Non-Functional Requirements

Version: 0.5

1.1 Table of Contents

1.2 Document Versioning

Version	Author	Date	Changes
0.1	Zabair Zafar	16/04/2019	Template and First Draft
0.2	Zabair Zafar	29/04/2019	Updated following internal review with Jan
0.3	Zabair Zafar	08/05/2019	Updated following sessions with Oracle and Inoapps
0.4	Zabair Zafar	10/05/2019	Updated following internal review with Jan
0.5	Zabair Zafar	17/06/2019	Updated following review with internal stakeholders

1.3 Reviewers

Name	Organisation	Role	Sign-off/Reviewer
		IT Programme Director	Sign-off
		Enterprise Architect	Sign-off
		Finance Programme Director	Reviewer
		Consultancy Programme Director	Reviewer
		Construction Programme Director	Reviewer
		Technical Lead	Reviewer
		Comm4 SME	Reviewer
		HCM SME	Reviewer
		Head of ICT Security	Reviewer
		ICT Infrastructure and Operations	Reviewer
		ICT Transition Manager	Reviewer
		Integration Lead	Reviewer
		Functional SME	Reviewer
		PwC Lead	Reviewer

1.4 Acronyms

Term	Description
AD	Active Directory
ADFS	Active Directory Federation Services
AES	Advanced Encryption Standard
BMS	Business Management System
CODA	Legacy finance system
Comm4	Construction-specific custom [Client] SaaS solution
CPU	Central Processing Unit
DoS	Denial of Service
DSAR	Data Subject Access Requests
ERP	Enterprise Resource Planning
GDPR	General Data Protection Regulation
GL	General Ledger
HCM	Human Capital Management
HMRC	Her Majesty's Revenue and Customs
ICT	Information and communications technology
KMA	Key Management Appliance
NFR	Non-Functional Requirement
NFS	Network File System
LDAP	Lightweight Directory Access Protocol
OBS	Oracle Secure Backup
PO	Purchase Order
RMAN	Recovery Manager
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SaaS	Software as a Service
SSO	Single Sign-On
SME	Subject Matter Expert
TDE	Transparent Data Encryption
TLS	Transport Layer Security
VM	Virtual Machine

2. Introduction

Document Purpose

The purpose of this document is to capture the Non-Functional Requirements (NFRs) associated with the [Programme] Programme implementation of Oracle ERP Cloud and Comm4.

The document also captures the current state of the Cloud ERP and Comm4 systems in relation to the NFR's.

Non-functional Requirements capture conditions that do not directly relate to the behaviour or functionality of the solution, but rather describe environmental conditions under which the solution must remain effective or qualities that the systems must have.

These NFRs will be used together with the Functional Requirements to form the basis of the [Programme] Solution and as inputs to the project team, service contracting, and the service acceptance process.

2.1 Document Scope

The diagram below illustrates the scope of the NFRs. All components within the boundary of the dotted line are considered in scope. The NFRs essentially cover Oracle Cloud HCM/ERP, Comm4 and the inbound/outbound interfaces (including the interfaces between HCM/ERP and Comm4).

[DIAGRAM]

In terms of organisational scope, the NFRs cover [Client] Construction and Consulting in the UK and across [Client] international regions.

2.2 Document Approach

The document captures the Non-Functional Requirements for the [Programme] programme, along with the current state of each requirement for Oracle ERP Cloud and Comm4.

Requirements Definition

The NFRs are being defined at a time when the [Programme] programme has already selected, and is progressing with, the Oracle HCM/ERP SaaS offering and the Inoapps Comm4 custom SaaS solution. Therefore, it became necessary to take a bottom-up approach to defining the [Programme] NFRs, as illustrated in the diagram below:
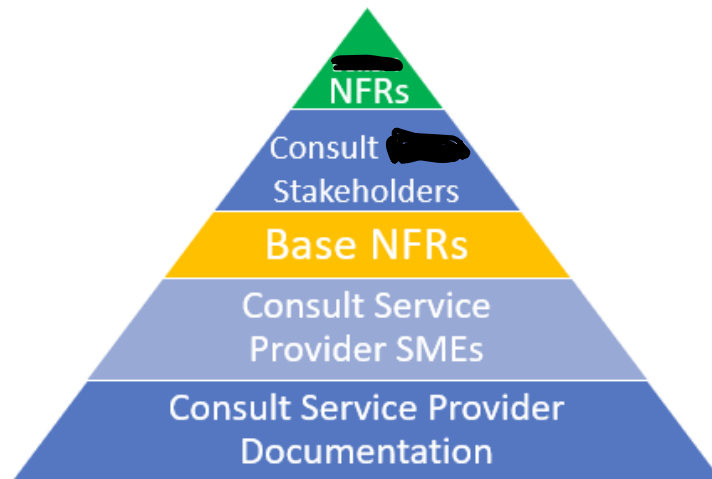
Consult Service Provider Documentation

The documentation for both SaaS solutions has been consulted to initially understand and capture the base non-functional qualities of the services being provided by Oracle and Inoapps. The following documentation has been consulted:

Document Name	Organisation	Version/Date

Consult Service Provider SMEs

As part of the process of capturing the base NFRs and to ensure the supplier documentation provided an accurate reflection of the actual services being provided to [Client], the following SMEs have been consulted from the respective service providers:

SME	Role	Organisation	Engagement Type
			Email and Conference call
			Email and face-to-face meeting

Base NFRs

The information gathered from the supplier documentation, re-enforced by the SME engagement, created the initial set of base NFRs. The base NFRs represented a view of the non-functional characteristics of the SaaS solutions from Oracle and Inoapps.

Consult [Client] Stakeholders

The base NFRs were then presented to key [Client] stakeholders, in individual and collective meetings, to determine if additional NFRs were required and whether the base NFRs were acceptable or needed to be amended. The following people within [Client] were consulted to define the [Programme] NFRs:

Name	Role	NFR Input Area	Engagement Type
	IT Programme Director	All	NFR walkthrough/review
	Enterprise Architect	All	NFR walkthrough/review
	Finance Programme Director	Summary NFRs	NFR walkthrough/review
	Consultancy Programme Director	Summary NFRs	NFR walkthrough/review
	Construction Programme Director	Summary NFRs	NFR walkthrough/review
	Comm4 SME	All	NFR walkthrough/review
	Head of ICT Security	Security	NFR walkthrough/review
	HCM SME	All	NFR walkthrough/review
	ICT Infrastructure and Operations	All	NFR walkthrough/review
	ICT Transition Manager	All	NFR walkthrough/review
	Integration Lead	Interoperability	NFR walkthrough/review
	Service contracts	Operability	NFR walkthrough/review

The [Programme] NFRs are the output from the [Client] Stakeholder engagement, which took the form of NFR document walkthrough sessions and document review requests. Feedback from the walkthrough sessions and the comments received from the review requests defined the final set of NFRs.

