Master SaaS Framework

ProjectVIEW ERP — Cloud Platform Reference

This document serves as a comprehensive reference collateral to the commercial agreement for the DANAOS ProjectVIEW ERP SaaS Platform.

Document Type	Client Reference Collateral
Version	4.0
Classification	Confidential
Date	January 2026
Provider	DANAOS Projects Software Solutions LLC
Jurisdiction	Dubai, UAE
SLO Target	99.9% Monthly Uptime
Chapters	12

Table of Contents

1 Definitions & Interpretation

1.1 Definitions

In this Framework, unless the context otherwise requires, the following terms shall have the meanings set out below:

Term	Definition
Acceptable Use Policy	The set of rules and restrictions governing the Customer's and its Authorised Users' permitted use of the Platform/Applications/Portals of ProjectVIEW ERP and/or all associated Addons, including prohibitions on unlawful use, reverse-engineering, credential sharing, and automated scraping, as defined in Chapter 12.
AI Agent (Software Quality)	A custom AI Testing Agent configured with Customer-specific domain knowledge (module configuration, business rules, data schema, role taxonomy) that autonomously executes test scenarios against the Customer's ProjectVIEW ERP instance via the Provider's secure API integration layer, as defined in Chapter 5.
Authorised User	Any individual who is authorised by the Customer to access and use the Platform, each of whom shall be assigned a unique user identity.
Availability	The percentage of time during a calendar month that the Platform is operational and accessible to Authorised Users, calculated in accordance with Section 3 (SLA).
Azure	Microsoft Azure, the cloud computing platform operated by Microsoft Corporation on which the Platform is hosted, including Microsoft Entra ID (formerly Azure Active Directory) for identity and access management.
ARR (Annual Recurring Revenue)	The annualised value of the Customer's subscription, comprising the aggregate of module subscription fees (per-user annual fees across all licensed modules within the applicable Volume Band), Addon/Connector/Portal subscription fees, and any recurring ancillary fees designated as ARR-contributing in the Commercial Contract. ARR excludes one-off implementation/services fees, bespoke customisation charges, Extended Support premiums, Escrow Agent fees, and accommodation costs. ARR is the basis for calculating SLA Non-Compliance Penalties (Chapter 3, §3.8) and is detailed in Chapter 11, §11.5.
Annual Subscription Fee	The annual fee payable by the Customer for access to the Platform based on the Universal/Concurrent User licensing model, as specified in the Commercial Contract. The fee is determined by the Volume Band applicable to the Customer's total Concurrent User count and encompasses platform access, dedicated cloud infrastructure, support services, releases, major-version upgrades, COTS maintenance, Lifetime Software Warranty, BCDR, and compliance. See Chapter 11, §11.4.1.
BCDR (Business Continuity & Disaster Recovery)	The Provider's integrated programme of business-continuity planning, backup management, data replication, and disaster-recovery procedures that ensure the Platform remains available and Customer Data remains recoverable within contracted RPO and RTO targets, as defined in Chapter 9.

BCMS (Business Continuity Management System)	The Provider's management system aligned with ISO 22301:2019, encompassing the policies, procedures, governance, and continual-improvement mechanisms that establish and maintain business-continuity capability for the Platform, as defined in Chapter 9.
BCP (Business Continuity Plan)	The documented set of procedures, roles, communication protocols, resource inventories, and recovery workflows that the Provider maintains to restore or sustain Platform services during a disruption, as defined in Section 9.8.2.
BIA (Business Impact Analysis)	A structured assessment that identifies critical business processes supported by the Platform, maps their dependencies on Platform components, and quantifies the impact of service disruption to calibrate recovery objectives (RPO/RTO), as defined in Section 9.8.1.
Billing Period	A period of twelve (12) months starting on the date of the Framework (Contract) signing, representing one annual licensing subscription cycle. Each Billing Period includes Second Level Support (maintenance and support) and free Software Updates and Upgrades. See Chapter 11, §11.12.1.
Binding Period	The minimum subscription commitment binding the Customer to ProjectVIEW ERP enrolment, comprising the number of Billing Periods specified in the Commercial Contract. Neither Party may terminate for convenience during the Binding Period. See Chapter 11, §11.12.1.
Business Day	Any day other than a Friday, Saturday, or public holiday in the United Arab Emirates, unless otherwise agreed between the Parties.
CAB (Change Advisory Board)	The governance body responsible for reviewing, approving, or rejecting Normal and Emergency changes to the Platform, as detailed in Section 4.6.
Cessation Plan	The structured exit plan prepared by the Provider upon receipt of a Customer's formal notification to cease the Subscription without transitioning to the successor version. The Cessation Plan covers data return, environment decommissioning, integration disconnection, and surviving-obligation management, as defined in Section 10.9.
Change Request	A formal request for modification to the Platform's configuration, functionality, or integration, managed through the Change Management process defined in Section 4.6.
Champion (DANAOS ProjectVIEW ERP)	A Customer-designated senior power user who has completed the specialised Champions Training Programme and passed the formal Champion examination (§6.6.3). Each Customer must designate a minimum of two (2) Champions (Main and Deputy). Champions serve as the Customer's Level 1 support contact for intranet (company) and extranet (portal) users, and as the primary communication channel with the Provider from Go-Live onwards (§6.6.4).
CI/CD (Continuous Integration / Continuous Delivery)	The Provider's automated software delivery pipeline that builds, tests, and deploys code changes from the Git repository through to the Staging Environment, ensuring consistency and reducing manual deployment errors.
CMT (Crisis Management Team)	The Provider's designated leadership team activated during DR-1 and DR-2 disaster-recovery events, comprising the CTO (Incident Commander), Cloud Operations Lead, DBA Lead, Customer Account Manager, and Communications Lead, as defined in Section 9.8.2.

CSI (Continual Service Improvement)	The ITIL-aligned programme operated by the Provider to drive ongoing improvements in service quality, operational efficiency, and Customer satisfaction, as defined in Section 4.10.
CISO	Chief Information Security Officer — the Provider's designated executive responsible for the information-security programme, ISMS governance, and approval of security-related changes, as referenced in Chapter 8.
Concurrent User	An individual simultaneously logged in and actively using the Platform under the Universal/Concurrent User licensing model. The number of Concurrent Users at any point in time shall not exceed the Customer's licensed Universal User count as specified in the Commercial Contract and governed by the applicable Volume Band. See Chapter 11, §11.3.2.
Confidential Information	All information disclosed by one Party to the other, whether orally, in writing, or by any other means, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of disclosure.
CSP (Content Security Policy)	An HTTP security header enforced by the Platform to mitigate cross-site scripting (XSS) and data-injection attacks by specifying approved content sources, as defined in Section 8.4.4.
CVSS (Common Vulnerability Scoring System)	An industry-standard framework for rating the severity of software vulnerabilities on a 0.0–10.0 scale, used by the Provider to prioritise vulnerability remediation timelines, as defined in Section 8.7.2.
Customer	The entity identified in the Commercial Contract that has entered into this Framework for the provision of the Platform and related Services.
Customer Data	All data, information, documents, and materials uploaded to, generated within, or processed by the Platform by or on behalf of the Customer, including Personal Data.
Data Controller	As defined in Article 4(7) of the GDPR: the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. In respect of Customer Data, the Customer acts as Data Controller.
Data-Integrity Report	An automated report generated by AI agents at the conclusion of each test cycle, documenting the results of referential, computational, and temporal integrity assertions executed against the Customer's data schema, as defined in Section 5.7.3.
Data Processor	As defined in Article 4(8) of the GDPR: the natural or legal person which processes Personal Data on behalf of the Data Controller. In respect of Customer Data, the Provider acts as Data Processor.
Data Protection Laws	The General Data Protection Regulation (EU) 2016/679 (GDPR), the UAE Federal Decree-Law No. 45 of 2021 on Personal Data Protection (PDPL), and any other applicable data protection and privacy legislation in the jurisdictions in which the Parties operate.
Data Subject	An identified or identifiable natural person whose Personal Data is processed under this Framework, as defined in Article 4(1) of the GDPR and Article 1 of the UAE PDPL.
DIAC (Dubai International Arbitration Centre)	The arbitration and mediation institution designated under this Framework for the resolution of disputes that cannot be settled through good-faith negotiation. Mediation and binding arbitration shall be conducted under DIAC's applicable rules, with the seat in Dubai, UAE, as defined in Chapter 12, §12.10.

Decommissioning Certificate	A formal written confirmation issued by the Provider upon completion of all environment-decommissioning activities, certifying that all Customer Data has been permanently erased from production, staging, and backup infrastructure in accordance with NIST SP 800-88 media-sanitisation guidelines, as defined in Section 10.10.
Platform Release Centre	The Provider's integrated release management module within the ProjectVIEW ERP Platform, used for release distribution, version tracking, and deployment history. Provides role-based access to release catalogues, release notes, and deployment records directly within each Customer's Platform environment.
DPA	Data Processing Agreement, the terms governing the processing of Personal Data by the Provider on behalf of the Customer, as set out in Section 17.
DPO	Data Protection Officer, the individual appointed by the Provider in accordance with Articles 37–39 of the GDPR and Article 10 of the UAE PDPL to oversee data protection compliance.
DR (Disaster Recovery)	The set of policies, procedures, and technical mechanisms used to recover or continue the operation of the Platform following a significant disruption, including failover to secondary infrastructure, database restoration, and service verification, as defined in Section 9.7.
DAST (Dynamic Application Security Testing)	Automated runtime testing of the deployed Platform to detect security vulnerabilities (e.g., OWASP Top 10) in the Staging Environment before production deployment, as defined in Section 8.9.
Embedded Ticketing System	The native ITSM ticketing capability built into the ProjectVIEW ERP Platform, serving as the system of record for all support interactions including incident logging, service requests, ticket lifecycle tracking, SLA measurement, and reporting, as detailed in Section 4.2.1.
EBCM (Enterprise Business Continuity Management)	Microsoft's Enterprise Business Continuity Management programme governing Azure platform resilience, availability-zone architecture, and geo-redundant infrastructure, upon which the Provider's BCDR commitments are predicated, as referenced in Section 9.3.
Enterprise License Agreement (ELA)	The licensing instrument governing the Customer's entitlement to use the ProjectVIEW ERP Platform under the Universal/Concurrent User model. The ELA specifies the Volume Band, Binding Period, Billing Period, licensed modules, Addon/Connector/Portal entitlements, and associated fee schedule. The ELA is appended to or incorporated within the Commercial Contract. See Chapter 11, §11.3.1.
Evergreen Contract	The auto-renewal mechanism whereby the Subscription Term renews automatically at the expiry of each Billing Period beyond the Binding Period, unless terminated by either Party in accordance with the notice provisions set out in Chapter 11, §11.12.2.
EOE (End of Engineering)	The date after which the Provider ceases all feature development, non-critical bug fixes, and enhancement work for a given major version. Critical-security and P1-severity patches continue until the End-of-Life (EOL) date. EOE is triggered thirty (30) days before EOL, as defined in Section 10.3.
EOL (End of Life)	The date after which a major version of the Platform is no longer supported, patched, or hosted by the Provider under standard Subscription terms. All Customers must have transitioned to the successor version or ceased their Subscription by the EOL date, as defined in Section 10.3.

Escrow Agent	The independent third-party custodian appointed by the Provider to hold the Platform's source code, build scripts, database schemas, and deployment documentation under a Source Code Escrow arrangement. The Escrow Agent releases the deposit to the Customer upon the occurrence of specified release conditions (insolvency, cessation of business, material breach, or product discontinuation), as defined in Section 9.14.
Extended Support	An optional, time-limited support arrangement available for up to twelve (12) months post-EOL, providing P1/P2 incident response and critical-security patching only, at a premium of twenty percent (20%) of the prevailing ARR, as defined in Section 10.13.
Executive Steering Committee	The highest governance body comprising senior representatives from both Parties (minimum two per Party), convened semi-annually to review strategic alignment, approve material changes, resolve escalated disputes, and endorse improvement plans, as defined in Chapter 12, §12.1.2.
Extranet User	A User classified under the Intranet/Extranet licensing model who accesses the Platform exclusively through portal-based interfaces with limited functional scope. Extranet Users are typically external stakeholders (e.g., sub-contractors, blue-collar site personnel, external project managers) who require visibility into specific project data without full module access. See Chapter 11, §11.3.3.
Flexible Subscription Model	The usage-based mechanism enabling the Customer to add or remove Universal User Licences during the Subscription Term, subject to the Minimum Licence Commitment. Additions are invoiced pro-rata from the Activation Date. Removals take effect at the next Billing Period renewal. See Chapter 11, §11.3.6.
Force Majeure Event	Any event beyond the reasonable control of a Party, including acts of God, war, terrorism, pandemic, governmental action, fire, flood, earthquake, cyber-attack by state actors, or failure of third-party telecommunications or power supply.
GA (General Availability)	The date on which a new major version of the Platform is officially released for production deployment to all Customers, marking the commencement of full support, SLA coverage, and the standard version-lifecycle timeline, as defined in Section 10.3.
GAP Analysis Document	A consolidated report produced by the Provider at the conclusion of the implementation training phase (§6.4.6), categorising all qualms, configuration requirements, and change requests registered by attendees during training. The GAP Analysis Document is formally presented to the Customer for written approval and forms a binding addendum to the Implementation Plan.
Go-Live	The date on which the Production Environment is made available to all Authorised Users for live operational use, following successful completion of UAT and written Customer sign-off. Upon Go-Live, the Development/Sandbox environment transitions to become the Staging Environment.
Governance Action Register	The shared action log maintained by the Provider to track decisions, action items, and follow-ups arising from all governance meetings (Monthly Operations, QSR, and Executive Steering Committee). Actions not closed within two (2) consecutive review cycles are automatically escalated to the next governance tier, as defined in Chapter 12, §12.1.4.

