testing. Some attackers look for vulnerabilities in these components which they can then use to orchestrate attacks. Some of the more popular components are used on hundreds of thousands of websites; an attacker finding a security hole in one of these components could leave hundreds of thousands of sites vulnerable to exploit. Component developers often offer security patches and updates to plug up known vulnerabilities, but web application developers don't always have the patched or most-recent versions of components running on their applications. To minimize the risk of running components with known vulnerabilities, developers should remove unused components from their projects, as well as ensuring that they are receiving components from a trusted source and ensuring they are up to date.
	Cradle SaaS	**Compliant** **An application is likely to be vulnerable:** • **If the supplier does not know the versions of all components being used (both client-side and server-side). This includes components that are used directly as well as all nested dependencies.** **Not vulnerable**. All components' versions are known. Cradle web UIs do not use a traditional web application stack, see "Web Architecture" on page 24, so only a limited set of components are used, and only in some example web UIs. • **If software is vulnerable, unsupported, or out of date. This includes the OS, web/application server, database management system (DBMS), applications, APIs and all components, runtime environments, and libraries.** **Not vulnerable**. The example web UIs use some third party libraries which are updated at each major release, when updates are required. Cradle v7.4: OpenSSL: v1.0.1 Angular: v1.6.6 D3: v3.5.17 Jquery: v3.2.1 Cradle v7.5: OpenSSL: v1.0.1 Angular: v1.7.5 D3: v5.7.0 Jquery: v3.3.1 Cradle v7.6: OpenSSL: v1.1.1 Angular: v1.7.9 D3: v5.15.0 Jquery: v3.4.1 • **If you do not scan for vulnerabilities regularly and subscribe to security bulletins related to the components you use.** **Not vulnerable**, all libraries and components shipped with Cradle are checked during the final release checklist. If an urgent update to a component or library occurs, a new Cradle release is produced to ensure all shipped Cradle systems include stable components and libraries.

Table 6: OWASP Top 10 Compliance (continued)

#	Details	
		• **If you do not fix or upgrade the underlying platform, frameworks, and dependencies in a risk-based, timely fashion. This commonly happens in environments when patching is a monthly or quarterly task under change control, which leaves organizations open to many days or months of unnecessary exposure to fixed vulnerabilities.** **Not vulnerable**, see previous response. Cradle web UIs do not use a traditional web application stack, see “Web Architecture” on page 24, so a limited set of components are used, and only in some example web UIs. • **If software developers do not test the compatibility of updated, upgraded, or patched libraries.** **Not vulnerable**, see previous response. • **If you do not secure the components' configurations (see A6:2017-Security Misconfiguration).** **Not vulnerable**, see previous response
10	Name	**Insufficient Logging And Monitoring**
	Summary	Many web applications are not taking enough steps to detect data breaches. The average discovery time for a breach is around 200 days after it has happened. This gives attackers a lot of time to cause damage before there is any response. OWASP recommends that web developers should implement logging and monitoring as well as incident response plans to ensure that they are made aware of attacks on their applications.
	Cradle SaaS	**Compliant** Cradle provides full logging of users’ interaction with the system and the data in its databases. **Insufficient logging, detection, monitoring and active response occurs any time:** • **Auditable events, such as logins, failed logins, and high-value transactions are not logged.** **Not vulnerable**. Cradle logs all attempts to connect to the Cradle servers (accepted and rejected) and all login attempts (successful and unsuccessful). User-defined actions (such as logging) can occur for all item, cross reference, user and operation events. • **Warnings and errors generate no, inadequate, or unclear log messages.** **Not vulnerable**. See previous response. User-defined actions can include any logging with any degree of detail required. All logs occur server-side. • **Logs of applications and APIs are not monitored for suspicious activity.** **Not vulnerable**. See previous responses. User-defined actions can include priority for important events, such as automated e-mail alerts. • **Logs are only stored locally.** **Not vulnerable**. All logs occur server-side. • **Appropriate alerting thresholds and response escalation processes are not in place or effective.** **Not vulnerable**. See previous response. Each database’s users decide the logging that they require. • **Penetration testing and scans by DAST tools (such as OWASP ZAP) do not trigger alerts.** **Not vulnerable**. Penetration testing to be arranged by you. 3SL commits to working with you and your penetration testers to resolve any issues that may be found prior to your production use of Cradle.