[Programme] NFRs

What is contained in this document represents the [Programme] NFRs after undergoing the process outlined above.
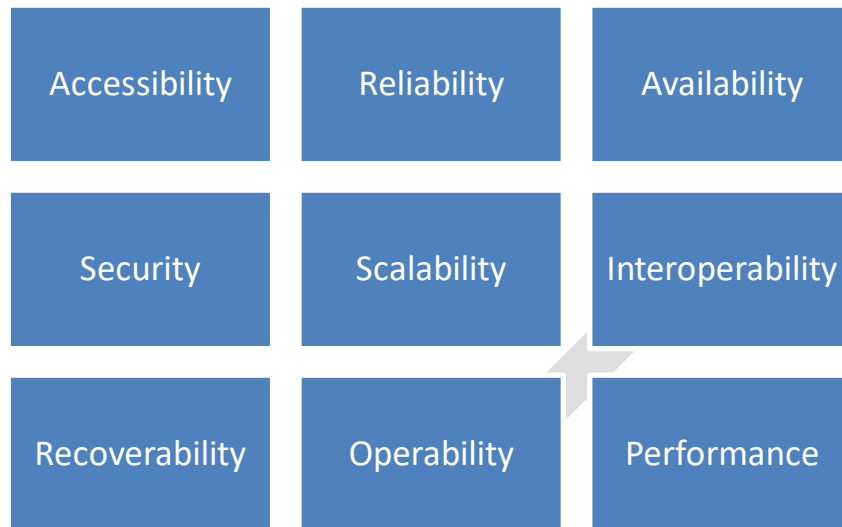
Requirements State

The requirement state represents a *'snapshot'* of the solution in its current implementation. A requirement will have one of the following states:

Met – Validation required	This status indicates that there is supporting documentation to suggest that a requirement has been met. However, further validation is required from the service provider to ensure the requirement has been comprehensively met by the service.
Met – Validated	This status indicates that there is supporting documentation to suggest that a requirement has been met and/or the service provider has offered sufficient proof.
Not Met – Further input required	This status indicates that there is supporting documentation to suggest that a requirement has not been met. Further work needs to be done to ensure the requirement is met.
Pending – Further input required	This status indicates that further work needs to be done to confirm whether a requirement has been met or not.

It's important to note that the sign-off of this document is only on the NFRs that have been captured. The state of a requirement is for information only, and it's an acknowledgment of additional work that is required, which needs to be done outside of this document, to ensure all NFR's are satisfactorily met.

2.3 Non-Functional Requirements

The following NFRs are addressed in this document:

Accessibility	Reliability	Availability
Security	Scalability	Interoperability
Recoverability	Operability	Performance

1. **Accessibility:** Ensuring an equivalent experience for everyone who will use the system.
2. **Reliability:** Refers to the probability of a system or system element performing its intended function under stated conditions without failure for a given period.
3. **Availability:** Degree to which users can depend on the system to be up (able to function) during normal operating times.
4. **Security:** Address what needs to be satisfied to achieve the security attributes of an IT system and meet [Client]'s IT security requirements.
5. **Scalability:** How well the system can expand its processing capabilities, upward and outward, to support business growth.
6. **Interoperability:** The extent to which the software system can facilitate the interface with other systems.
7. **Recoverability:** Addresses how quickly a system can be recovered after experiencing a system failure.
8. **Operability:** The ability to keep a system in a safe and reliable functioning condition
9. **Performance:** The responsiveness of a system to perform specific actions in a given time span.
10. **GDPR:** The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment.

3. Accessibility Requirements

Accessibility requirements refer to ensuring an equivalent experience for everyone who will use a particular system. Accessibility means that everyone can perceive, understand, navigate and interact with the system. The aim of accessibility is that there should be no system-related barriers to people contributing equally.

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
NFR-ACS-001	ERP Cloud & Comm4	Users must be able to access the user interface using Google Chrome 73+ Microsoft Edge 42+ Microsoft Internet Explorer 11.* Including Safari on iOS and Chrome on Android devices.	UI access on the required bowsers should include all future releases of the browsers.	**Met** - Validated Desktop User Interface on Desktop Devices: Apple Safari 11.* and 10.* Google Chrome 60+ Microsoft Edge 40+ Microsoft Internet Explorer 11.* Mozilla Firefox 52+ **REF:** *System Requirements for Oracle Applications Cloud*	**Met** - Validated Comm4 is accessible via a web browser only. Comm4 supports the current and prior major release of Google Chrome, Firefox, Microsoft Internet Explorer and Microsoft Edge. **REF**: *Comm4 Application Technical Solution Design [p.21]*
NFR-ACS-002	ERP Cloud & Comm4	The system user interface must support the English language.	English is the only language that is required to be supported by the system, which includes international users.	**Met** - Validated Oracle ERP Cloud is available in the following 25 languages: Arabic, Dutch, German, Korean, Russian, Chinese-Simplified, English, Hebrew, Norwegian, Spanish, Chinese-Traditional, Finnish, Hungarian, Polish, Swedish, Czech, French-Canada, Italian, Portuguese-Brazil, Thai, Danish, French-France, Japanese, Romanian, Turkish **REF:** *Oracle ERP Cloud Release 13 Global Catalog [p.8]*	**Met** - Validated The screens are only available in English. **REF**: *Comm4 Application Technical Solution Design [p.26]*