GOS (Grade of Service)	The percentage of Incidents within each priority level that are resolved within the applicable MTTR target during the measurement period, as defined in Section 3.6.
GRS (Geo-Redundant Storage)	An Azure Storage replication option that maintains six copies of Customer Data — three in the primary Azure region and three in a geographically paired secondary region (hundreds of kilometres apart) — providing 16-nines durability with automatic cross-region failover, as defined in Section 9.6.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.
Hypercare	An intensified post-migration support period of thirty (30) days during which the Provider allocates dedicated resources for accelerated incident resolution, configuration fine-tuning, and user-adoption monitoring following a version transition, as defined in Section 10.5.
IMAC/RD	Install, Move, Add, Change, Remove, Dispose — the categories of service requests managed under this Framework, as detailed in Section 4.8.
IRBC (ICT Readiness for Business Continuity)	The extension of business-continuity management to information and communication technology services as defined in ISO 27031:2011, ensuring ICT systems can support the Provider's business-continuity objectives within agreed RPO and RTO targets, as referenced in Section 9.3.
ITIL	Information Technology Infrastructure Library — the globally recognised framework of best practices for IT service management. The Provider aligns its support processes with ITIL 4 guidelines.
ITSM (IT Service Management)	The Provider's IT Service Management capability, delivered through the Platform's Embedded Ticketing System, used for recording, tracking, managing, and reporting all support tickets, incidents, service requests, problems, and change requests throughout their lifecycle.
Incident	An unplanned interruption to or reduction in the quality of the Platform or Services that requires remedial action by the Provider.
Initial Term	The initial period of the subscription commencing on the Subscription Start Date and continuing for the duration of the Binding Period as specified in the Commercial Contract and Enterprise License Agreement. The Initial Term comprises the minimum number of consecutive Billing Periods during which the Customer is contractually bound to the Platform. See Chapter 11, §11.12.1.
Intranet User	A User classified under the Intranet/Extranet licensing model who accesses the full Platform functionality through the internal corporate network or VPN. Intranet Users are typically white-collar office-based personnel (e.g., project managers, quantity surveyors, procurement officers, finance teams) with enhanced module access. See Chapter 11, §11.3.3.
Intellectual Property Rights	All patents, copyrights, trademarks, trade secrets, database rights, design rights, know-how, and all other intellectual property rights, whether registered or unregistered, and all applications for the same.
LRS (Locally Redundant Storage)	An Azure Storage replication option that maintains three copies of Customer Data within a single facility in a single Azure region, providing 11-nines durability. Used for non-critical temporary storage where cross-facility redundancy is not required, as defined in Section 9.6.

Knowledge Base	The Provider's comprehensive repository of platform documentation, process guides, video tutorials, FAQ articles, and release notes, hosted on the the Platform's integrated release management module and the per-Client Training Wiki (https://docs.projectview.wiki/[client]), accessible to all Authorised Users, as defined in Section 6.7.
Minimum Licence Commitment	The minimum number of Universal/Concurrent User Licences (not fewer than twenty (20)) that the Customer commits to maintain for the duration of the Binding Period as specified in the Commercial Contract and Enterprise License Agreement. Removals of User Licences via the Flexible Subscription Model shall not reduce the active licence count below this threshold. See Chapter 11, §11.5.4.
Module Activation Amendment	A formal amendment to the Commercial Contract executed by the Parties to activate additional ProjectVIEW ERP modules or Addons/Connectors/Portals mid-term. The amendment specifies the component(s), Activation Date, licensing metric, and pro-rata fees. See Chapter 11, §11.3.4.
Named User	A uniquely identified individual authorised to access specific Addons, Connectors, or Portals under a Named-User licensing model. Named-User licences apply to supplementary platform components where per-individual tracking is required and are non-transferable except via Seat Reassignment. Core Platform access is governed by the Universal/Concurrent User model. See Chapter 11, §11.3.4.
Per-Client Training Wiki	A dedicated, AI-enhanced documentation portal provisioned for each Customer at https://docs.projectview.wiki/[client], containing personalised training materials, recorded session libraries with AI-generated transcripts, role-specific manuals, training plans, and curated FAQ content unique to the Customer's configuration and terminology, as defined in Section 6.7.1.
Commercial Contract	The document executed by the Parties specifying the Platform modules, number of Universal/Concurrent Users, applicable Volume Band, Binding Period, Billing Period, Addon/Connector/Portal entitlements, Named-User allocations (where applicable), currency, Minimum Licence Commitment, and any Customer-specific configurations. The Commercial Contract incorporates the Enterprise License Agreement and takes precedence over all other provisions per §1.3. See Chapter 11, §11.1.
NSG (Network Security Group)	An Azure-native stateful firewall applied to each virtual machine and subnet within the Customer's sovereign environment, enforcing inbound and outbound traffic rules with a default deny-all policy, as defined in Section 8.5.1.
Omnichannel Support Model	The Provider's unified support delivery approach integrating the Embedded Ticketing System, WhatsApp Business Channel, telephone, and email into a single traceable support workflow, as detailed in Section 4.2.
Personal Data	Any information relating to an identified or identifiable natural person, as defined in Article 4(1) of the GDPR and Article 1 of the UAE PDPL.
PDCA (Plan-Do-Check-Act)	The continuous-improvement methodology prescribed by ISO 22301:2019, applied by the Provider to its BCDR programme: Plan (BIA review and recovery-objective calibration), Do (backup and DR execution), Check (drill results and monitoring), Act (corrective actions and architecture improvements), as defined in Section 9.12.

PIMS (Privacy Information Management System)	The extension to the Provider's Information Security Management System (ISMS) that establishes privacy-specific controls, procedures, and documentation in accordance with ISO/IEC 27701:2019, governing the processing of Personal Data by the Provider as Data Processor.
PIR (Post-Incident Report)	A formal report produced by the Provider within five (5) Business Days of resolving a DR-1 or DR-2 disaster-recovery event, containing root-cause analysis, timeline of actions, corrective measures, and BCDR plan updates, delivered to the Customer, as defined in Section 9.7.2.
Platform	The DANAOS ProjectVIEW ERP software application. When delivered as a Software-as-a-Service (SaaS) solution hosted on the DANAOS Cloud (Microsoft Azure), the terms of this Framework apply in full. The Platform includes all modules, updates, and enhancements provided under this Framework.
Provider	DANAOS Projects Software Solutions LLC, a company registered in the United Arab Emirates, with an EU entity registered in Greece, and its affiliated companies.
Provider Service Desk (PSD)	The primary point of contact operated by the Provider for recording and managing all technical support-related tickets via the Omnichannel Support Model (Embedded Ticketing System, WhatsApp Business, telephone, and email), accessible 24 hours per day, 7 days per week, 365 days per year.
Process Optimisation Advisory	A proactive service whereby the Provider analyses AI-agent test-execution data to identify workflow inefficiencies, configuration anomalies, and improvement opportunities within the Customer's ProjectVIEW deployment, delivering recommendations during Quarterly Service Reviews, as defined in Section 5.9.
RPO	Recovery Point Objective — the maximum acceptable period of data loss measured in time. The Platform target RPO is fifteen (15) minutes.
RBAC (Role-Based Access Control)	The authorisation model implemented by the Platform's Users & Roles Management module (STY), enforcing granular permissions at the module, function, field, and record level based on assigned roles, as defined in Section 8.4.2.
RA-GRS (Read-Access Geo-Redundant Storage)	An Azure Storage replication option that extends GRS by providing read-only access to Customer Data in the secondary region during a primary-region outage, enabling immediate data retrieval prior to full failover completion, as defined in Section 9.6.
RTO	Recovery Time Objective — the maximum acceptable duration for restoring the Platform following a significant disruption. The Platform target RTO is four (4) hours.
Record of Processing Activities (RoPA)	The documented record of all Personal Data processing activities maintained by the Provider as Data Processor in accordance with GDPR Article 30 and UAE PDPL, specifying the categories of processing, purposes, data subjects, recipients, transfer mechanisms, and retention periods, as described in Section 7.11.
Release / Update	An incremental software delivery within the current major version (e.g., v11.01, v11.02… v11.xx) addressing change requests, bug fixes, and minor enhancements specific to the Customer's implementation. Delivered via Agile sprints as defined in Section 4.7.1.
Renewal Term	Each successive Billing Period following the expiry of the Binding Period during which the subscription automatically renews under the Evergreen

	Contract mechanism, unless either Party provides written non-renewal notice at least ninety (90) calendar days before the expiry of the then-current Billing Period. See Chapter 11, §11.12.2.
SAST (Static Application Security Testing)	Automated source-code analysis run on every code commit to detect security vulnerabilities before deployment, with Critical/High findings blocking the build, as defined in Section 8.9.
SCA (Software Composition Analysis)	Automated scanning of third-party libraries and dependencies for known vulnerabilities (CVEs) and licence compliance, integrated into the Provider's CI/CD pipeline, as defined in Section 8.9.
SCCs (Standard Contractual Clauses)	The European Union Standard Contractual Clauses adopted under Commission Implementing Decision (EU) 2021/914 for the transfer of Personal Data to third countries not covered by an adequacy decision under GDPR Article 45, as referenced in Section 7.14.
Seat Reassignment	The transfer of a Named-User licence (for Addons, Connectors, or Portals) from a departing individual to a replacement individual who permanently assumes the departing user's role. Seat Reassignment does not incur additional licence fees provided the total active Named-User count does not exceed the licensed count. Not applicable to Universal/Concurrent User Licences, which are floating. See Chapter 11, §11.3.4.
Scheduled Downtime	Any planned period of unavailability of the Platform for maintenance purposes, communicated to the Customer in advance in accordance with Section 3.
Service Request	A formal request from the Customer for something to be provided, changed, or actioned that is not an Incident — for example, new user creation, access permission changes, or report configuration.
Simulation Scenario	A parameterised, end-to-end test specification that defines a complete business-process transaction path (e.g., project initiation through to invoicing) executed by AI agents against the Customer's Dev/Sandbox environment to validate data flows, business rules, and integration integrity, as defined in Section 5.5.2.
SLA Non-Compliance Penalty	A financial penalty payable by the Provider to the Customer, calculated as a percentage of the total ARR in accordance with Section 3.8, where the Provider fails to meet the applicable Service Level or GOS targets.
Service Level	The performance metrics and targets set out in Section 3 and Appendix A against which the Provider's performance shall be measured.
SLO	Service Level Objective — the target availability for the Platform, being ninety-nine point nine nine percent (99.9%) uptime per calendar month, excluding Scheduled Downtime.
Source Code Escrow	The arrangement maintained by the Provider with an independent Escrow Agent for the custody of the Platform's complete source code, build scripts, database schemas, dependency manifests, and deployment documentation. The escrow deposit is updated quarterly and upon each major version release, and is subject to annual verification. Release conditions and Customer rights are defined in Section 9.14.
Sprint	A short-cycle Agile development iteration averaging 3 Business Days, during which the Provider delivers a defined set of change requests, bug fixes, or configuration changes to the Customer's Staging Environment, as detailed in Section 4.7.1.

Staging Environment	The non-production environment used post Go-Live for debugging, change requests, software updates, and Universal User Acceptance Testing (UAT) prior to deployment to the Production Environment. The Staging Environment is the post Go-Live continuation of the Development/Sandbox environment provisioned during implementation.
Super User	A Customer-designated employee who has completed the Provider's Train-the-Trainer (T3) certification programme and is authorised to deliver first-line internal training, conduct new-user onboarding, and provide first-level troubleshooting support within the Customer's organisation, as defined in Section 6.5.
Sub-Processor	Any third party engaged by the Provider to process Personal Data on behalf of the Customer, including Microsoft Corporation (as Azure cloud provider).
Subscription Start Date	The date on which the Customer's subscription commences, being the date of Agreement signing as specified in the Commercial Contract. The Subscription Start Date triggers the Binding Period, the first Billing Period, and the Initial Term. See Chapter 11, §11.12.1.
Subscription Term	The aggregate period comprising the Initial Term (Binding Period) and any Renewal Terms under the Evergreen Contract mechanism during which the Customer is entitled to access and use the Platform, as specified in the Commercial Contract and Enterprise License Agreement. See Chapter 11, §11.12.
Subscription Year	Synonymous with Billing Period. Each consecutive twelve (12) month period within the Subscription Term, commencing on the date of Agreement signing or the anniversary thereof. Subscription Years / Billing Periods are the basis for billing cadence, ARR recalculation, price escalation, and licence-compliance auditing. See Chapter 11, §11.5.
Supervisory Authority	An independent public authority established by an EU Member State pursuant to GDPR Article 51, or the UAE Data Office under Federal Decree-Law No. 44 of 2021, responsible for monitoring the application of data-protection law within its jurisdiction.
SIEM (Security Information and Event Management)	The cloud-native security-monitoring platform (Microsoft Sentinel) that aggregates and correlates logs from all infrastructure, application, and database layers to detect threats and anomalous behaviour in real time, as defined in Section 8.8.1.
TDE	Transparent Data Encryption — the encryption technology applied to all data at rest within the Platform's database layer using AES-256 encryption.
SQT (Software Quality & Testing)	The Provider's AI-augmented software quality and testing framework encompassing automated data-flow simulation, user-interaction simulation, data-integrity validation, regression testing, and process-optimisation advisory services, as defined in Chapter 5.
Test Evidence Repository	The centralised, immutable store maintained by the Provider for each Customer containing test plans, AI-agent execution logs, data-integrity reports, process-optimisation reports, UAT evidence packs, and regression-suite history, as defined in Section 5.10.1.
TKT (Training & Knowledge Transfer)	The Provider's continuous enablement framework encompassing instructor-led training, self-paced digital learning, in-application AI guidance, train-the-trainer certification, and knowledge-base maintenance, as defined in Chapter 6.