Table 6: OWASP Top 10 Compliance (continued)		
#	Details	
		• **The application is unable to detect, escalate, or alert for active attacks in real time or near real time. You are vulnerable to information leakage if you make logging and alerting events visible to a user or an attacker (see A3:2017Sensitive Information Exposure).** **Not vulnerable**. See previous responses. User-defined actions can include priority for important events, such as automated e-mail alerts.

6 Security Governance Framework

3SL has a framework for the governance of the security and integrity of all SaaS systems. This framework consists of a set of policies that are reviewed as part of 3SL's quarterly ISO 9001 management audit. The key policies are:

Table 7: Governance Framework Policies		
#	Name	Details
A: Responsibility and Accountability		
POL-A-1	3SL Responsibility	3SL's Director Mark Walker has overall responsibility for all aspects of 3SL's SaaS services
POL-A-2	Individual Responsibility	Everyone in 3SL who does work within, or related to, a SaaS service, is responsible for a) the successful completion of his / her work, b) to check that their work is complete, and c) to have their work peer reviewed for accuracy, completeness and quality.
POL-A-3	Confidentiality	All 3SL staff are required to annually re-confirm, as a condition of their continued employment, their acceptance of, and adherence to, 3SL's confidentiality agreement that requires that they keep secret information that is confidential 3SL, its partners, customers and suppliers and advises of the personal legal and financial consequences of non-compliance.
B: Legal and Regulatory Compliance		
POL-B-1	Regulatory Compliance	Assess information updates, bulletins and other announcements from Government, industry trade bodies, international bodies, professional bodies, and hardware and software manufacturers to ensure that 3SL is aware of all legal, regulatory, technical and commercial changes and can assess their impact, if any, on 3SL's SaaS services.
POL-B-2	Professional Advice	Secure sources of legal advice on relevant matters including personnel and HR, trademark and copyright, service liability and indemnity
POL-B-3	Insurances and Indemnities	Secure adequate insurances for employers liability, third party liability, business continuity, disaster recovery, professional indemnity
C: User Accounts		
POL-C-1	Minimum Privileges	Login accounts will have the minimum possible privileges. Default logins will be to minimum privilege accounts. Wherever possible, administrator accounts will not allow logins but will be an assumed role after login to a minimum capability account.
POL-C-2	Timeouts	Wherever possible, all logins and sessions are to timeout after a period of inactivity based on the scope and sensitivity of the access underway but in no event longer than 30 minutes.