				Current State	
NFR-ID	System	Requirement Statement	Note	HCM/ERP Cloud	Comm4
NFR-ACS-003	ERP Cloud & Comm4	Date format shall be UK-compliant across all [Client] locations.	The date format: dd/mm/yyyy	**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Met** - Validated Checked via the UI.
NFR-ACS-004	ERP Cloud & Comm4	Number format shall be UK-compliant across all [Client] locations.	The number format: 123,456.78	**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Met** - Validated Checked via the UI.
NFR-ACS-005	ERP Cloud & Comm4	The system must comply with the Equality Act 2010 (supersedes Disability Discrimination Act 1995). **Justification:** Legal requirement.	At a minimum this should include: • Text to accompany non-text elements (pictures or graphical buttons). • Coloured content can be inferred or is available without colour. • Labelling the websites content.	**Met** - Validated Oracle Fusion Applications is designed with accessibility features that support assistive technologies, such as screen readers. You can set accessibility preferences to use the application in accessibility mode. **REF:** *Oracle Applications Cloud Using Common Features Release 13 [p.89]*	**Not Met** – Further Input Required The UK Disability Discrimination Act 1995 was not defined as a requirement when the Comm4 system was being designed. Therefore, the compliance of Comm4 against the requirements of that Act is not fully defined at this time. **REF**: *Comm4 Application Technical Solution Design [P.21]*
NFR-ACS-006	ERP Cloud & Comm4	The system must be accessible from a Microsoft Windows-based desktop PC and a laptop, which includes laptops (including laptops with touchscreen capability) and mobile devices.	Access on iOS or Android devices via Safari and Google Chrome is required to be supported by Oracle HCM/ERP and Comm4.	**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Pending** – Further Input Required The Comm4 system has been designed to work on desktop devices only. Mobile devices may render the Comm4 application, but this has not been part of the design process. **REF**: *Comm4 Application Technical Solution Design [P.22]* Retrospectively, this requirement indicates a desire for the Comm4

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
					UI to support mobile devices. However, the pursuit of this requirement needs to be balanced with the understanding of the cost and effort required to enable mobile device support.
NFR-ACS-007	ERP Cloud & Comm4	The system must be accessible over the internet from any location.	The system should not enforce geographical restrictions on accessibility. This includes access from the Middle East and China.	Met - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	Met - Validation Required

4. Reliability Requirements

Reliability requirements refers to the probability of a system or system element performing its intended function under stated conditions without failure for a given period of time. A precise definition must include a detailed description of the function, the environment, the time scale, and what constitutes a failure.

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
NFR-REL-001	ERP Cloud & Comm4	The service shall not have a single point of failure that would cause a major system outage. Exceptions should be agreed, documented and mechanisms in place for recovery within service levels. **Justification:** A single point of failure has direct impact on service availability and recovery.	At present, the [Client] AD domain controller is a single point of failure.	**Met** - Validated Clustered web, app and database tier. ***REF:*** *Fusion Cloud Service Disaster Recovery Evidence Summary [p.1]*	**Not Met** – Further Input Required Single instance web, app and database service. Not clear how these will be timely recovered. ***REF****: Comm4 Application Technical Solution Design (p.6)*
NFR-REL-002	ERP Cloud & Comm4	The service shall be able to continue to operate potentially in a degraded state due to a failure in a dependant system.	This ensures a system is loosely coupled with the remaining system landscape.	**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Met** - Validation Required Production services may operate in a degraded state of performance for the duration of the disaster event. ***REF****: Comm4 Application Technical Solution Design (p.23)*
NFR-REL-003	ERP Cloud & Comm4	A Disaster Recovery plan shall support RPO and RTO as detailed in Section 9.		**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Not Met** – Further Input Required Backups not in line with required RPO.
NFR-REL-004	ERP Cloud & Comm4	The currency values must have a precision of 13 and a scale of 2.	Precision is the number of significant digits. Scale is the number of digits to the right of the decimal point.	**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Met** - Validated Proven via the Comm4 UI.

5. Availability Requirements

Availability is the degree to which users can depend on the system to be up (able to function) during normal operating times.

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
NFR-AVL-001	ERP Cloud & Comm4	The system must be available to users for 99.5%. **Justification:** Business impact: More than 4 hours not acceptable.	99.5 % uptime/availability results in the following periods of allowed downtime/unavailability: Daily: 7m 12.0s Weekly: 50m 24.0s Monthly: 3h 39m 8.7s Yearly: 1d 19h 49m 44.8s The 99.5% uptime excludes planned outage.	**Met** - Validated Commencing at Oracle's activation of Your production Oracle Cloud Service, Oracle works to meet the Target Service Availability Level, or Target Service Uptime, of 99.5%. ***REF:*** *Oracle Cloud Hosting and Delivery Policies*	**Met** - Validated DBaaS, OCI Compute, OCI Block Storage etc all have 99.5% or better availability. ***REF:*** *NFRs: Initial questions for Inoapps-01/05/2019 (email)*
NFR-AVL-002	ERP Cloud & Comm4	Scheduled downtime must not cause disruption to the service during 8:00am to 6:00pm UK office hours, unless explicitly agreed with [Client].	Scheduled downtime should be agreed with the business.	**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Pending** – Further Input Required
NFR-AVL-003	ERP Cloud & Comm4	In the event of a complete failure of the Production primary site, the system must have the capability to failover to a secondary site.	A secondary site ensures the system remains available in the event of the primary site being destroyed in a disaster or becoming unavailable.	**Met** - Validated The Oracle Fusion Cloud Service DR solution has two sites, primary and secondary. Under normal operating conditions, the primary site is running and in active mode, while the secondary site, which replicates the primary site, is in passive mode. In the event of an Oracle declared disaster, Oracle will resume production of primary services at a secondary facility.	**Not Met** – Further Input Required Comm4 was designed and built to run in standard DBaaS single instance machine and has all the characteristics of such, there is no synchronization to remote sites. ***REF***: *NFRs: Initial questions for Inoapps 01/05/2019 (email)*

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
				REF: Fusion Cloud Service Disaster Recovery Evidence Summary	

6. Security Requirements

Security Requirements describe what needs to be satisfied in order to achieve the security attributes of an IT system.