TNA (Training Needs Assessment)	A structured assessment conducted by the Provider in collaboration with the Customer to identify activated modules, organisational roles, proficiency gaps, and training requirements prior to the design of a Training Plan, as defined in Section 6.4.1.
TNRA (Training Needs Re-Assessment)	A structured re-evaluation of the Customer's training requirements conducted within sixty (60) days of an EOL Announcement, assessing the impact of successor-version changes on existing competencies, roles, and workflows to produce a Transition Training Plan, as defined in Section 10.7.
Training Coordinator	The Customer-designated single point of contact responsible for all training logistics, scheduling, attendee nomination, feedback collection, and internal distribution of Provider-supplied training materials, as defined in Section 6.9.
Transition Training Plan	A customised training programme developed following the TNRA to re-certify the Customer's users, Champions, and Super Users on the successor version. Includes "What's New" briefings, hands-on workshops, Champion re-certification, API/integration workshops, UAT guidance, Go-Live readiness checks, and post-migration clinics, as defined in Section 10.7.
True-Up Notice	A written notice issued by the Provider following a licence-compliance audit, specifying any excess usage of Universal/Concurrent Users, Named Users (for Addons/Portals), or modules beyond the licensed entitlements and the applicable fees for regularisation. See Chapter 11, §11.11.3.
UAT (Universal User Acceptance Testing)	The formal testing process in which the Customer validates that all software changes, patches, updates, and new features function correctly in the Staging Environment before deployment to Production. UAT requires written Customer sign-off prior to production release.
Upgrade (Major Version)	A product-wide new major version of the Platform (e.g., v11 → v12) encompassing significant functional enhancements, UI/UX redesigns, new APIs/SDKs, and major COTS version upgrades. Released approximately annually. Governed by the End-of-Life policy in Chapter 10.
User Licence Amendment	A formal amendment to the Commercial Contract executed by the Parties to add or remove Universal/Concurrent User Licences mid-term under the Flexible Subscription Model. Additions are invoiced pro-rata from the Activation Date, with the ARR recalculated based on the new Volume Band. Removals take effect at the next Billing Period renewal and are subject to the Minimum Licence Commitment. See Chapter 11, §11.3.6.
UAE Data Office	The national data privacy regulator of the United Arab Emirates, established under Federal Decree-Law No. 44 of 2021, responsible for regulating the application of the UAE PDPL.
UAE PDPL	Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data, the first comprehensive federal data privacy law in the United Arab Emirates, effective 2 January 2022.
Universal User	A floating licence entitlement under the Universal/Concurrent User per Device licensing model that permits any authorised individual to access the Platform, provided the total number of simultaneously active sessions (Concurrent Users) does not exceed the licensed count specified in the Commercial Contract. Universal User Licences are not tied to specific named individuals. See Chapter 11, §11.3.2.

Volume Band	The tiered pricing bracket applicable to the Customer's Annual Subscription Fee, determined by the total number of licensed Universal/Concurrent Users. Five Volume Bands are defined: Band 1 (Minimum–20 Users), Band 2 (21–30), Band 3 (31–50), Band 4 (51–100), and Band 5 (100+). Higher Volume Bands attract progressively reduced per-user rates. See Chapter 11, §11.4.1.
WAF (Web Application Firewall)	Azure Web Application Firewall deployed in front of the Platform's application tier to protect against OWASP Top 10 web-application attacks including SQL injection, cross-site scripting, and request smuggling, as defined in Section 8.5.1.
Warranty Period (Lifetime Warranty)	The entire duration of the Customer's active Subscription Term and any renewal thereof, during which the Provider warrants that the Platform shall perform materially in accordance with this Framework, remain free from material defects, receive continuous security patching, and maintain performance at or above the contracted SLO and recovery objectives. The warranty is co-extensive with the Subscription and does not expire, reduce in scope, or require separate renewal. Defined in Section 9.13.
WhatsApp Business Channel	A dedicated WhatsApp Business group established for each Customer, connecting the Customer's key users with the Provider's assigned consultants for expedient informal communication. Governed by the data protection and formalisation rules set out in Section 4.2.3.
ZRS (Zone-Redundant Storage)	An Azure Storage replication option that maintains three copies of Customer Data across two to three availability zones within a single Azure region, providing 12-nines durability and protection against single availability-zone failure, as defined in Section 9.6.

1.2 Interpretation

In this Framework, unless the context otherwise requires:

(a) References to **Sections** and **Appendices** are to sections of, and appendices to, this Framework.

(b) Words importing the singular include the plural and vice versa, and words importing any gender include all genders.

(c) References to any statute, regulation, or legislative provision include any modification, re-enactment, or extension thereof, including but not limited to the **GDPR**, the **UAE PDPL**, , and any successor legislation or implementing regulations (including any Executive Regulations issued by the UAE Data Office).

(d) The headings in this Framework are for convenience only and shall not affect its interpretation.

(e) The terms *"include"* and *"including"* shall be construed without limitation.

(f) Where any obligation in this Framework requires compliance with a standard (including ISO 27001, ISO 9001, or ISO 20000-1), the reference shall be to the version current at the date of this Framework or, where the Provider has transitioned to a later version, that later version.

(g) References to a Party include that Party's successors and permitted assigns.

(h) Any obligation on a Party not to do something includes an obligation not to allow, cause, or permit that thing to be done.

1.3 Order of Precedence

In the event of any conflict or inconsistency between the provisions of this Framework, the following order of precedence shall apply (in descending order):

(i) **The Commercial Contract** (including any Customer-specific terms agreed therein);

(j) **Part A** (Commercial & Legal Framework) of this Framework;

(k) **Parts B through E** (Technical & Operational Provisions) of this Framework;

(l) **The Appendices** to this Framework.

1.4 Regulatory References

This Framework references the following regulatory frameworks and standards. Where applicable, external links are provided for verification and further reading:

- **GDPR** — Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data

https://eur-lex.europa.eu/eli/reg/2016/679/oj

- **UAE PDPL** — Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (United Arab Emirates). Effective 2 January 2022. Establishes comprehensive data protection obligations for entities processing personal data of natural persons in or from the UAE, including requirements for DPO appointment, data breach notification, Data Protection Impact Assessments (DPIAs), cross-border transfer safeguards, and a Record of Processing Activities (ROPA). Regulated by the UAE Data Office under Federal Decree-Law No. 44 of 2021.

UAE Government Data Protection Laws: https://u.ae/en/about-the-uae/digital-uae/data/data-protection-laws

Full text: https://uaelegislation.gov.ae/en/legislations/1972/download

National Privacy Commission:

- **ISO/IEC 27001:2022** — Information Security Management Systems
- **ISO 9001:2015** — Quality Management Systems
- **ISO/IEC 20000-1:2018** — IT Service Management

DANAOS ISO Certifications: https://danaos-projects.com/iso-certifications/

- **Microsoft Azure Compliance** — SOC 1/2/3, ISO 27001/27017/27018, FedRAMP, PCI DSS, CSA STAR

Microsoft Service Trust Portal: https://servicetrust.microsoft.com/

Azure Trust Center: https://azure.microsoft.com/en-us/explore/trusted-cloud

***Note:** The Provider maintains compliance with all applicable data protection regulations in each jurisdiction of operation. Given the Provider's principal place of business in the United Arab Emirates, the UAE PDPL is of primary relevance alongside the GDPR. The Provider monitors the issuance of Executive Regulations by the UAE Data Office and will update its data protection practices accordingly within the compliance transition period prescribed by the UAE PDPL.*

1.5 Process Register

The following table summarises the governance processes established in this Chapter, including responsible roles, expected outcomes, and cross-references to related processes in other Chapters.

Role Legend: P = Provider | C = Customer | SC = Steering Committee | DPO = Data Protection Officer | SDM = Service Delivery Manager

1.5.1 Process Registry

Ref	Process	Trigger	Handler	Approver	Expected Outcome	Cross-Ref
P-1.01	Agreement Amendment	Either Party requests modification to terms	Legal Counsel (P/C)	Steering Committee	Executed written amendment to Agreement	§ 7, § 1.3
P-1.02	Precedence Dispute Resolution	Conflict identified between Agreement documents	SDM / Customer IT Liaison	Steering Committee	Binding interpretation per § 1.3 hierarchy	§ 1.3, § 3.11
P-1.03	Regulatory Compliance Update	New or amended Data Protection Law	DPO / Legal Counsel	Steering Committee	Updated DPA, privacy notices, and processing records	§ 1.4, § 17

1.5.2 RACI Matrix

Process (Ref)	Provider	Customer	Steering Committee	DPO
P-1.01 Agreement Amendment	C	C	A	I
P-1.02 Precedence Dispute	R	C	A	—
P-1.03 Regulatory Update	R	I	A	R

R = Responsible (executes) | **A** = Accountable (sign-off) | **C** = Consulted | **I** = Informed | **—** = Not Involved

1.5.3 Process Flow — Agreement Governance Lifecycle

Stage	Activity	Role	Output
① **Initiation**	Amendment or dispute request raised	Either Party	Written request submitted

② **Assessment**	Legal/regulatory impact analysis	Provider + DPO	Impact assessment report
③ **Review**	Steering Committee review and decision	Steering Committee	Approval / rejection / deferral
④ **Execution**	Signed amendment or updated DPA	Both Parties	Executed document → Agreement updated

2 Service Description & Scope

2.1 Overview of the Platform

The Provider delivers **ProjectVIEW ERP** as a fully managed Software-as-a-Service (SaaS) solution. ProjectVIEW ERP is a cloud-based, integrated, and highly adaptable **Construction-grade ERP** purpose-built for **Capital-Intensive Project Industries**. Its core strength is precise **Cost Control, Construction Management**, and end-to-end visibility across complex engineering projects.

ProjectVIEW ERP is composed of a unified constellation of **10+1 enterprise modules** that digitally transform **Commercial, Operational, Production, and Financial** processes. By enforcing structured data, standardised workflows, and seamless field-to-office integration, it becomes the **central hub for Project Performance Management** and a foundational enabler of AI-ready operations.

ProjectVIEW ERP serves as **The Operating System for the BUILD World** — powering organisations that deliver the world's most demanding capital projects.

2.1.1 Dedicated Private Sovereign Environment

Each Customer's instance of ProjectVIEW ERP is hosted in a **dedicated, private, sovereign cloud environment** on Microsoft Azure. This means:

- **Complete tenant isolation:** Each Customer operates within its own dedicated Azure Virtual Machines, database instances, and storage accounts. There is no shared infrastructure or multi-tenant data commingling.
- **Data sovereignty:** Customer Data resides in the Azure region specified in the Commercial Contract, ensuring compliance with local data residency requirements and applicable Data Protection Laws.
- **Customisation freedom:** The dedicated environment enables Customer-specific configurations, customisations, and update schedules without impacting other Customer instances.
- **Security boundary:** Each environment is protected by its own Azure Virtual Network (VNet), Network Security Groups (NSGs), and firewall rules, creating a complete security perimeter.

Microsoft Azure Regions: https://azure.microsoft.com/en-us/explore/global-infrastructure/geographies/

2.2 Industries Served

ProjectVIEW ERP is not a generic ERP platform. It is a **full-spectrum, Tier-1 enterprise system purpose-built for the Build World**, engineered to handle the complexity, scale, and cost intensity of real construction and project-driven operations. Designed for **capital-intensive environments** where BoQ, WBS, time, and cost must work in unison, ProjectVIEW ERP powers the full breadth of Build World industries:

#	Industry	Description
1	**Construction**	Civil, infrastructure, building, and heavy construction — from foundations to handover. Full EPC, EPCM, and EPCi project lifecycle support.
2	**Marine Engineering | Offshore Construction**	Offshore platforms, subsea installations, marine infrastructure, and coastal engineering projects with complex logistics and safety requirements.

3	**Mining & Quarrying**	Open-pit and underground mining operations, quarrying, mineral processing, and associated infrastructure development.
4	**Shipbuilding & Repairs (SBR)**	New-build vessel construction, ship repair and conversion, dry-docking operations, and marine equipment fabrication.
5	**Project-based Manufacturing**	Structural steel fabrication, modular construction, pre-fabrication facilities, and engineered-to-order manufacturing.