Table 7: Governance Framework Policies (continued)		
#	**Name**	**Details**
POL-C-3	Password Complexity	All passwords will be a minimum of 12 characters, requiring one or more lowercase and uppercase letters, number and other special (printable) character
POL-C-4	Password for Keypair	All login accounts will have personal, not generic, usernames with a password. If a login uses a keypair, it will also have a password known only to one individual, so that a group of people cannot share the same keypair based login capability.
D: Data Integrity		
POL-D-1	Backups Successful	Whether created automatically or manually, backups are to be created as defined for the SaaS service and any applicable SLA. Creation of backups and all associated integrity log files are to be checked not less than weekly.
POL-D-2	Backups Valid	The accuracy (has correct content) and validity (content is complete and correct) of each type of backup (administrative, database and so on) to be confirmed by manual verification not less than monthly.
POL-D-3	Snapshots Successful	Whether created automatically or manually, snapshots are to be created as defined for the SaaS service and any applicable SLA. Creation of the snapshots and all associated integrity log files are to be checked not less than weekly.
POL-D-4	Snapshot Valid	The accuracy (has correct content) and validity (content is complete and correct) of the snapshots of each server in the VPC are to be confirmed by manual verification not less than quarterly.
POL-D-5	Personal Data	Ensure that all personal data held for the SaaS is minimised, strictly necessary to provide the SaaS, and deleted as soon as practicable. Review this information not less than quarterly.
E: Operational Integrity		
POL-E-1	Document Changes	All changes are recorded in a Subscription Management Record (SMR) that 3SL maintains for each Cradle SaaS service. This SMR is sent to your lead users after every change. The SMR primarily records users, locations and databases.
POL-E-2	Change Planning	All changes will be planned and their timing agreed with you in an agreed service outage. All changes will have a back-out plan and success criteria. If the success criteria are not met then the back-out plan will be performed so that the change is fully reversed. The failure of the success criteria will be reviewed with you so that a revised change can be planned and completed at a later date.
POL-E-3	Licences Valid	Ensure that all operating licences (O/S, SALs, applications, KVM and so on) are valid and that the correct number of all licences have been created for the SaaS with its current configuration and set of users.
POL-E-4	O/S Up to Date	The existence of O/S updates will be checked not less than monthly. Which O/S updates are to be applied will be discussed with you, or not, as you prefer, and their installation planned in an agreed change.
POL-E-5	Applications Up to Date	The existence of application updates will be checked not less than monthly. Which O/S updates are to be applied will be discussed with you, or not, as you prefer, and their installation planned in an agreed change.
POL-E-6	Adequate Disk Space	The presence of sufficient disk space will be reviewed not less than monthly. Additional disk, and any resulting additional charges, will be discussed with you and its addition will be planned in an agreed change.

Table 7: Governance Framework Policies (continued)

#	Name	Details
POL-E-7	Adequate Computer Resources	The availability of sufficient CPU / cores and RAM in each server in the Cradle SaaS service will be reviewed not less than quarterly. Additional computer resources, and any resulting additional charges, will be discussed with you and its addition will be planned in an agreed change.
POL-E-8	Adequate I/O Bandwidth	The availability of sufficient I/O bandwidth in the Cradle SaaS service will be reviewed not less than quarterly. Additional I/O bandwidth, and any resulting additional charges, will be discussed with you and its addition will be planned in an agreed change.
F: Security Integrity		
POL-F-1	Security Alerts	Ensure that the alerting mechanism(s) for all security threats to and alarms at perimeter, communications, network, host, O/S and application levels within the SaaS are working, with a manual check not less than weekly.
POL-F-2	Perimeter Integrity	Ensure that all perimeter integrity checks (particularly firewall rules) have been done not less than weekly
POL-F-3	User Access Integrity	Ensure that all user access integrity checks (attempted logins and/or user attempts to access applications) have been done not less than weekly
POL-F-4	Application Integrity	Ensure that all application logs for illegal startup requests, data requests and invalid operations have been checked, not less than weekly
POL-F-5	Usage Integrity	Ensure that all application logs for attempted illegal operations by users of all applications have been checked, not less than weekly.
POL-F-6	Security Log Reviews	Ensure that all O/S and application security logs are reviewed not less than weekly.
POL-F-7	Vulnerability Reviews	Ensure that all vulnerabilities reported by security alerts from hardware and software vendors are assessed to decide applicability to the SaaS and scope, impact and risk to the SaaS, required actions and urgency.