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
NFR-SEC-001	Oracle ERP & Comm4	The system shall obtain the user identities for internal users from Active Directory.		**Met** - Validated Users are created in AD and Oracle separately. Oracle then syncs to BMS via an integration package, BMS then syncs to Active Directory via Quest Quick Connect. *REF: James Smith - RE: Document Review: Non-Functional Requirements v0.4[DRAFT] 15/05/2019 (email)*	**Met** - Validated [Client] internal user access to Comm4 is controlled using the [Client] LDAP, Microsoft Active Directory. Sub-contractor application has a separate administration page that allows [Client] internal admin user to create sub-contractor (external) usernames. The usernames are stored in the Comm4 database within the [Client] schema. *REF: Comm4 Application Technical Solution Design [p.8]*
NFR-SEC-002	Comm4	The system shall obtain the user identities for external/sub-contractor users from a database.			**Met** - Validated Sub-contractor application has a separate administration page that allows [CLIENT] internal admin user to create sub-contractor (external) usernames. The usernames are stored in the Comm4 database within the [CLIENT] schema. *REF: Comm4 Application Technical Solution Design [p.9]*

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
NFR-SEC-003	Oracle ERP & Comm4	The system shall provide the ability to manage users, groups and roles.		**Met** - Validated The User Accounts page also serves as a gateway to account-management actions you can complete. *REF: Oracle ERP Cloud Securing ERP Release 13 [p.29]*	**Met** - Validated Manage project user and roles. *REF: PM Construction User Guide (p.14)*
NFR-SEC-004	Oracle ERP & Comm4	The system shall support role-based access control to screens, data and reports.	It is assumed that role-based access will be implemented as part of functional activities.	**Met** - Validated Oracle Enterprise Resource Planning (Oracle ERP) Cloud defines the following types of roles: • Job roles • Abstract roles • Duty roles • Aggregate privileges *REF: Oracle ERP Cloud Securing ERP Release 13 [p.3]*	**Met** - Validated Manage project user and roles. *REF: PM Construction User Guide (p.14)*
NFR-SEC-005	Oracle ERP & Comm4	Authentication will be handled by Active directory. AD shall support [Client] policies for password management.		**Met** - Validated Oracle Fusion authentication is handled by ADFS (currently, will be moved to Azure AD SSO). Email address is used as the authentication method between Oracle Fusion and ADFS. *REF: James Smith - RE: Document Review: Non-Functional Requirements v0.4[DRAFT] 15/05/2019 (email)*	**Met** - Validation [Client] internal user access to Comm4 is controlled using the [Client] LDAP, Microsoft Active Directory. *REF: Comm4 Application Technical Solution Design [p.8]*
NFR-SEC-006	Oracle ERP & Comm4	The system shall implement error message handling for failed user authentication.		**Met** - Validated	**Met** - Validated

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
				A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	The APEX framework used by COMM4 includes monitoring views that allow use to see all authentication attempts (successful and failed). *REF: NFRs: Initial questions for Inoapps-2 10/05/2019 (email)*
NFR-SEC-007	Oracle ERP & Comm4	Sensitive data and passwords, including incorrect password shall not be included in log files.		**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Met** - Validated Incorrect passwords are not written, in clear text, to log files. *REF: NFRs: Initial questions for Inoapps-2 10/05/2019 (email)*
NFR-SEC-008	Oracle ERP & Comm4	Credentials will not traverse any system or network unencrypted.		**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Not Met** – Further Input Required Additional security benefits could be achieved by adding an additional layer of SSL encryption to the account authentication process between [Client] AD and Comm4. *A move to ADFS is also an option.* *REF: Comm4 Application Technical Solution Design [p.9]*

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
NFR-SEC-009	Oracle ERP & Comm4	All transactions and communication to and from the system should be encrypted over a secure connection.		**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Met** - Validation Required There are several interfaces provisioned for Comm4. – All interfaces are secured using SSL Certs to encrypt the data in transit, ensuring the security and control of all data interface flows. *REF: Comm4 Application Technical Solution Design [P.11]*
NFR-SEC-010	Oracle ERP & Comm4	All client communication must be performed over a secure, authenticated connection.		**Met** - Validation Your access to Oracle Cloud Services is through a secure communication protocol provided by Oracle. If access is through a Transport Layer Security (TLS) enabled connection, that connection is negotiated for at least 128 bit encryption. The private key used to generate the cipher key is at least 2048 bits. TLS is implemented or configurable for all web-based TLS-certified applications deployed at Oracle. *REF: Oracle Cloud Hosting and Delivery Policies*	**Not Met** – Further Input Required AD connectivity is currently unencrypted.

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
NFR-SEC-011	Oracle ERP & Comm4	The system shall comply with current [Client] protocols for login, passwords, authentication, credentials, auditing. Policy for passwords: 1) Password expires after 60 days -> force reset 2) 5 incorrect password = locked for 15 mins 3) Password min 12 characters, needs to have at least X numeric and X alpha character.		**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Not Met** – Further Input Required Sub-contractor: o [Client] have not yet defined the required password policy for Subcontractor accounts, and as such no specific password policy regime is in place. • [Client] internal users: The password profile is defined within [CLIENT] security policy • Oracle Database Accounts: o The following password profile has been adopted: FAILED_LOGIN_ATTEMPTS 3 PASSWORD_LIFE_TIME 60 PASSWORD_LOCK_TIME 1 PASSWORD_REUSE_MAX 5 PASSWORD_REUSE_TIME 365 *REF: Comm4 Application Technical Solution Design [P.11]*
NFR-SEC-012	Oracle ERP & Comm4	Access to database layers, file systems and other non-end-user facing functions must be restricted.		**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Not Met** – Further Input Required Web/app and database on the same layer i.e. all on one VM (Virtual Machine).
NFR-SEC-013	Oracle ERP & Comm4	The data is to be stored on servers within the EU.		**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Met** - Validated

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
NFR-SEC-014	Oracle ERP & Comm4	The system must provide SSO (Single Sign-On) for user system access.		**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Not Met** – Further Input Required There is a desire within [Client] to implement a single sign on solution, but this is not part of the current solution. *REF: Comm4 Application Technical Solution Design [P.8]*
NFR-SEC-015	Oracle ERP & Comm4	Data at rest, residing in the system database, shall be encrypted. **Justification:** Sensitive payment data and employee personal data is stored in the database.		**Not Met** – Further Input Required Data encryption is not enabled by default. It is an optional feature that requires additional licencing.	**Met** - Validated Comm4 database uses Oracle Transparent Data Encryption (TDE) to secure all database data files and backups. Encrypted data is also protected in temporary tablespace, undo segments and redo logs. *REF: Comm4 Application Technical Solution Design [p.10]*
NFR-SEC-016	Comm4	User identities for external/sub-contractor users that are stored in the database shall be encrypted.			**Met** - Validated User credentials stored in the database are encrypted. *REF: NFRs: Initial questions for Inoapps-2 01/05/2019 (email)*
NFR-SEC-017	Oracle ERP & Comm4	The service shall be protected against malicious interference.	The service has to be protected from infection by unauthorised attacks or undesirable software programs: DoS, dictionary attack, brute force attack, viruses, worms, Trojan horses and others.	**Met** - Validated Covered in the penetration test report. *REF: Oracle Confidential Security Assessment Fusion Release 13*	**Not Met** – Further Input Required *"…WAF (Web Application Firewall) was mentioned at the time of the project but was not implemented…"* *REF: NFRs: Initial questions for Inoapps-3 23/05/2019 (email)*