Industries We Serve: https://danaos-projects.com/industries-we-serve/

2.3 Platform Modules & Functional Scope

Subject to the Commercial Contract, ProjectVIEW ERP comprises **10+1 enterprise modules** organised as follows:

#	Module	Functional Scope
01	**Budget Estimation - Bidding**	Bill of Quantities (BoQ) import from any .xls in tree-structured format, BIM model validation via .ifc, quantity take-off (QTO), measured vs. lump sum comparison, BoQ-WBS synchronisation, inflation/overhead/risk/profit modelling, what-if/what-will bid simulations, and rough-cut capacity planning.
02	**Cost Control**	Real-time cost monitoring against budget, earned value management (EVM), cost-to-complete and estimate-at-completion forecasting, variance analysis, cashflow projections, and multi-dimensional cost breakdown structures (CBS).
03	**Subcontractors Management**	Subcontract creation and lifecycle management, progress measurement and certification, variation orders, claims management, retention tracking, and subcontractor performance evaluation.
04	**Procurement**	Purchase requisitions, purchase orders, RFQs, comparative bid analysis, supplier qualification and management, procurement-to-pay workflows, and commitment tracking.
05	**Materials & Production Management**	Inventory and warehouse operations, material requisitions, goods receipt, stock transfers, min/max levels, barcode/RFID integration, production tracking, and material reconciliation.
06	**Machinery Management**	Fleet and equipment management, internal/external costing and allocation, maintenance scheduling (preventive and corrective), utilisation tracking, rental rate management, and equipment depreciation.
07	**HRMS - Payroll**	Employee records and lifecycle management, time and attendance, leave management, payroll processing (including WPS compliance for UAE), workforce planning, and labour cost allocation to projects.
08	**Accounting - Finance Management**	General ledger, chart of accounts, multi-currency management, intercompany transactions, fixed assets, tax management (including VAT), financial consolidation, and statutory reporting.
09	**Suppliers Account Payables**	Supplier invoice processing, payment scheduling, ageing analysis, retention management, debit/credit notes, and automated payment reconciliation.
10	**Customers Account Receivables**	Customer invoicing, interim payment certificates (IPC), revenue recognition, ageing analysis, retention tracking, and collection management.

00	**ProjectVIEW ERP Core**	The foundational platform layer encompassing: user and role management (STY), workflow engine, approval hierarchies, dashboard and KPI framework, Power BI integration, document management, audit trail, notification engine, API gateway, and system administration.

Note: *The specific modules activated for the Customer are detailed in the Commercial Contract. Additional modules may be added during the Subscription Term subject to mutual written agreement and adjustment of Fees.*

Explore ProjectVIEW ERP Modules: https://danaos-projects.com/projectview-erp/explore-projectview-erp/

2.4 SaaS Delivery Model

Applicability: This SaaS Delivery Model and the obligations described in this Framework apply exclusively when ProjectVIEW ERP is hosted on the DANAOS Cloud (Microsoft Azure infrastructure managed by the Provider). Customers operating ProjectVIEW under an on-premises or third-party-hosted deployment model should refer to the applicable licence and support agreement.

ProjectVIEW ERP is delivered exclusively as a **fully managed SaaS solution**. The Provider assumes end-to-end responsibility for all layers of the technology stack — from infrastructure provisioning and security management through application delivery and ongoing support. The Customer consumes the Platform as a service and is not required to manage any underlying infrastructure, middleware, or platform components.

The SaaS delivery model incorporates the following managed capabilities:

Capability	Description
Security Management	Proactive security monitoring, vulnerability scanning, patch management, intrusion detection, and incident response. Includes Cloudflare WAF with DDoS protection and OWASP Top 10:2025 ruleset coverage.
Backup Management	Automated backup schedules: database backups every 12 hours with transaction log backups every 15–60 minutes, daily incremental file backups, weekly and monthly full backups. All backups encrypted at rest.
Resource Management	Performance monitoring, capacity planning, proactive scaling recommendations, and resource optimisation to ensure consistent application performance.
Guaranteed Performance	SLO of 99.9% uptime, RPO of 15 minutes, RTO of 4 hours. Detailed performance targets and Service Credits defined in Section 3.
Update Management	Regular platform updates, patches, hot-fixes, and feature releases delivered through a controlled CI/CD pipeline with develop-test-live deployment methodology.
Monitoring & Observability	Azure Monitor, Application Insights, and Microsoft Defender for Cloud for continuous platform observability, alerting, and proactive issue resolution.

2.5 Platform Architecture

The Platform operates on a **three-tier architecture** within the dedicated private sovereign Azure environment:

Tier	Technology	Description
Presentation	HTML5 / JavaScript	Browser-based thin client — the DANAOS Web Enterprise Suite. No client-side installations or plugins required. Responsive design supporting desktop, tablet, and mobile access.
Application	.NET 10 C# MVC / IIS 10.0	Business logic layer with RESTful API gateway. JWT token-based authentication with Microsoft Entra ID SSO and MFA. Hosted on dedicated Azure Virtual Machines with load balancing.
Data	SQL Server 2025	Enterprise database with Transparent Data Encryption (TDE / AES-256), automated point-in-time recovery, and configurable geo-replication.

Technology References:

Microsoft .NET 10 (LTS): https://dotnet.microsoft.com/en-us/download/dotnet/10.0

Microsoft SQL Server 2025: https://learn.microsoft.com/en-us/sql/sql-server/what-s-new-in-sql-server-2025

Microsoft Entra ID (Identity & Access): https://www.microsoft.com/en-us/security/business/identity-access/microsoft-entra-id

Internet Information Services (IIS) 10.0: https://www.iis.net/

Cloudflare Web Application Firewall: https://developers.cloudflare.com/waf/

OWASP Top 10:2025: https://owasp.org/Top10/2025/

Microsoft Defender for Cloud: https://azure.microsoft.com/en-us/products/defender-for-cloud

Azure Monitor & Application Insights: https://azure.microsoft.com/en-us/products/monitor

Microsoft Power BI: https://powerbi.microsoft.com/

2.5.1 Deployment Methodology & Environment Lifecycle

The Provider maintains a strict **develop-test-live** approach for all software deployments, underpinned by a two-environment architecture:

(a) **During Implementation:** The Provider provisions two (2) environments — a **Development / Sandbox** environment for configuration, customisation, and Universal User Acceptance Testing (UAT), and a **Production** environment for live operations.

(b) **Post Go-Live Transition:** Upon Go-Live, the Development / Sandbox environment transitions to become the permanent **Staging Environment**, used for debugging, change requests, software updates, and UAT prior to production deployment.

(c) **UAT Gate:** No changes are deployed to Production without prior validation and **written Customer UAT sign-off** in the Staging Environment, except in cases of Emergency Maintenance (see Section 3.2.3).

Where appropriate, the Provider practices Continuous Integration / Continuous Delivery (CI/CD) to minimise deployment risk and accelerate release cycles. The full environment lifecycle is detailed in Section 3.3.

2.6 Service Scope

The Services provided under this Framework include, but are not limited to:

#	Service Area	Description
1	Requirements Engineering	Elicitation of Customer requirements and development/customisation to specifications. Additional customisation costs shall be agreed upon in writing before commencement.
2	Project Management	Turn-key project management of software implementation utilising agile methodology.
3	Documentation	Provision of required software documents including: high-level and low-level requirement/design documents, User Requirements Specification (URS), System Requirements Specification (SRS), flow charts, test plans, system documentation, end-user guides, installation guides, and Defect Track Logs.
4	Database Documentation	Provision of database documents including: Data Flow Diagrams (DFD), Entity-Relationship Diagrams (ERD), and Data Dictionaries.
5	Patches & Hot-Fixes	Delivery of software patches and hot-fixes at no additional cost to the Customer.
6	Continual Improvement	Continuous improvement approach to software development, incorporating Customer feedback and industry best practices.
7	Fault Resolution	Debugging and resolution of software faults resulting from normal operation.
8	Support Response	Response to software support calls as per the SLA Matrix defined in Section 3 and Appendix A.
9	Embedded Ticketing System	Native in-application ITSM ticketing system within ProjectVIEW ERP for incident logging, ticket lifecycle tracking, SLA measurement, knowledge base access, and self-service support.
10	24/7 Omnichannel Service Desk	Access to the Provider Service Desk (PSD) 24×7×365 via the Embedded Ticketing System, WhatsApp Business Channel, telephone, and email for ticket logging and management.
11	WhatsApp Business Support	Dedicated WhatsApp Business group connecting the Customer’s key users with the Provider’s assigned consultants for expedient informal communication and quick enquiries.
12	Training	Provision of required end-user and administrative training, including onboarding for new Authorised Users.
13	Preventive Maintenance	Monthly preventive maintenance on all Platform modules as agreed with the Customer.
14	Reporting	Submission of quarterly service reports in the Customer’s agreed format, including SLA performance metrics.

2.7 Exclusions

Unless explicitly agreed in the Commercial Contract or a separate Statement of Work, the following are excluded from the scope of this Framework:

(a) Hardware procurement, installation, or maintenance at Customer premises

(b) Third-party software licensing (other than the Platform and its bundled components)

(c) Network infrastructure, internet connectivity, or local area network management at Customer sites

(d) Custom integrations with third-party systems not specified in the Commercial Contract

(e) Data migration from legacy systems (available as a separately scoped engagement)

(f) On-site consulting, training, or support beyond the scope specified in the Commercial Contract

(g) Recovery from incidents caused by Customer misuse, unauthorised modifications, or third-party software interference

(h) Compliance activities specific to the Customer's own regulatory obligations (the Provider's compliance obligations are set out in Part C)

2.8 Customer Obligations

To enable the Provider to deliver the Services effectively, the Customer shall:

(a) Designate a primary point of contact and an escalation contact for day-to-day service management

(b) Provide timely access to relevant business information, documentation, and subject-matter experts required for requirements engineering and implementation

(c) Ensure that Authorised Users comply with the Provider's Acceptable Use Policy and all applicable security policies

(d) Maintain adequate internet connectivity at Customer premises to access the Platform

(e) Report Incidents and service requests through the **Provider Service Desk (PSD)** in accordance with the procedures set out in Section 4

(f) Participate in user acceptance testing (UAT) within agreed timeframes and provide written sign-off on deliverables

(g) Ensure that all Customer Data uploaded to the Platform complies with applicable Data Protection Laws and does not contain prohibited content

(h) Maintain current and accurate Authorised User records and promptly revoke access for departing personnel

Failure by the Customer to meet the obligations set out in this Section 2.8 may affect the Provider's ability to meet Service Levels, and such impact shall be excluded from SLA calculations as set out in Section 3.

2.9 Process Register

The following table summarises the service delivery processes established in this Chapter, including responsible roles, expected outcomes, and cross-references to related processes in other Chapters.

Role Legend: P = Provider | C = Customer | PM = Provider Project Manager | SDM = Service Delivery Manager | SC = Steering Committee

2.9.1 Process Registry

Ref	Process	Trigger	Handler	Approver	Expected Outcome	Cross-Ref
P-2.01	Environment Provisioning	Commercial Contract executed	Provider (Infra)	SDM	Dev/Sandbox + Production	§ 3.3

					environments operational	
P-2.02	Module Activation	Commercial Contract or amendment	Provider (Dev)	Customer IT Liaison	Licensed modules accessible in Production	§ 2.3, § 6
P-2.03	Customer Onboarding	Go-Live readiness achieved	PM (Provider)	Customer IT Liaison	All users provisioned, trained, and operational	§ 5, § 3.9
P-2.04	UAT Execution & Sign-Off	Changes deployed to Staging	Customer	Customer IT Liaison	Written UAT sign-off within 5 BD	§ 3.3.1, § 4.7
P-2.05	Scope Change Request	Customer requests additional modules/services	PM (Provider)	Steering Committee	Amended Commercial Contract with adjusted fees	§ 6, § 4.8
P-2.06	Post Go-Live Transition	Go-Live completed	Provider (Infra)	SDM	Dev/Sandbox → Staging Environment	§ 3.3.1, § 4.7

2.9.2 RACI Matrix

Process (Ref)	Provider	Customer	PM	SDM	SC
P-2.01 Env Provisioning	R	I	C	A	—
P-2.02 Module Activation	R	A	R	I	—
P-2.03 Customer Onboarding	R	C	A	I	—
P-2.04 UAT & Sign-Off	C	R/A	C	I	—
P-2.05 Scope Change	R	C	R	I	A
P-2.06 Post Go-Live	R	I	R	A	I

R = Responsible (executes) | **A** = Accountable (sign-off) | **C** = Consulted | **I** = Informed | **—** = Not Involved

2.9.3 Process Flow — Service Delivery Lifecycle

Stage	Activity	Role	Output
① **Contract**	Commercial Contract executed, scope and modules agreed	Provider + Customer	Signed Commercial Contract
② **Provisioning**	Azure environments provisioned (Dev/Sandbox + Production)	Provider (Infra)	2 environments operational
③ **Configuration**	Platform configured, customised, data migrated	Provider (Dev) + PM	Configured platform in Staging
④ **UAT**	Customer validates in Staging (min 5 BD)	Customer	Written UAT sign-off
⑤ **Go-Live**	Production deployment, user onboarding, training	Provider + Customer	Operational Production system

⑥ **Transition**	Dev/Sandbox becomes permanent Staging	Provider (Infra)	2-env steady state → § 3.3.1

3 Service Level Agreement

3.1 SLA Overview

This Section defines the **Service Levels** that the Provider commits to achieving in the delivery and support of the Platform. The Provider shall use commercially reasonable endeavours to meet or exceed the Service Levels set out in this Section when providing the Services. Service Levels cover **platform availability, incident response, resolution targets, backup and recovery objectives**, and associated **Service Credits** in the event of non-compliance.