7 Service Level Agreement

The KPIs (***Key Performance Indicators***) that 3SL will provide for the Cradle SaaS service (all times are in working hours for 8-hour man-days) are:

Table 8: SLA KPIs

#	Name	Details	Value
Service Availability			
KPI-1	Service Platform Availability	Availability of the Cradle server, derived from the AWS EC2 SLA at: `https://aws.amazon.com/compute/sla/`	99.99%
KPI-2	Server Restore	Time to restore a server snapshot	2 hours
Access to Service			
KPI-3	Add Location	Add a location that can access the Cradle SaaS service	8 hours
KPI-4	Change Location	Change a location that can access the Cradle SaaS service	8 hours
KPI-5	Delete Location	Delete a location that can access the Cradle SaaS service	8 hours
Cradle Databases			
KPI-6	Create Database	Create a new Cradle database in the Cradle SaaS service, and create an initial set of Cradle user profiles if requested	8 hours
KPI-7	Restore Database - RTO	Restore a database from a specific backup	4 hours
KPI-8	Delete Database	Delete a Cradle database and remove all of its backups	8 hours
Technical Support			
KPI-9	Acknowledge Support Call	Time to acknowledge a support call with a call number and assign an engineer to the call	1 hour
KPI-10	P1 Fix Time	Time to fix a P1 (**URGENT**) priority support call if that fix is to restore a database	2 hours
KPI-11	P2 Fix Time	Time to fix a P2 (**HIGH**) priority support call if that fix does not require user data and does not require a database restoration	4 hours
KPI-12	P1-P2 Close Time	Time to close a P1 or P2 support call that does not require any user data or a database restoration and is not a bug or an enhancement request	8 hours
KPI-13	P3-P4 Close Time	Time to close a P3 or P4 (**MEDIUM**) priority support call that does not require any user data and is not a bug or an enhancement request	16 hours
KPI-14	P5 Close Time	Time to close a P5 (**LOW**) priority support call that does not require any user data and is not a bug or an enhancement request	24 hours
KPI-15	Support Call Close	All other support calls not categorised in any other KPI. This includes those calls where the customer will need to provide data to 3SL and where a bug or enhancement is being identified or reproduced, characterised or specified, and reviewed and confirmed.	Best efforts or 40 hours

8 On-boarding

On-boarding the **3SL Cradle** service is the combination of:

1. Server build and configuration, including installing application software preferences, creating user accounts on the server, and implementing the backup regime
2. Optional consultancy services to prepare Cradle to support your project, containing activities such as:
    a) Defining the structure of the Cradle database (called a ***schema***) to support the process that your project will use
    b) Creating appropriate queries, views, forms and other definitions for your data
    c) Defining templates for the documents that your project will produce
    d) Loading any of your data into your Cradle database. Cradle can load data in the following formats:
        i) Cradle
        ii) CSV, TSV
        iii) XML, subject to an XSD file defining the structure of the XML data
        iv) ReqIF
        v) Word document
        vi) Excel spreadsheet

    You can choose which, if any, of these services are needed from 3SL's range of Cloud Support consultancy products.

9 Off-Boarding

Off-boarding for the **3SL Cradle** service means to download your data from the server providing the service before the server is destroyed. Off-boarding is your decision and optional. You can download in the following formats:

1. Cradle
2. CSV, TSV
3. RTF
4. HTML
5. XML, subject to an XSD file defining the structure of the XML data
6. ReqIF
7. Word document
8. Excel spreadsheet

If you want 3SL to help you to off-board your data, then you can choose from 3SL's range of Cloud Support consultancy products.

10 Pricing

Please refer to the document “G-Cloud 13 - 3SL Cradle Cloud Software and Cloud Support Price List”, reference SG174/08.

11 Service Management

3SL’s preferred Cloud Hosting partners FCO Services, UKCloud, AWS and OVH, will mandate the service. Please refer to their corresponding G-Cloud service descriptions for more information on Service Management.

12 Service Constraints

3SL’s preferred Cloud Hosting partners FCO Services, UKCloud, AWS and OVH, will mandate the service. Please refer to their corresponding G-Cloud service descriptions for more information on Service Constraints.

13 Service Levels

3SL’s preferred Cloud Hosting partners FCO Services, UK Cloud, UK Fast, AWS and OVH, will mandate the service levels. Please refer to their corresponding G-Cloud service descriptions for more information on Service Levels.