NFR-ID	System	Requirement Statement	Note		Current State	
					HCM/ERP Cloud	Comm4
NFR-SEC-018	Oracle ERP & Comm4	The system shall pass a penetration test with no critical failures and an acceptable non critical failures.			Met - Validated	Not Met – Further Input Required
					Penetration testing done by Secarma Ltd. *REF: Oracle Confidential Security Assessment Fusion Release 13*	*"…no penetration testing was done, but again there is no reason not to consider it now you are revisiting things."* *REF: NFRs: Initial questions for Inoapps-3 23/05/2019 (email)*

7. Scalability Requirements

Scalability is specified as how well the system is able to expand its processing capabilities upward and outward to support business growth. A system is described as scalable, if it will remain effective when there is a significant increase in the number of resources and the number of users. The solution must allow the hardware and the deployed software services and components to be scaled horizontally as well as vertically. Horizontal scaling involves replicating the same functionality across additional nodes; vertical scaling involves adding more resources such as memory, CPU and storage to existing infrastructure.

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
NFR-SCL-001	Oracle ERP & Comm4	The system must be scalable to support 5 years of projected growth with an expected growth rate of 20% from the user/data volume listed in Appendix B.		Met - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	Pending – Further Input Required

8. Interoperability Requirements

Interoperability is the extent to which the software system is able to couple or facilitate the interface with other systems.

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
NFR-INT-001	Oracle ERP & Comm4	An interface shall resume data sync after a service disruption	An interface must be able to recover from a failed execution without data loss and maintaining integrity of the data.	**Met** - Validated The interfaces between Fusion and the Integration Database have been (or will be) developed so they can be recovered, either by doing a full transfer or incremental transfer with data stamp.	**Pending** – Further Input Required Synchronisation processes have been written that allow data in Fusion to be synchronised with Comm4. The process would view what data is in Comm4 against what is in FUSION, and the difference is then synchronised with Comm4. As such, and any temporary loss of service would be fully recovered from, and no data would be lost as a result. Outbound interfaces to Oracle are asynchronous and messages can be 'replayed'. ***REF***: *Comm4 Application Technical Solution Design [p.12] and meeting with Inoapps 3rd May 2019.*
NFR-INT-002	Oracle ERP & Comm4	Any time-critical interface must complete within the allocated time window.		**Pending** – Further Input Required [Further analysis required.]	**Pending** – Further Input Required [Further analysis required.]
NFR-INT-003	Oracle ERP & Comm4	An interface failure must be logged in a log file.		**Pending** – Further Input Required [Further analysis required.]	**Met** - Validated Log tables in the COMM4 database record the requests and responses for all interface calls that write data from COMM4 to Fusion.

					REF: NFRs: Initial questions for Inoapps-2 10/05/2019 (email)
NFR-INT-004	Oracle ERP & Comm4	Interfaces inbound/outbound from/to external systems must be encrypted.		**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Met** - Validation Required There are several interfaces provisioned for Comm4. – All interfaces are secured using SSL Certs to encrypt the data in transit, ensuring the security and control of all data interface flows. *REF: Comm4 Application Technical Solution Design [P.11]*
NFR-INT-005	Oracle ERP & Comm4	All reports that have been identified for printing shall allow 'print friendly' printing on [Client] printers.	Printable on A4 and A3 paper.	**Met** - Validation A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Met** - Validation

9. Recoverability Requirements

Recoverability addresses how quickly a system can be recovered, with minimum or no data loss, after experiencing a system failure.

NFR-ID	System	Requirement Statement	Note	Current State HCM/ERP Cloud	Comm4
NFR-REC-001	Oracle ERP & Comm4	The RPO (Recovery Point Objective) must not exceed 1 hour. **Justification:** Loss of data over an hour will require significant manual intervention.	Refer to Appendix A for an explanation of the RPO.	**Met** - Validated The RPO is 1 hour. The RPO is Oracle's objective for the maximum period of data loss measured as the time from which the first transaction is lost until Oracle's declaration of the disaster. The RPO does not apply to any data loads that are underway when the disaster occurs. *REF: Oracle SaaS Public Cloud Services*	**Not Met** – Further Input Required The RPO to 24 hours. Recovery point objective is Inoapps objective for the maximum period of data loss measured as the time from which the first transaction is lost. *REF: Comm4 Application Technical Solution Design [P.23]*
NFR-REC-002	Oracle ERP & Comm4	The RTO (Recovery Time Objective) must not exceed 12 hours.	Refer to Appendix A for an explanation of the RTO. The RTO should also cover the following low risk and high impact scenarios: 1. Data corruption has occurred 2. Failure of SAN technology (dual site). RTO excludes incident management 'think time', to make a decision on recovery. RTO Includes time to recover from a	**Met** - Validated The RTO is 12 hours. The RTO is Oracle's objective for the maximum period of time between Oracle's decision to activate the DR recovery processes described in this document to failover the Oracle SaaS Public Cloud Service to a secondary site due to a declared disaster and the point at which You can resume production operations in the standby production environment at the secondary site. *REF: Oracle SaaS Public Cloud Services*	**Not Met** – Further Input Required The RTO is 24 hours. Recovery time objective is Inoapps objective for the maximum period of time between Inoapps decision to activate a recovery and the service being restored. *REF: Comm4 Application Technical Solution Design [P.23]*

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
			backup and apply redo/archive logs.		
NFR-REC-003	Oracle ERP & Comm4	Upon performing data recovery, the system shall be able to catch-up and remain consist with the integrated systems.	It must be possible to re-synchronise the data across the systems without data integrity impacts.	**Met** - Validated A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	**Met** - Validation Required Synchronisation processes have been written that allow data in Fusion to be synchronised with Comm4. The process would view what data is in Comm4 against what is in FUSION, and the difference is then synchronised with Comm4. As such, and any temporary loss of service would be fully recovered from, and no data would be lost as a result. **REF**: *Comm4 Application Technical Solution Design [p.12]*
NFR-REC-004	Oracle ERP & Comm4	A backup process must be utilised to support the required RPO.		**Met** - Validated Recovery Manager (RMAN) is used to take weekly backup of Oracle Databases. **REF**: *Oracle Fusion Cloud Service Backup Practices*	**Not Met** – Further Input Required Current backup process does not support required RPO.
NFR-REC-005	Oracle ERP & Comm4	Backups must be copied to a secondary storage media to mitigate against disk storage failure.		**Met** - Validated Weekly backup, 7 days retention on disk and 60 days retention on tape. **REF**: *Oracle Fusion Cloud Service Backup Practices*	**Not Met** – Further Input Required Object Storage Classic backups are in the same datacentre as the DBaaS, identity domains created before 2018 march do not have geo replication support by default.