The SLA applies to the **production environment** of the Platform only. Non-production environments (development, sandbox/test) are excluded from SLA measurement unless otherwise specified in the Commercial Contract.

3.1 Platform Availability

3.1.1 Service Level Objective (SLO)

The Provider commits to a Service Level Objective of **99.9% monthly uptime** for the production environment of the Platform, measured as a percentage of total minutes in the applicable calendar month.

Metric	Target	Measurement Period
Service Level Objective (SLO)	**99.9%**	Calendar month
Maximum Permitted Downtime	**4.32 minutes / month**	Calculated: (1 – 0.9999) × 43,200 mins

3.1.2 Availability Calculation

Monthly Availability is calculated using the following formula:

Availability % = ((Total Minutes – Downtime Minutes) / Total Minutes) × 100

Where:

- **Total Minutes** = the total number of minutes in the applicable calendar month
- **Downtime Minutes** = the total minutes during which the production environment is unavailable, excluding Scheduled Maintenance and Excluded Events

3.1.3 Scheduled Maintenance

The Provider shall perform scheduled maintenance during pre-agreed **Maintenance Windows**. Scheduled Maintenance is excluded from Availability calculations provided that:

(a) The Provider gives the Customer a minimum of **5 Business Days' advance written notice** of scheduled maintenance;

(b) Maintenance is scheduled during **Off-Peak Hours** (between 22:00 and 06:00 local time at the Customer's primary site), unless otherwise agreed;

(c) Total Scheduled Maintenance does not exceed 4 hours per calendar month;

(d) The Provider uses commercially reasonable efforts to minimise the duration and impact of each maintenance window.

Emergency Maintenance: In the event of a critical security vulnerability or imminent system failure, the Provider may perform emergency maintenance with less than 5 Business Days' notice. The Provider shall notify the Customer as soon as reasonably practicable and provide a post-maintenance report within 2 Business Days.

3.2 Environment Lifecycle

During implementation, the Provider provisions **two (2) distinct environments** for the Customer:

Phase	Environment	Purpose
Implementation	**Development / Sandbox**	Configuration, customisation, data migration, integration testing, and Universal User Acceptance Testing (UAT). The Customer and Provider jointly validate all functional requirements prior to Go-Live.
Implementation	**Production**	The live operational environment for all Authorised Users. Subject to the full SLA metrics defined in this Section 3.

3.2.1 Post Go-Live Environment Transition

Upon **Go-Live**, the environment structure transitions as follows:

Environment	Post Go-Live Role	Purpose
Development / Sandbox	**Staging Environment**	Becomes the permanent staging environment used for: debugging and fault reproduction, change requests and enhancement development, software updates and patch testing, and Universal User Acceptance Testing (UAT) prior to production deployment.
Production	**Production Environment**	Continues as the live operational environment. No changes are deployed to production without prior validation and UAT sign-off in the Staging Environment.

Universal User Acceptance Testing (UAT): All software changes, patches, updates, and new feature releases must pass through UAT in the Staging Environment before deployment to Production. The Customer shall be given a minimum of **5 Business Days** to complete UAT, and deployment to Production requires **written Customer sign-off**. The Provider shall not deploy any change to the

Production Environment without confirmed UAT approval, except in the case of Emergency Maintenance as defined in Section 3.2.3.

The Provider shall maintain environment parity between Staging and Production to ensure that UAT results are representative of production behaviour. Both environments shall run identical software versions, configurations, and security policies at all times, differing only in data content.

3.3 Recovery Objectives

The Provider commits to the following recovery objectives for the production environment, aligned with the Platform's **Business Continuity and Disaster Recovery (BC/DR)** architecture:

Metric	Target	Definition
Recovery Point Objective (RPO)	**15 minutes**	The maximum acceptable amount of data loss measured in time. Transaction log backups run every 15 minutes, ensuring no more than 15 minutes of data may be lost in a disaster scenario.
Recovery Time Objective (RTO)	**4 hours**	The maximum acceptable duration of service interruption. The Provider shall restore full platform functionality within 4 hours of declaring a disaster event.

These recovery objectives are supported by the following **backup architecture**:

Backup Type	Frequency	Retention	Encryption
Transaction log backups	Every 15 minutes	7 days	AES-256 at rest
Database full backups	Every 12 hours	30 days	AES-256 at rest
Incremental file backups	Daily	30 days	AES-256 at rest
Weekly full backups	Weekly (Sunday)	90 days	AES-256 at rest
Monthly archival backups	Monthly (1st)	12 months	AES-256 at rest

All backups are stored in **geo-redundant Azure storage** within the Customer's designated Azure region, with optional cross-region replication as specified in the Commercial Contract. Backup integrity is verified through automated restoration tests performed **quarterly**.

Azure Backup Overview: https://azure.microsoft.com/en-us/products/backup

3.4 Incident Priority Classification

All Incidents reported to the Provider Service Desk (PSD) shall be classified according to the following priority levels:

Priority	Severity	Definition	Example

P1	**Critical**	Complete system unavailability or critical business function failure affecting all or substantially all Authorised Users. Data integrity at risk.	Production server down, critical database corruption, platform entirely inaccessible, data loss event.
P2	**Urgent**	Significant degradation of a critical business function. System operational but with severely limited functionality. Major feature unavailable.	Key module non-functional (e.g., Cost Control), severe performance degradation, critical integration failure.
P3	**Major**	Non-critical function impaired or degraded performance that does not prevent core business operations. A reasonable workaround exists.	Report generation failure, non-critical module issue, cosmetic defect impacting usability, minor integration fault.
P4	Minor	Cosmetic issue, informational request, or enhancement suggestion with no immediate operational impact.	UI alignment issue, documentation correction, feature request, general inquiry.

Priority classification shall be **mutually agreed** between the Customer and the Provider at the time of ticket logging. If the Parties cannot agree, the Customer's classification shall prevail pending review by the Service Delivery Manager at the next scheduled Service Review meeting.

P1 and P2 Incidents must be reported by **telephone** to the Provider Service Desk to ensure immediate attention. P3 and P4 Incidents may be reported by email, the PSD portal, or telephone.

3.5 SLA Response & Resolution Matrix

The Provider shall respond to and resolve Incidents within the targets set out in the SLA Matrix below:

Priority	Response Time	MTTR Target	Workaround Target	Operation Window	GOS Target
P1 – Critical	**Immediate**	**4 Hours**	Continuous effort until resolved	24 × 7 × 365	**98%**
P2 – Urgent	**Immediate**	**8 Hours**	15 Business Days	24 × 7 × 365	**95%**
P3 – Major	**Within 2 Hours**	**12 Hours**	20 Business Days	24 × 7 × 365	**93%**
P4 – Minor	**Within 4 Hours**	Next Release	Next scheduled release	Business Hours	**90%**

Where:

- **Response Time** = time from Incident acknowledgement by PSD to first diagnostic action by an assigned engineer
- **MTTR (Mean Time to Repair)** = target elapsed time from Incident acknowledgement to full resolution or effective workaround
- **Workaround Target** = maximum elapsed time to provide a temporary resolution that restores core business functionality pending permanent fix

- **GOS (Grade of Service)** = the percentage of Incidents within each priority level that are resolved within the MTTR target during the measurement period

3.6 SLA Exclusions

The following events are excluded from SLA measurement and shall not count as Downtime or impact GOS calculations:

(a) **Scheduled Maintenance**: pre-notified maintenance performed within agreed Maintenance Windows as defined in Section 3.2.3

(b) **Security Events**: any Downtime resulting from security breaches, DDoS attacks, or emergency security patches applied to protect the Platform and Customer Data

(c) **Force Majeure**: events beyond the reasonable control of the Provider as defined in Section 9

(d) **Customer-Caused Delays**: delays arising from the Customer's failure to meet its obligations under Section 2.8, including failure to provide timely information, approval delays, or unauthorised modifications

(e) **Third-Party Failures**: outages in internet connectivity, DNS, or other services not under the Provider's direct control, including Microsoft Azure platform outages that affect the underlying infrastructure

(f) **Approval Lifecycle Delays**: delays caused by Customer approval workflows or sign-off processes that prevent the Provider from proceeding with resolution activities

In the event of an Azure platform outage, the Provider shall provide the Customer with the relevant **Microsoft Root Cause Analysis (RCA)** report within 5 Business Days of its publication by Microsoft.

Azure Service Health: https://azure.microsoft.com/en-us/features/service-health/

Azure Status: https://status.azure.com/

3.7 SLA Non-Compliance Penalties

Where the Provider fails to achieve the SLO or Grade of Service (GOS) targets set out in this Section 3, the Provider shall pay the Customer **financial penalties** calculated as a percentage of the Customer's **total Annual Recurring Revenue (ARR)** (being the annual subscription licensing fees payable under the Commercial Contract), as follows:

Variance from Target	Penalty (% of Total ARR)	Payment Trigger
≥ 2.00%	**20% of ARR**	Payable within 30 days of breach notification
1.00% – 1.99%	**10% of ARR**	Payable within 30 days of breach notification
0.51% – 0.99%	**5% of ARR**	Payable within 30 days of breach notification
≤ 0.50%	0% (within tolerance)	No penalty — within acceptable tolerance

3.7.1 Calculation Methodology

Penalties are calculated as follows:

(e) **ARR Basis:** The penalty is calculated against the **total Annual Recurring Revenue (ARR)** as defined in the Commercial Contract at the time of the breach. ARR includes all subscription licensing fees for all Authorised Users and modules then in effect, including any additional licences added during the Subscription Term.

(f) **Availability-based variance:** The percentage deviation is calculated as a proportion of the SLO target. For example, if the SLO target is 99.9% and 2% of that target is breached, the threshold is (0.02 × 99.99) = 1.9998%, meaning actual Availability below 98.0002% triggers the 20% penalty.

(g) **GOS-based variance:** Similarly calculated as a proportion of the GOS target for each priority level.

(h) **Weighted Average:** Where the Availability-based and GOS-based penalty calculations yield different values, the final penalty shall be the **Weighted Average** with Availability carrying a weight of **70%** and GOS carrying a weight of **30%**.

3.7.2 Penalty Payment Terms

(i) Penalties shall be paid by the Provider to the Customer as a **direct financial payment** (not a credit note) within **30 days** of the Customer's written penalty claim being validated.

(j) The maximum aggregate penalty in any calendar quarter shall not exceed **25% of the quarterly ARR** for the affected Service.

(k) The Customer must submit a penalty claim in writing within **30 days** of the end of the month in which the SLA breach occurred, specifying the relevant Incidents and supporting evidence.

(l) The Provider shall validate or dispute the claim within **10 Business Days** of receipt. Any dispute shall be escalated to the Steering Committee for resolution.

(m) Penalties represent the Customer's sole and exclusive financial remedy for failure to meet Service Levels. This does not limit the Customer's right to terminate the Framework for material breach under Section 7.

(n) Penalties shall not be payable where the SLA failure results from an **Excluded Event** as defined in Section 3.7.

3.8 Additional Licences & New Users

Where the Customer elects to add **new Authorised Users** (additional licences) during the Subscription Term, the following provisions apply:

(o) **Same SLA Coverage:** All Service Levels, performance targets, recovery objectives, and penalty provisions set out in this Section 3 shall apply equally to all additional Authorised Users and licences from the date of activation. There is no reduced or phased SLA for new users.

(p) **ARR Adjustment:** The ARR used for penalty calculations under Section 3.8 shall be recalculated to include the additional licence fees from the date of activation, on a pro-rata basis for the remainder of the applicable measurement period.

(q) **Environment Consistency:** New users shall have access to the same Production and Staging environments. The Provider shall ensure that the Platform scales to accommodate the additional users without degradation of performance or Availability.

(r) **Onboarding SLA:** The Provider shall activate new user accounts within **2 Business Days** of receiving a completed licence addition request from the Customer, including role assignment, access provisioning, and initial training materials.

(s) **Capacity Guarantee:** The Provider warrants that the dedicated private sovereign environment has sufficient headroom, or shall be proactively scaled, to support the additional users without impacting the SLO of 99.9% or any GOS targets.

The procedure for adding new licences, including pricing and Commercial Contract amendment requirements, is set out in Section 6 (Fees, Invoicing & Payment Terms).