3SL re-packages these service levels in the KPIs for the **3SL Cradle** service, see “Service Level Agreement” on page 51.

14 Financial Recompense

Not applicable.

15 Training

Training is available from 3SL’s range of Cloud Support training products.

16 Service Term

The minimum term for the **3SL Cradle** service provided through an Unassured Cloud service (formerly known as IL0) is 6 months. The minimum term for the **3SL Cradle** service provided through an Accredited Public Cloud service (formerly known as IL3) is 12 months.

If you do not send 3SL a notice of termination (see “Termination by You” on page 55), the then current term will automatically continue into a new term of equal duration.

17 Ordering and Invoice Process

The **3SL Cradle** service can be ordered directly from the price list or (only for Cloud Hosting fees) after discussion with 3SL if a non-default server is required. An order for the **3SL Cradle** service will contain:

1. Any Cloud Hosting on-boarding fees required by your choice of Unassured Cloud service or Accredited Public Cloud service
2. Any 3SL Cloud Support products that you require to help you with on-boarding
3. The 3SL Cloud Software charge for the **3SL Cradle** service, derived from:
   - a) The number of users that you require
   - b) The term of service that you require
   - c) The **3SL Cradle** service charge per user per month, for each month of the term
   - d) The Cloud Hosting service charge per month, for each month of the term
4. Any 3SL Cloud Support training products that you require to train you to use Cradle
5. Any 3SL Cloud Support consultancy products that you require to configure Cradle for your project and process
6. Any 3SL Cloud Support consultancy products that you require during the term

3SL will invoice you:

- At the start of the term for any on-boarding fees
- Monthly in arrears for the Cloud Hosting and Cloud Software fees
- After completion of each Cloud Support training or consultancy product

3SL’s invoices must be paid within 30 days by BACS transfer with a Remittance Advice sent by e-mail to your 3SL contact that includes your order number and 3SL’s invoice number.

18 Termination

18.1 Termination by You

The minimum notice period to terminate a **3SL Cradle** service provided through an Unassured Cloud service (formerly known as IL0) is 2 months. The minimum term for the **3SL Cradle** service provided through an Accredited Public Cloud service (formerly known as IL3) is 3 months.

18.2 Termination by 3SL

3SL reserves the right to terminate an active service if one or more of the following conditions apply:

- You do not pay for the service provision at agreed rates and charges
- Force majeure
- Insolvency
- Material breach

19 Data Restoration/Service Migration

See off-boarding in “On-boarding” on page 52.

20 Your Responsibilities

You must define the control and management of access and responsibilities for end users within Cradle databases.

21 Technical Requirements

Technical requirements for the **3SL Cradle** service and hosting server will be discussed with you before any orders for the service.

22 Trial of Service

3SL offers a free trial of the **3SL Cradle** service provided through an Unassured Cloud service (formerly IL0) for a period of one month. This will use 3SL's own servers which are located in the UK and are UK sovereign.

Free trials of the **3SL Cradle** service provided through an Accredited Public Cloud service (OFFICIAL, formerly IL3) are not available.

23 Free Service

3SL offers a free use of the **3SL Cradle** service provided through an Unassured Cloud service hosted by 3SL. This free service is limited to product exploration and experimentation and is not intended for production use.

24 Sub-Contractors

Other than its Cloud Hosting partners, 3SL does not use any third party sub-contractors to deliver its Cloud Software or Cloud Support services.

25 About 3SL

Structured Software Systems Limited (3SL) is an independent software vendor founded in 1987. We are an SME and the only UK-owned, UK-based developer of ALM, enterprise architecture, requirements management, systems engineering, risk management, test execution, configuration management and document management software tools. 3SL has ISO9001 and Cyber Essentials/IASME certification. We have a global network of distributors and a global customer base.