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
NFR-REC-006	Oracle ERP & Comm4	Backups on secondary storage media must be sent offsite to mitigate against a site disaster.		**Met** - Validated Tapes are sent to an offsite location on a weekly basis. *REF: Oracle Fusion Cloud Service Backup Practices*	**Not Met** – Further Input Required
NFR-REC-007	Oracle ERP & Comm4	All backups of the system shall be encrypted on disk and on secondary storage.		**Not Met** – Further Input Required Data encryption is not enabled by default. It is an optional feature that requires additional licencing. *REF: Oracle meeting (08/05/2019)*	**Not Met** – Further Input Required

10.Operability Requirements

Operability is the ability to keep a system in a safe and reliable functioning condition, according to pre-defined operational requirements.

NFR-ID	System	Requirement Statement	Note	Current State HCM/ERP Cloud	Current State Comm4
NFR-0PR-001	Oracle ERP & Comm4	The service availability shall be monitored either by [Client] IT (via a portal provided by the service provider) or by the service provider who will inform [Client] IT of any outages.		**Met** - Validated Oracle will provide You with access to a Customer notifications portal. This portal will provide metrics on the Service Availability Level for Oracle Cloud Services that You purchased under Your order. **REF:** *Oracle Cloud Hosting and Delivery Policies*	**Met** - Validation Required
NFR-0PR-002	Oracle ERP & Comm4	[Client] IT or the service provider will have an automated tool set to monitor service availability and enable monthly availability reporting.		**Met** - Validation Required See above.	**Pending** – Further Input Required
NFR-0PR-003	Oacle ERP & Comm4	[Client] IT or the service provider shall have an automated tool set to monitor service online performance and enable monthly system performance monitoring reports.		**Met** - Validation Required See above.	**Pending** – Further Input Required Inoapps monitoring is deployed on all servers before the project goes live. This ensures all instances can be monitored during key phases of the project. This service is only available to Inoapps staff and will be used to manage the Comm4 service. **REF**: *Comm4 Application Technical Solution Design [P.24]*
NFR-0PR-004	Oracle ERP & Comm4	In the event of a termination of service, the service provider must provide secure access to retrieve content/data held on the cloud service		**Met** - Validation Required For a period of 60 days upon termination of the Oracle Cloud Services, Oracle will make available via secure protocols, Your Content	**Not Met** – Further Input Required To be included in future Inoapps support contract.

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
				residing in the production Cloud Services environment, or keep the service system accessible, for the purpose of data retrieval by You. *REF: Oracle Cloud Hosting and Delivery Policies*	
NFR-0PR-005	Oracle ERP & Comm4	[Client] IT or the service provider shall have the capability to monitor the inbound/outbound interfaces	Automated interfaces need be monitored for failure and, if relevant, against expected runtimes.	Pending – Further Input Required Not clear whether there is a consistent mechanism to monitor interfaces into the integration DB.	Not Met – Further Input Required *"Currently there has been no specific additional requirement requested for monitoring for [Client], so it Is just the standard monitoring. But it can be done if the requirements are defined and setup.* *So if additional monitoring goes into your NFRs you are producing then this can be setup."* *[Duncan, Inoapps]* *REF: NFRs: Initial questions for Inoapps-2 14/05/2019 (email)*
NFR-0PR-006	Oracle ERP & Comm4	The system shall be cloned from the Production to a Test or Development environment on request by [Client].	The clone of the system should be available for [Client] Dev and Test environments. Also, the environments should not run on the same hardware as the live service.	Met - Validation Required A standard requirement considered to be met by an enterprise solution such as Oracle ERP Cloud.	Not Met – Further Input Required The technical solution exists. To include in future support contract with time limit of 2 business days.
NFR-0PR-007	Comm4	An escrow agreement must be in place to give [Client] access to the Comm4 source code in case Inoapps becomes insolvent.	Storing source code and other critical material with an independent neutral 3rd party escrow agent.		Not Met – Further Input Required To be included in future Inoapps support contract.

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
NFR-0PR-008	Comm4	In case Inoapps becomes insolvent, the relevant Oracle IaaS and DBaaS services should be able to transfer ownership to [Client].			Not Met – Further Input Required To be included in future Inoapps support contract.
NFR-0PR-009	Oracle ERP & Comm4	The service should provide a configurable archiving capability.		Pending – Further Input Required	Not Met – Further Input Required
NFR-0PR-010	Oracle ERP & Comm4	Scheduled batch processes must not use hardcoded dates and must be configurable.	Periodic processing dates must not be hard coded and should be configurable to consider public holidays and territorial differences, or other such eventualities (e.g., re-running the monthly batch).	Pending – Further Input Required	Pending – Further Input Required
NFR-0PR-011	Oracle ERP & Comm4	The service shall automatically purge redundant files transferred to external systems.	An automated facility must exist to purge redundant files after transfer to external systems has occurred and confirmation of receipt has been received.	Pending – Further Input Required	Pending – Further Input Required
NFR-0PR-012	Oracle ERP & Comm4	The service provider shall ensure that the service is on a supported software version.		Met - Validation Required	Met - Validation Required

11. Performance Requirements

Performance requirements focus on the responsiveness of a system to perform specific actions in a given time span. Performance is measured in terms of throughput or latency. Latency is the time taken by the application to respond to an event. Throughput is the number of events measured in a given time interval. The performance targets shall be considered against the volumetrics in Appendix B.

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
NFR-PER-001	Comm4	Page response times shall take less than 2 seconds for 80% of the pages when accessed in the UK over a fast internet connection (so that 'server time' is considered instead of bandwidth').	A performance objective is proposed for Comm4 given this is a custom solution developed for [Client]. Fast internet connection: At a minimum, this should meet the UK national average of 54.2Mbps download and 7.2Mbps upload (Ofcom Home Broadband Report 2018)	Oracle does not guarantee performance response times. However, response times are monitored. There is a performance support team. [Client] is a medium size customer.	Pending – Further Input Required
NFR-PER-002	Comm4	Production of a simple report shall take less than 5 seconds for 80% of the cases.	This includes users outside of Europe.	Oracle does not guarantee performance response times. Reports may be tuned, possibly with support from the performance team.	Pending – Further Input Required
NFR-PER-003		The service shall be sized to meet peak utilisation and the peak number of users as referenced in the Appendix B.		Pending – Further Input Required	Pending – Further Input Required

Users in other (international) offices may experience a reduced performance based on the available internet connectivity.