3.9 SLA Reporting & Service Reviews

3.9.1 Monthly SLA Report

The Provider shall deliver a monthly SLA performance report to the Customer within 10 Business Days of the end of each calendar month. The report shall include:

(t) Monthly Availability percentage and comparison against SLO target

(u) Total number of Incidents by priority level, with response and resolution times

(v) GOS achievement per priority level

(w) Backup success rates and any failed backup events

(x) Any SLA breaches with root cause analysis and corrective actions

(y) Penalty calculations (if applicable) with ARR basis shown

(z) Trend analysis comparing performance against prior 3 months

3.9.2 Quarterly Service Review

The Parties shall conduct a **Quarterly Service Review** meeting to review SLA performance, discuss service improvement initiatives, and address any outstanding issues. The Provider shall prepare and submit a quarterly service report in the Customer's agreed format at least **5 Business Days** prior to each review meeting. The quarterly report shall include:

(aa) Consolidated SLA performance across the quarter

(bb) Major Incident summaries with root cause analysis

(cc) Service improvement plan updates and progress

(dd) Capacity and performance trend analysis

(ee) Change management summary (patches, updates, releases deployed)

(ff) Forward-looking risk assessment and mitigation plan

3.9.3 Continual Service Improvement

The Provider shall maintain a **Continual Service Improvement (CSI) register** documenting identified improvement opportunities, agreed actions, responsible parties, and target completion dates. The CSI register shall be reviewed at each Quarterly Service Review.

3.10 SLA Governance

The following governance structure applies to SLA management:

Role	Responsibility	Frequency
Service Delivery Manager (Provider)	Primary point of accountability for SLA performance. Owns the monthly SLA report, escalation management, and CSI register.	Ongoing

Account Manager (Provider)	Commercial relationship management. Escalation point for SLA disputes and Service Credit claims.	As required
Customer IT Liaison	Primary Customer contact for day-to-day service management, Incident reporting, and UAT coordination.	Ongoing
Steering Committee	Joint senior management forum for strategic review of the service relationship, major Incident review, and contract-level decisions.	Bi-annual

The SLA targets set out in this Section shall be reviewed **annually** at the Steering Committee meeting and may be amended by mutual written agreement of the Parties.

Azure SLA Summary: https://azure.microsoft.com/en-us/support/legal/sla/summary/

ITIL Service Level Management: https://www.axelos.com/best-practice-solutions/itil

3.11 Process Register

The following table summarises the SLA management processes established in this Chapter, including responsible roles, expected outcomes, and cross-references to related processes in other Chapters.

Role Legend: P = Provider | C = Customer | PSD = Provider Service Desk | SDM = Service Delivery Manager | SC = Steering Committee

3.11.1 Process Registry

Ref	Process	Trigger	Handler	Approver	Expected Outcome	Cross-Ref
P-3.01	Availability Monitoring	Continuous (automated)	Provider (NOC)	SDM	99.9% SLO maintained; alerts on threshold breach	§ 3.2
P-3.02	Incident Classification	Incident reported to PSD	PSD	Customer / SDM	Mutually agreed priority (P1–P4)	§ 3.5, § 4.3
P-3.03	SLA Performance Measurement	Month-end close	SDM	—	Monthly SLA report within 10 BD	§ 3.10.1
P-3.04	SLA Breach Detection	Monthly SLA report reveals breach	SDM	Provider Account Mgr	Penalty calculation initiated	§ 3.8
P-3.05	Penalty Claim & Payment	Customer submits claim within 30 days	Provider Finance	Provider Account Mgr	Financial payment within 30 days of validation	§ 3.8.2
P-3.06	Quarterly Service Review	Quarter-end	SDM + Customer IT Liaison	Steering Committee	Service review completed; CSI register updated	§ 3.10.2, § 4.10

P-3.07	New User Activation	Customer licence addition request	Provider (PSD)	Customer IT Liaison	User active within 2 BD; ARR adjusted pro-rata	§ 3.9, § 6
P-3.08	Scheduled Maintenance	Maintenance window planned	Provider (Infra)	SDM	Maintenance completed; ≤ 4 hrs/month; Customer notified 5 BD prior	§ 3.2.3

3.11.2 RACI Matrix

Process (Ref)	Provider	PSD	Customer	SDM	SC
P-3.01 Availability Monitoring	R	I	I	A	—
P-3.02 Incident Classification	—	R	C	A	—
P-3.03 SLA Measurement	—	—	I	R/A	I
P-3.04 Breach Detection	—	—	I	R	I
P-3.05 Penalty Claim	R	—	R	A	I
P-3.06 Quarterly Review	C	—	R	R	A
P-3.07 User Activation	R	R	A	I	—
P-3.08 Scheduled Maintenance	R	I	I	A	—

R = Responsible (executes) | **A** = Accountable (sign-off) | **C** = Consulted | **I** = Informed | **—** = Not Involved

3.11.3 Process Flow — SLA Lifecycle

Stage	Activity	Role	Output
① **Monitor**	Continuous availability and performance monitoring (Azure Monitor, Defender)	Provider (NOC)	Real-time alerts; uptime data
② **Detect**	Incident detected or reported via PSD omnichannel	PSD / Customer	Ticket created → § 4.3
③ **Classify**	Priority assigned (P1–P4), SLA clock starts	PSD + Customer	Agreed priority; response timer
④ **Resolve**	Resolution per MTTR target; escalation if needed	Provider Engineering	Incident resolved → § 4.4
⑤ **Report**	Monthly SLA report generated; GOS and Availability calculated	SDM	SLA report → § 3.10.1
⑥ **Review**	Quarterly Service Review; CSI register updated	SDM + Customer + SC	CSI actions → § 4.10
⑦ **Penalise**	If breached: penalty claim, validation, financial payment	Customer → Provider Finance	Payment within 30 days

4 Service Support & Operations

4.1 Overview

This Section defines the operational support framework through which the Provider delivers day-to-day support services for the Platform. It establishes the structure, processes, and responsibilities for incident management, ticket lifecycle management, preventive maintenance, technical escalation, and operational change control. All support processes align with **ITIL 4 best-practice guidelines** and leverage the Provider's **omnichannel support model** to ensure rapid, traceable, and context-rich service delivery across all communication channels.

Support services apply to the **Production Environment** and, where explicitly agreed in the Commercial Contract, the **Staging Environment**. The Provider shall maintain documented support procedures and make them available to the Customer upon reasonable request. All support activities are recorded and tracked through the Platform's **embedded ticketing system**, providing end-to-end visibility for both the Provider and the Customer.

4.2 Provider Service Desk (PSD)

The **Provider Service Desk (PSD)** is the single point of contact for recording, managing, and resolving all technical support-related tickets, including Incidents, Service Requests, Problems, and Change Requests raised by the Customer. The PSD operates an **omnichannel support model** that unifies formal ticketing, real-time messaging, and traditional communication channels into a single, traceable support workflow. The PSD coordinates with the Customer's designated IT liaison for all support and maintenance services.

4.2.1 Embedded Ticketing System

The Platform incorporates a **native embedded ticketing system** within the ProjectVIEW ERP application itself. This integrated ITSM capability allows Authorised Users to raise, track, and manage support tickets directly from within the Platform without leaving the ERP environment. The embedded ticketing system provides:

(a) **In-Application Ticket Logging:** Users raise tickets directly within the ProjectVIEW ERP interface, with automatic capture of contextual information including the active module, screen, user role, and any associated data records;

(b) **Real-Time Status Tracking:** A unified dashboard within the ERP displays all open, in-progress, and resolved tickets with full lifecycle visibility, SLA countdown timers, and priority indicators;

(c) **Bi-Directional Communication:** Threaded conversations between the Customer and the assigned support engineer occur within the ticket itself, maintaining a complete chronological audit trail;

(d) **Attachment & Evidence Capture:** Users attach screenshots, error logs, documents, and screen recordings directly to tickets, eliminating context loss during escalation;

(e) **SLA Metrics & Reporting:** Built-in SLA tracking with automated alerts when response or resolution targets approach threshold, along with real-time reporting on ticket volumes, categories, and resolution performance;

(f) **Knowledge Base Integration:** The ticketing system links to the Provider's embedded knowledge base (wiki), surfacing relevant articles and known solutions during ticket creation to enable self-service resolution;

(g) **Automated Notifications:** Email and in-application notifications are triggered at each ticket state transition (logged, acknowledged, assigned, updated, resolved, closed), keeping all stakeholders informed.

The embedded ticketing system serves as the **system of record** for all support interactions. Regardless of the channel through which an issue is initially reported (telephone, email, WhatsApp, or in-application), all tickets must be formalised within the embedded ticketing system to ensure SLA measurement, auditability, and compliance.

4.2.2 Omnichannel Support Channels

The Provider shall provide the Customer with access to the PSD through the following channels:

Channel	Availability	Ticket Types	Use Case
Embedded Ticketing (In-Application)	**24 × 7 × 365**	All types	Primary channel. Authorised Users raise tickets directly within ProjectVIEW ERP with automatic context capture. Recommended for all non-emergency issues.
WhatsApp Business (Dedicated Group)	**24 × 7 × 365**	P3, P4, Enquiries	Shared WhatsApp group between the Customer's key users and the Provider's assigned consultants for expedient informal communication, quick enquiries, and ad-hoc guidance. Messages requiring formal action are escalated to the embedded ticketing system.
Telephone	**24 × 7 × 365**	P1, P2	Priority-1 (Critical) and Priority-2 (Urgent) incidents requiring immediate attention. The Customer shall report P1 and P2 incidents by telephone to ensure prompt escalation.
Email	**24 × 7 × 365**	All types	Formal ticket logging for all ticket types. Emails sent to the designated PSD address are automatically ingested into the embedded ticketing system and assigned a ticket reference.

4.2.3 WhatsApp Business Support Channel

The Provider establishes a **dedicated WhatsApp Business group** for each Customer, connecting the Customer's designated key users with the Provider's assigned consultants. This channel operates as an **expedient informal communication layer** to complement the formal ticketing system. The WhatsApp channel is governed by the following rules:

(a) **Scope:** Quick enquiries, usage guidance, clarification of functionality, informal discussion of potential change requests, and preliminary reporting of non-critical issues. The WhatsApp channel is ***not*** a substitute for formal ticket logging;

(b) **Formalisation Rule:** Any issue communicated via WhatsApp that requires formal tracking, SLA measurement, code change, configuration modification, or escalation **must be logged as a ticket** in the embedded ticketing system by the Provider consultant within **4 hours** of identification. The Customer shall be notified of the ticket reference;

(c) **SLA Exclusion:** SLA response and resolution timers commence upon formalisation of the ticket in the embedded ticketing system, not upon initial WhatsApp communication;

(d) **Data Protection:** Participants shall not share Personal Data, credentials, database content, or Confidential Information via WhatsApp. The Provider shall brief all participants on data handling obligations under the applicable Data Protection Laws (ref. Section 17);

(e) **Retention:** WhatsApp messages are retained in accordance with the Provider's data retention policy. For auditability purposes, any substantive technical discussion or decision made via WhatsApp shall be summarised in the corresponding ticket record;

(f) **Group Membership:** Group membership is managed jointly. The Provider shall update group membership within 2 Business Days of any personnel change. The Customer shall notify the Provider of any changes to its designated key users.

4.2.4 PSD Operating Hours & Availability

The PSD operates **24 hours per day, 7 days per week, 365 days per year** for ticket logging across all channels. Resolution activities follow the operation windows defined in the SLA Response & Resolution Matrix (Section 3.6). UAE Government public holidays are excluded from Business Day calculations but P1 incidents are attended to regardless of public holiday schedules.

4.2.5 PSD Responsibilities

The PSD shall:

(a) Record all Customer-reported incidents and service requests in the **embedded ticketing system**, assigning a unique ticket reference number with automatic contextual metadata capture;

(b) Agree with the Customer the **priority level** to be allocated to each ticket in accordance with the Incident Priority Classification defined in Section 3.5;

(c) Provide the Customer with acknowledgement of ticket receipt, including the assigned ticket number, assigned engineer name, and estimated response time;

(d) Manage all necessary escalations to restore the Services within the applicable Service Level targets;

(e) Provide the Customer with regular progress updates via the ticketing system, telephone, email, or WhatsApp at mutually agreed intervals;

(f) Advise the Customer upon ticket resolution, including a brief description of the root cause, corrective action taken, and whether the ticket is to be closed or requires further action;

(g) Where possible, first attempt to resolve tickets **remotely**. Where remote resolution is not feasible, the Provider shall dispatch a qualified engineer to the Customer's premises as required;

(h) Formalise any issues initially communicated via WhatsApp or telephone into the embedded ticketing system within 4 hours;

(i) Maintain a complete audit trail of all ticket interactions, status changes, and resolution activities within the embedded ticketing system.

4.3 Ticket Lifecycle Management

All support interactions follow a structured **ticket lifecycle** managed through the Platform's embedded ticketing system to ensure traceability, accountability, and compliance with the SLA targets. The lifecycle applies to all ticket types: Incidents, Service Requests, Problems, and Change Requests, regardless of the channel through which the issue was initially reported.

4.3.1 Ticket Logging

When a ticket is logged by the Customer, the following minimum information shall be provided to the PSD:

(a) Customer name and contract reference (*auto-populated* when tickets are raised via the embedded ticketing system);

(b) Name and contact details of the person reporting the issue;

(c) A clear description of the issue, including **steps to reproduce** (for incidents) or the nature of the request (for service requests);

(d) The affected module(s) and number of impacted Authorised Users;

(e) Any diagnostics, screenshots, or error messages obtained by the Customer;

(f) The Customer's **proposed priority level** for the ticket.