12.Regulatory & GDPR Requirements

The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment. The regulation contains provisions and requirements pertaining to the processing of personal data of individuals.

NFR-ID	System	Requirement Statement	Note	Current State	
				HCM/ERP Cloud	Comm4
NFR-GDP-001	Oracle ERP & Comm4	The system shall comply with the [Client] retention policy, as set forth in Appendix B.		**Not Met** – Further Input Required The data retention policy has not been implemented, including for HCM. *REF: [Client] Group - DPIA of Oracle Cloud Services [p.17]*	**Not Met** – Further Input Required The data retention policy has not been implemented.
NFR-GDP-002	Oracle ERP & Comm4	The system shall support a DSAR (Data Subject Access Requests).	The data subject should have a right to a copy of their data in a commonly used format. This can be in the form of a CSV, Excel, XML etc.	Met - Validated A manual task performed by Oracle support, when requested by the client. *REF: Oracle meeting (08/05/2019)*	Met - Validated Yes, it would be possible to extract in any format mentioned - this would be a manual support task. *REF: NFRs: Initial questions for Inoapps-2 10/05/2019 (email)*
NFR-GDP-003	Oracle ERP & Comm4	The system shall technically support a "right to forget" request by an ex-employee.		Met - Validated A manual task performed by Oracle support, when requested by the client. *REF: Oracle meeting (08/05/2019)*	Met - Validated If it were required/possible to completely remove the record from Fusion, then we could also completely remove the associated record from COMM4 if needed. This would be a manual support task. *REF: NFRs: Initial questions for Inoapps-2 10/05/2019 (email)*

NFR-GDP-004	Oracle ERP & Comm4	The system shall technically support a "right to forget" request by contact.		**Met** - Validated A manual task performed by Oracle support, when requested by the client. *REF: Oracle meeting (08/05/2019)*	**Met** - Validated If it were required/possible to completely remove the record from Fusion, then we could also completely remove the associated record from COMM4 if needed. This would be a manual support task. *REF: NFRs: Initial questions for Inoapps-2 10/05/2019 (email)*
NFR-GDP-005	Oracle ERP & Comm4	The system shall encrypt personal data held in the database.	In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Recitals 83 and Articles 6-4(e), 32-1(a)	**Not Met** – Further Input Required Data encryption is not enabled by default. It is an optional feature that requires additional licencing. *REF: Oracle meeting (08/05/2019)*	**Met** - Validation Required Comm4 database uses Oracle Transparent Data Encryption (TDE) to secure all database data files and backups. Encrypted data is also protected in temporary tablespace, undo segments and redo logs. *REF: Comm4 Application Technical Solution Design [p.10]*
NFR-GDP-006	Oracle ERP & Comm4	Data access shall be GDPR compliant in Non-Production environments.		**Pending** – Further Input Required	**Pending** – Further Input Required

13.Assumptions, Dependencies and Risks

The document is based on following key assumptions. In case these assumptions no longer hold, then this will impact the content of this document:

Nb.	Assumption
01	Any foreign currency requirements need to be covered in functional requirements and are considered out of scope for the NFRs.
02	Requirements for auditing of actions such as creation/deletion of users and assets are considered out of scope for the NFRs.
03	Role-based access control is available on both Oracle ERP Cloud and Comm4. However, at the time of writing, the implementation of role-based access is under review and has not been fully implemented. It is assumed that the specific requirements for role-based access will be implemented as part of functional activities.
04	It is assumed that the specific requirements for system audit logging are not part of the NFRs. These are considered functional requirements.
05	It is assumed that service related requirements such as incident and request resolution SLA's and support hours will be defined in the service contract. For Oracle these are already available. For Comm4, this is assumed to be covered in the future SaaS support contract. These NFRs have been omitted on purpose from this document to avoid overlap.

This document is dependent on following external dependencies:

Nb.	Dependency

The key risks for the Non-Functional Requirements are as follows:

Nb.	Risk	Action (Accept, mitigate, avoid, transfer)
01	**Performance:** The Comm4 service has not been performance tested and therefore there is a risk that the service may not perform sufficiently to accommodate future load requirements. Whilst many performance issues could be addressed during a 'slow ramp-up' by SQL tuning or hardware scaling, re-architecting the infrastructure or the software solution may delay the deployment.	**Mitigate:** Conduct a performance test with adequate representative data and user volumes to identify software architectural issues. (Alternative option is Avoid: provide performance monitoring and, if required, tuning during ramp-up.)
02	**Operability:** It is not clear whether interfaces are consistently monitored.	**Mitigate:** Further analysis required.

Nb.		
03	**Interoperability:** There are several interfaces between Oracle and COMM4 resp. [Client]'s legacy systems that are not incremental. Over time, these may result in performance issues.	**Mitigate:** Conduct a performance test with adequate representative data to identify interface performance issues. (Alternative option is Avoid: provide performance monitoring and, if required, tuning during ramp-up.)

14. Open Issues

The following Open Issues have been identified against the NFRs to date. Note that not all issues carry the same impact – and these have not been prioritised.

Nb.	Issue
01	**Availability:** The [Client] on-premise Active Directory domain controller used by Comm4 represents a single-point-of-failure. Therefore, if the domain controller becomes unavailable then the Comm4 service will not be accessible by front-end users.
02	**Security:** The connectivity between the [Client] on-premise Active Directory server and the Comm4 service is unencrypted. Therefore, user credentials are being exposed to the outside world.
03	**Security:** Role-based access control is available on both Oracle ERP Cloud and Comm4. At the time of writing, this functionality has not been fully implemented. However, it is planned to be implemented in ERP R2/R3.
04	**Accessibility:** Comm4 does not comply with the Equality Act 2010 for UI accessibility. This is a legal requirement.
05	**Availability:** The Comm4 service architecture, web/app and database, has been deployed to a single Virtual Machine, which presents a single point of failure.
06	**Recoverability**: The existing Comm4 backup strategy will not meet the required RPO of 1 hour. Comm4 currently supports an RPO of 24 hours, which is unacceptable to the business.
07	**Recoverability:** The Comm4 service architecture does not utilise a DR site. If the Production site becomes unavailable, then this may cause a major service outage.
08	**Security:** There is no password policy defined for sub-contractor accounts in Comm4. This needs to be defined by [Client] and communicated to Inoapps.
09	**Security:** SSO has not been implemented for Comm4.
10	**Regulatory / GDPR and Security:** Data at rest is not encrypted in Oracle ERP Cloud. Therefore, sensitive data is at risk of being exposed. Data encryption is an optional feature that requires additional licencing.
11	**Recoverability:** Comm4 backups are not transferred off-site. Therefore, if the Production site is destroyed in a disaster then all data will be lost.
12	**Operability, Contractual:** An escrow agreement is not in place with Inoapps. Therefore, the Comm4 service may not be available if Inoapps becomes insolvent.
13	**Scalability:** The Comm4 service architecture (infrastructure) is not horizontally scalable.
14	**Recoverability and Security:** The Comm4 service architecture, web/app and database, has been deployed to a single Virtual Machine, which presents a security risk. There is no DMZ.

15	**Regulatory / GDPR:** [Client]'s data retention policy has not been implemented on Oracle and Comm4. This implementation may be process-driven or it may require system changes. Specifically, this applies to HCM.
16	**Operability, Contractual:** In case Inoapps becomes insolvent, the relevant Oracle IaaS and DBaaS services should be able to transfer ownership to [Client]. This is not in place today.
17	**Operability, Contractual:** In case [Client] end service with Inoapps, or equivalent, Inoapps should provide the Comm4 data to [Client].
18	**Regulatory / GDPR:** There is no evidence to suggest that adequate access roles have been defined in HCM. (Audit and tailoring of the user access management roles in HR.)
19	**Security:** Penetration testing has not been performed on Comm4. Therefore, the service may be vulnerable to security threats.
20	**Recoverability:** The Comm4 solution does not meeting the requirement RTO, Recovery Time Objective, of 12 hours.
21	**Accessibility:** Inoapps does not currently support the Comm4 UI on mobile devices. Retrospectively, this requirement indicates a desire for the Comm4 UI to support mobile devices. However, the pursuit of this requirement needs to be balanced with the understanding of the cost and effort required to enable mobile device support.

15. Appendix A – RTO & RPO Explained

15.1 Recovery Time Objective

The RTO is a measurement, as a unit of time(hours), of how long the business can survive following a disaster before operations are reinstated. If the RTO is 12 hours, it means that the business can sustain operations for 12 hours without the system being available. If the system is not recovered within 12 hours, the business could endure severe reputational or financial damage.

15.2 Recovery Point Objective

The RPO is a measurement, as a unit of time(hours), of the maximum acceptable amount of data that can be lost following a disaster. It measures how much time can occur between the last data backup and a disaster without causing serious harm to the business. RPO is useful for determining how often to perform data backups.

If the RPO is 1 hour, it means it's acceptable for the business to lose no more than 1 hour of data. Therefore, an hourly data backup should be taken.

15.3 Required RTO and RPO for Oracle ERP Cloud and Comm4

The diagram below illustrates the RTO and RPO requirements for Oracle ERP Cloud and Comm4:
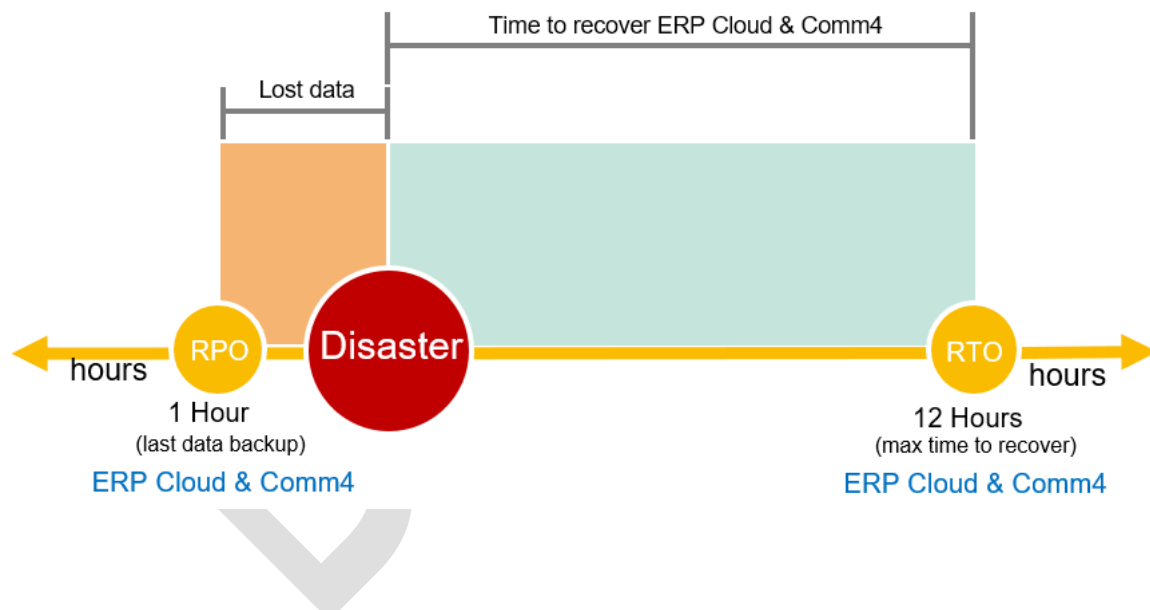
16. Appendix B – Reference Documents

16.1 Volumetrics

The attached document presents the volumetric data collected so far. Additional work needs to be done, outside of this document, to ensure the data is complete and accurate.

16.2 User Volumetrics

HCM/ERP

Area/Function	Current	Forecast after 5 years
ERP		
AP	60	90
AR	60	90
GL	75	100
Assets	75	100
Projects	700	1,000
Procurement	1,000	1,400
Expenses	4,000	5,500
HCM		
Workers	6,300	9000

Comm4

User Types	Total	Concurrent Avg	Concurrent Peak	Peak Time in Month	Forecast after 5 years
Cost Managers	200	40	80	month-end	250
Subcon/Designer	600	20	300	spread across month	750
Finance	20	10	20	First 10 days of month	25
Total	820	70	400		1025

16.3 [Client] Retention Policy

16.4 DPIA of Oracle Cloud Services

16.5   Summary NFRs

The attached summary NFR document was presented to the business directors for approval.