4.3.2 Ticket Processing Workflow

The following procedure defines the method by which a ticket is processed from initial logging through to closure:

Step	Action	Responsibility
1	Customer logs a ticket via the embedded ticketing system (in-application), email, telephone, or WhatsApp. Tickets raised via the embedded system automatically capture module context, screen, user role, and related data records.	Customer
2	PSD receives the ticket in the embedded ticketing system (or formalises it from telephone/WhatsApp within 4 hours), assigns a unique ticket number, and allocates the ticket to the appropriate support engineer based on module expertise and priority.	PSD
3	PSD acknowledges the ticket via the embedded ticketing system and email, containing: ticket reference number, assigned engineer name, priority classification, and expected response time.	PSD
4	The assigned engineer contacts the Customer within the applicable response time, confirms the issue details, and begins diagnosis. Remote troubleshooting is attempted first.	Support Engineer
5	The engineer provides the Customer and PSD with an estimated time to resolution or, if applicable, confirms the ticket has been resolved remotely.	Support Engineer
6	Upon resolution, the engineer completes a Service Report detailing: ticket reference, time taken, root cause analysis, corrective action, and any preventive recommendations.	Support Engineer
7	PSD notifies the Customer of resolution via email, provides the Service Report, and requests confirmation to close the ticket or flags any required follow-up actions.	PSD
8	Customer confirms resolution or requests further action. Ticket is closed in the embedded ticketing system with full audit trail preserved.	Customer / PSD

Ticket Reopening: If the Customer reports that the same issue recurs within **5 Business Days** of ticket closure, the original ticket shall be reopened with the same priority classification within the embedded ticketing system. Reopened tickets are counted as a single incident for SLA measurement purposes.

4.3.3 Ticket Classification

Tickets are classified into the following categories:

Ticket Type	Definition	Examples
Incident	An unplanned interruption or reduction in quality of the Platform or a component thereof.	System unavailable, module crash, data not saving, report generation failure, login errors.
Service Request	A formal request from the Customer for something to be provided, changed, or actioned that is not an incident.	New user creation, password reset, access permission change, report configuration, data export.
Problem	The underlying root cause of one or more incidents, identified through trend analysis or post-incident review.	Recurring timeout errors traced to database indexing, repeated memory overflow from specific module.
Change Request	A formal request for modification to the Platform's configuration, functionality, or integration.	New field addition, workflow modification, API integration, report customisation, module enhancement.

4.4 Technical Escalation

The Provider maintains a structured **technical escalation matrix** to ensure that tickets are escalated to the appropriate level of expertise and management authority when resolution is not achieved within the applicable Service Level targets or when the severity of the issue requires senior intervention.

4.4.1 Escalation Levels

Level	Escalation Trigger	Escalated To	Target Action
Level 1 First Response	Ticket logged and assigned. Initial diagnosis and remote troubleshooting.	PSD Support Engineer	Diagnose, apply known fix, or escalate within response time.
Level 2 Specialist	Level 1 unable to resolve within MTTR target, or issue requires deep module expertise.	Senior Support Engineer / Module Specialist	In-depth analysis, code-level debugging, configuration review, hotfix development.
Level 3 Engineering	Level 2 unable to resolve, or issue involves core platform architecture, database, or infrastructure.	Development Team Lead / Principal Engineer	Code modification, database remediation, architectural intervention, patch release.
Level 4 Management	Resolution exceeds 2× MTTR target, or P1 incident not resolved within 8 hours, or Customer requests management escalation.	Service Delivery Manager / CTO	Resource reallocation, executive communication, recovery plan activation, post-incident review.

4.4.2 Customer-Initiated Escalation

The Customer may escalate a ticket at any time by contacting the PSD and requesting escalation. The Provider shall update the **Escalation Contact Matrix** at least annually or upon any change in personnel,

and shall provide the current matrix to the Customer within 5 Business Days of any update. The Escalation Contact Matrix shall include name, designation, direct contact numbers, and email address for each escalation level.

For **P1 (Critical) incidents**, the Provider shall automatically escalate to Level 2 within **30 minutes** if the initial response has not identified a resolution path, and to Level 3 within **2 hours** if the incident remains unresolved. The Customer's designated IT liaison and the Service Delivery Manager shall be notified of all P1 escalations in real time.

4.5 Preventive Maintenance

The Provider shall perform **monthly preventive maintenance** on all Platform components within the Customer's dedicated private sovereign environment. Preventive maintenance is conducted proactively to identify and remediate potential issues before they impact service availability or performance.

4.5.1 Preventive Maintenance Scope

Monthly preventive maintenance shall include, but is not limited to:

(a) **Infrastructure Health Checks:** Virtual machine performance monitoring, disk utilisation, memory allocation, CPU load analysis, and network latency assessment;

(b) **Database Maintenance:** Index rebuilding, statistics updates, transaction log management, integrity checks (DBCC CHECKDB), and storage optimisation;

(c) **Security Patching:** Review and application of operating system, middleware, and database security patches in accordance with the Provider's patch management policy (see Section 3.2.3 for maintenance windows);

(d) **Backup Verification:** Validation of backup job completion, backup integrity testing, and restore drill execution (quarterly);

(e) **Application Health:** Module-level functional checks, API endpoint validation, integration monitoring, and error log review across all active ProjectVIEW ERP modules;

(f) **SSL/TLS Certificate Management:** Certificate expiry monitoring, renewal, and rotation;

(g) **Capacity Review:** Assessment of current resource utilisation against provisioned capacity, with proactive scaling recommendations where utilisation exceeds 75% threshold.

4.5.2 Preventive Maintenance Reporting

Upon completion of each preventive maintenance cycle, the Provider's maintenance engineer shall submit a **Preventive Maintenance Report** to the Customer within **3 Business Days**. The report shall include:

- Date and duration of maintenance activity;
- Components inspected and actions performed;
- Identified risks or anomalies with recommended remediation;
- Current vs. provisioned resource utilisation metrics;
- Upcoming patch and update schedule;
- Confirmation of backup verification results.

4.6 Change Management

All modifications to the Platform's configuration, functionality, or infrastructure are governed by a formal **Change Management process** designed to minimise risk to the Production Environment. Changes are classified and managed in accordance with ITIL Change Management best practices.

4.6.1 Change Classification

Change Type	Definition	Approval	Deployment Path
Standard	Pre-authorised, low-risk changes with established procedures (e.g., user account creation, routine configuration).	Pre-approved	Direct to Staging → UAT → Production
Normal	Non-routine changes requiring assessment, planning, and approval (e.g., new module configuration, API integration, workflow modification).	Change Advisory Board (CAB) or Service Delivery Manager	Development → Staging → UAT → Customer Sign-off → Production
Emergency	Urgent changes required to restore service or address a critical security vulnerability. Bypasses standard CAB review.	Service Delivery Manager with post-implementation CAB review	Development → Production (with retrospective UAT and documentation)

4.6.2 Change Management Workflow

All Normal and Emergency changes follow this workflow:

(a) **Request:** The Customer or Provider submits a Change Request via the PSD with description, business justification, affected modules, and requested implementation date;

(b) **Assessment:** The Provider performs an impact assessment covering: technical risk, affected users, rollback plan, estimated effort, and dependencies;

(c) **Approval:** The Change Advisory Board (or Service Delivery Manager for emergency changes) reviews and approves or rejects the change;

(d) **Implementation:** The change is developed and deployed to the Staging Environment;

(e) **UAT:** The Customer performs Universal User Acceptance Testing in the Staging Environment. A minimum of 5 Business Days is provided for UAT. Written sign-off is required (ref. Section 3.3.1);

(f) **Deployment:** Upon Customer UAT sign-off, the change is deployed to Production during an agreed maintenance window;

(g) **Post-Implementation Review:** The Provider monitors the change for 5 Business Days post-deployment and provides a closure report to the Customer.

Rollback: Every Normal and Emergency change shall include a documented **rollback plan**. If the change causes an unplanned service degradation, the Provider shall execute the rollback within **2 hours** of identifying the issue and notify the Customer immediately.

4.6.3 Change Auditability

All changes to the Platform's configuration, codebase, and infrastructure are logged in the Provider's **Change Management System**. Each change record includes: requester, description, risk assessment,

approval chain, implementation date, implementing engineer, test results, and post-implementation status. Change logs are available to the Customer upon request and are included in the Quarterly Service Review (ref. Section 3.10.2).

4.7 Software Release Management

The Provider manages all software deliveries through a controlled **release management process** that distinguishes between two fundamentally different delivery types: **Releases/Updates** (incremental, client-specific, frequent) and **Upgrades** (major version, product-wide, annual). This distinction ensures that day-to-day agile delivery for the Customer does not conflict with the Provider's broader product roadmap.

4.7.1 Releases & Updates (Incremental – e.g. v11.xx)

Releases and updates are **incremental deliveries** within the current major version of the Platform (e.g., v11.01, v11.02, v11.15). They address change requests, bug fixes, configuration adjustments, and minor functional enhancements specific to the Customer's implementation. Releases are delivered using an **Agile execution methodology** tailored to the operational cadence of the Customer.

Agile Sprint Methodology: The Provider operates in **short-cycle sprints averaging 3 Business Days** per sprint. Each sprint delivers a defined set of change requests, bug fixes, or configuration changes agreed with the Customer at sprint planning. The sprint cycle is as follows:

Phase	Duration	Activities	Responsibility
Sprint Planning	0.5 day	Provider and Customer review the backlog, prioritise items, and agree on the sprint scope. Items are drawn from: open tickets, change requests, bug reports, and Customer-requested enhancements.	Provider + Customer
Development	1.5–2 days	The Provider's development team implements the agreed changes on the Customer's dedicated client branch in the Git repository. Unit testing is performed by DANAOS Support Engineers who are subject-matter experts within their domain.	Provider
Staging Deployment	0.25 day	Completed sprint items are deployed to the Staging Environment via the Provider's CI/CD pipeline for Customer validation.	Provider
UAT & Sign-Off	Per Section 3.3.1	The Customer performs Universal User Acceptance Testing on the sprint deliverables. Written sign-off is required before production deployment. Minimum 5 Business Days for UAT.	Customer
Production Deployment	0.25 day	Upon UAT sign-off, the sprint release is deployed to Production during an agreed maintenance window. Post-deployment monitoring is active for 2 Business Days.	Provider
Sprint Retrospective	Ad hoc	Brief review of sprint outcomes, issues encountered, and process improvements. Findings feed into the CSI register (ref. Section 4.10).	Provider + Customer

Release Versioning: Each incremental release is assigned a **semantic version number** within the current major version (e.g., v11.01, v11.02… v11.xx). The version number increments sequentially with each sprint delivery. The Provider maintains a release log accessible to the Customer through the Platform.

Release Category	Description	Frequency	Notice Period
Hotfix / Patch	Critical bug fixes and security patches addressing specific production issues or vulnerabilities. Deployed outside the normal sprint cycle.	As required	Emergency: ASAP Planned: 5 Business Days
Sprint Release (Client-Specific)	Bundled change requests, bug fixes, and minor enhancements delivered at the end of each sprint. Specific to the Customer's client branch.	Every 3–5 Business Days (per sprint cycle)	Sprint planning provides advance visibility
Maintenance Release	COTS updates (OS, database, middleware patches), security hardening, and infrastructure optimisation. Applied across all Customer environments.	3–4 per year	10 Business Days

4.7.2 Upgrades (Major Version – e.g. v11 → v12)

Upgrades represent a **new major version** of the Platform (e.g., v11 → v12, v12 → v13). Upgrades are **product-wide releases** that encompass significant functional enhancements, new modules, UI/UX redesigns, new APIs/SDKs, architectural improvements, and major COTS version upgrades (e.g., .NET framework, SQL Server engine). Upgrades are released approximately **once per year** and represent a new software version number.

Major Upgrades typically include:

- **New Functional Enhancements:** Feature additions, new module capabilities, and workflow improvements driven by the Provider's product roadmap and Customer Advisory Board feedback;
- **UI/UX Improvements:** Interface redesigns, usability enhancements, accessibility improvements, and responsive design updates;
- **API & SDK Extensions:** New integration endpoints, enhanced Web API capabilities, and updated Software Development Kits;
- **COTS Platform Upgrades:** Migration to new versions of underlying technologies (.NET, SQL Server, IIS) as part of the Provider's technology currency commitment;
- **Security Enhancements:** Implementation of new security standards, encryption upgrades, and compliance with emerging regulatory requirements.

4.7.3 Integrated Release Management & Deployment Process

All releases (incremental) and upgrades (major version) are managed through the **Platform Release Centre** (), which serves as the central release management and distribution platform. The Platform provides the following capabilities:

(h) **Release Catalogue:** A complete catalogue of all available releases for each Customer, organised by application and version. Each release entry includes the release date, version number, and detailed release notes describing new features, fixes, and known issues;

(i) **Credential-Based Access:** Access to the Platform is secured via unique credentials assigned to the Customer's designated administrators. Access rights determine visibility of releases applicable to the Customer's licensed modules;

(j) **Release Notes & Change Logs:** Each release is accompanied by semantic and contextual comments describing the latest features, functionalities, and bug fixes, reviewed and approved by the Provider's Reviewer before publication;

(k) **On-Demand Availability:** Releases are available for download on-demand, subject to Customer administrator acceptance. The Provider notifies the Customer when a new release is available;

(l) **Audit Trail:** The Platform maintains a complete record of which releases have been made available, downloaded, and deployed for each Customer environment.

SaaS Deployment Model: In the SaaS delivery model, the Provider manages all deployments to the Customer's dedicated sovereign environment. The Customer does ***not*** self-install releases. The deployment process is as follows:

Step	Action	Channel
1. Notification	Provider publishes the release within the Platform and notifies the Customer's designated administrator via email and, where applicable, the WhatsApp Business Channel.	Portal + Email + WhatsApp
2. Release Review	Customer reviews the release notes, change log, and impact assessment within the Platform. Customer may raise questions or concerns via the embedded ticketing system or WhatsApp.	Portal + Ticketing
3. Staging Deployment	Provider deploys the release to the Customer's Staging Environment. For sprint releases, this occurs automatically at the end of each sprint.	Provider-managed
4. UAT	Customer performs Universal User Acceptance Testing. Minimum 5 Business Days. Results are documented in the embedded ticketing system.	Staging Environment
5. Sign-Off	Customer provides written UAT sign-off via the embedded ticketing system or email. No production deployment occurs without sign-off (except Emergency Hotfixes).	Ticketing + Email
6. Production Deploy	Provider deploys the approved release to Production during an agreed maintenance window (ref. Section 3.2.3). Deployment is executed via the Provider's CI/CD pipeline.	Provider-managed
7. Verification	Provider performs post-deployment verification checks and monitors for 2 Business Days. Customer is notified of successful deployment via the Platform and email.	Portal + Email + Ticketing

4.7.4 End-of-Life & Version Transition

The Provider's End-of-Life (EOL) policy, version-transition lifecycle, migration services, re-training programme, data-return procedures, and subscription-cessation processes are comprehensively defined in **Chapter 10 — End-of-Life, Version Transition & Subscription Cessation**. Chapter 10

governs all aspects of version lifecycle management from General Availability (GA) through EOL Announcement, End of Engineering (EOE), End of Life, and optional Extended Support.

For purposes of this Chapter, the following summary applies: the Provider shall give the Customer a minimum of **twelve (12) months' written notice** before a major version reaches End of Life. Upgrade assistance, including migration planning, data migration, integration adoption, re-training, and UAT support, is included within the Subscription Term at no additional cost. Full terms, timelines, and procedures are set out in Sections 10.1 through 10.14.

4.7.5 Version Control & Source Code Escrow

The Provider maintains all source code in a **Git-based version control system** that incorporates:

- **Master Branch:** The standard DANAOS application ("Vanilla Version") representing the current generally available release;
- **Client Branches:** Customer-specific configurations and customisations maintained as dedicated branches. Sprint releases are developed on the client branch;
- **Working Clones:** Developer working copies that are merged under stable conditions to incorporate new functionalities into the Master and Client branches.

All code changes are subject to **peer review via Pull Requests**, automated testing, and compliance with the Provider's Programming Guidelines covering code quality, business logic, and security best standards. Upon executing Commit and Push, and after any Pull Request review, application versions are fully justified by the responsible programmer (or Agile Team) with semantic and contextual comments. Reviewers accept or reject changes based on the Provider's Programming Guidelines. Business logic is additionally verified by DANAOS Support Engineers who are subject-matter experts within their domain.

The Provider practices **Continuous Integration / Continuous Delivery (CI/CD)** for software deployment where appropriate. The CI/CD pipeline automates build, test, and deployment stages from the Git repository through to the Staging Environment, ensuring consistency and reducing manual deployment errors.

The Provider shall maintain a **Source Code Escrow** arrangement with an independent third-party Escrow Agent. The comprehensive terms governing the escrow deposit contents, update frequency, annual verification, release conditions, and Customer rights upon release are defined in **Section 9.14 (Source Code Escrow)**. The costs of the escrow arrangement, including the Escrow Agent's fees, shall be borne by the Customer (see § 9.14.4).

4.8 IMAC/RD Services

The Provider delivers **Install, Move, Add, Change, Remove, and Dispose (IMAC/RD)** services for the Platform as part of ongoing operational support. IMAC/RD activities are managed as Standard or Normal changes (ref. Section 4.6.1) and are subject to the following scope:

Type	Scope	Description
Install	Initial deployment	Installation and deployment of software applications, initial environment configuration, and integration setup for the Customer's dedicated sovereign environment.
Move	Relocation	Migration of workstation configurations, reassignment of user profiles, environment relocation (e.g., data centre migration), or transfer of services between environments.

Add	Configuration change	Addition or modification of software configurations, module customisation, user permission updates, installation of approved software updates, and integration of new API endpoints.
Change	Modification	Modification of existing configurations, workflow adjustments, report customisation, and platform parameter changes as agreed with the Customer.
Remove	Decommission	Controlled decommissioning of modules, features, or integrations. Includes secure data deletion where applicable, with deletion reports provided to the Customer.
Dispose	End-of-life	Environmentally responsible disposal of decommissioned hardware (if applicable), data carrier sanitisation in accordance with NIST SP 800-88, and disposal certification.

IMAC/RD activities that fall outside the scope of the Subscription Term shall be quoted separately on a **per-manday basis**, agreed in writing between the parties before commencement of work.

4.9 Enterprise Architecture Guidance

The Provider shall advise the Customer on **enterprise architecture** matters relating to the Platform, including system integration, data flow design, and technology alignment. This includes:

(m) **Integration Architecture:** Guidance on connecting ProjectVIEW ERP with the Customer's existing enterprise systems (e.g., SAP, Oracle, banking platforms, HR systems) via the Platform's native Web API (ref. Section 2.5);

(n) **Data Architecture:** Advisory on data flow, data migration planning, master data management, and reporting architecture within the Customer's dedicated sovereign environment;

(o) **Security Architecture:** Guidance on network security, access control policies, encryption standards, and alignment with the security framework detailed in Part B of this Framework;

(p) **Scalability Planning:** Proactive recommendations for environment scaling based on user growth projections, data volume trends, and module activation plans.

Enterprise architecture guidance is provided as an **advisory service** and does not extend to the design, development, or support of third-party systems. Implementation of architectural recommendations is subject to separate scoping and costing as agreed between the parties.

4.10 Continual Service Improvement (CSI)

The Provider operates a **Continual Service Improvement (CSI)** programme aligned with ITIL 4 practices and contemporary **AIOps methodologies** to drive ongoing improvements in service quality, operational efficiency, and Customer satisfaction. The CSI programme includes:

- **AI-Assisted Trend Analysis:** Monthly analysis of incident volumes, categories, recurring issues, and resolution times using pattern recognition and anomaly detection to identify systemic improvements proactively;
- **Root Cause Elimination:** Problem Management activities targeting the elimination of recurring incidents through permanent fixes, informed by cross-ticket correlation analysis;
- **Process Optimisation:** Regular review of support processes, ticket workflows, escalation procedures, and omnichannel support effectiveness to reduce resolution times and improve Customer experience;

- **Customer Feedback & Experience Management:** Incorporation of Customer satisfaction survey results, Quarterly Service Review feedback, and WhatsApp channel effectiveness metrics into the CSI register;
- **Technology Refresh:** Proactive identification of COTS updates, security enhancements, and platform optimisations that benefit the Customer;
- **Knowledge Management:** Continuous enrichment of the embedded knowledge base with solutions from resolved tickets, enabling higher self-service resolution rates and reducing repeat incident volumes.

The CSI register is maintained by the Service Delivery Manager and reviewed during each Quarterly Service Review (ref. Section 3.10.2). All CSI initiatives are tracked from identification through implementation with measurable outcomes. Where the Provider adopts AI-assisted tools in support operations, their use shall comply with applicable governance frameworks including the **EU AI Act** and the **NIST AI Risk Management Framework (AI RMF 1.0)**.

Reference URLs:

ITIL 4 Foundation – PeopleCert / Axelos

ProjectVIEW ERP Ticketing System – DANAOS Projects

WhatsApp Business Platform – Meta

Azure Service Health – Microsoft

NIST SP 800-88 Media Sanitization Guidelines

NIST AI Risk Management Framework (AI RMF 1.0)

EU AI Act – European Commission

4.11 Process Register

The following table summarises the service support and operational processes established in this Chapter, including responsible roles, expected outcomes, and cross-references to related processes in other Chapters.

Role Legend: P = Provider | C = Customer | PSD = Provider Service Desk | SDM = Service Delivery Manager | CAB = Change Advisory Board | SC = Steering Committee

4.11.1 Process Registry

Ref	Process	Trigger	Handler	Approver	Expected Outcome	Cross-Ref
P-4.01	Ticket Logging	Issue or request raised via any channel	PSD	—	Ticket created in Embedded Ticketing System (system of record)	§ 4.3.1, § 3.5

P-4.02	Ticket Lifecycle Mgmt	Ticket created	PSD / Engineering	Customer (closure)	Resolved and closed ticket with documented resolution	§ 4.3.2
P-4.03	WhatsApp Formalisation	Issue raised via WhatsApp channel	PSD	—	Formal ticket created within 4 hours	§ 4.2.3
P-4.04	Technical Escalation	Resolution time exceeded or complexity warrants	L1 → L2 → L3 → L4	SDM (L3+)	Issue escalated to appropriate expertise level	§ 4.4
P-4.05	Preventive Maintenance	Monthly schedule	Provider (Infra)	SDM	Health report delivered within 3 BD	§ 4.5, § 3.2.3
P-4.06	Change Management	Change Request submitted	Provider / CAB	CAB (Normal/Emergency)	Change deployed via UAT gate	§ 4.6
P-4.07	Sprint Release Deployment	Sprint completion (~3 BD cycle)	Provider (Dev)	Customer (UAT sign-off)	Release v11.xx deployed to Production	§ 4.7.1, § 3.3.1
P-4.08	Major Version Upgrade	Annual product release	Provider (Product)	Steering Committee	Customer upgraded to new major version	§ 4.7.2, Ch. 10
P-4.09	IMAC/RD Service Delivery	Customer service request	Provider (assigned team)	Customer IT Liaison	Service delivered; billed per manday pricing	§ 4.8, § 6
P-4.10	CSI Cycle	Quarterly Service Review	SDM	Steering Committee	CSI register updated; improvement actions tracked	§ 4.10, § 3.10.3

4.11.2 RACI Matrix

Process (Ref)	Provider	PSD	Customer	SDM	CAB/SC
P-4.01 Ticket Logging	—	R	C	I	—
P-4.02 Ticket Lifecycle	R	R	A	I	—
P-4.03 WhatsApp Formalise	—	R	I	I	—
P-4.04 Escalation	R	R	I	A	—
P-4.05 Prev. Maintenance	R	I	I	A	—

P-4.06 Change Mgmt	R	C	C	C	A
P-4.07 Sprint Release	R	I	A	C	I
P-4.08 Major Upgrade	R	I	C	R	A
P-4.09 IMAC/RD	R	C	A	I	—
P-4.10 CSI Cycle	C	I	C	R	A

R = Responsible (executes) | **A** = Accountable (sign-off) | **C** = Consulted | **I** = Informed | **—** = Not Involved

4.11.3 Process Flow — Support & Operations Lifecycle

Stage	Activity	Role	Output
① **Raise**	Issue raised via Embedded Ticketing, WhatsApp, phone, or email	Customer / PSD	Ticket in system of record
② **Triage**	PSD classifies (Incident / Service Request / Problem / Change) and assigns priority	PSD	Classified ticket → § 3.5
③ **Resolve**	Engineering resolves per MTTR; escalation if needed (L1→L4)	Provider Engineering	Resolution / workaround
④ **Change Gate**	If change required: RFC → CAB review → approval	Provider / CAB	Approved change → § 4.6
⑤ **Sprint / Build**	Development in 3-day Agile sprint; CI/CD to Staging	Provider (Dev)	Release in Staging → § 4.7.1
⑥ **UAT**	Customer validates in Staging; written sign-off required	Customer	UAT sign-off → § 3.3.1
⑦ **Deploy**	Production deployment via Platform Release Centre	Provider (Ops)	Live in Production → § 4.7.3
⑧ **Close & Learn**	Ticket closed; knowledge base updated; CSI input	PSD / SDM	Closed ticket; CSI register → § 4.10

5 Software Quality & Testing

5.1 Overview & Purpose

This chapter establishes the **Software Quality & Testing (SQT) framework** governing how the Provider assures the functional correctness, performance integrity, and data reliability of ProjectVIEW ERP prior to every deployment into the Customer's Production environment.

No Release, Update, or Upgrade (as defined in Chapter 1, §1.4) shall be promoted to Production without successfully completing the testing lifecycle described herein.

The Provider operates a differentiated, AI-augmented testing methodology that leverages custom AI Testing Agents built on the Provider's proprietary testing framework to interface directly with each Customer's ProjectVIEW ERP instance. This approach enables automated simulation of end-to-end data flows, realistic user-interaction scenarios, and comprehensive data-integrity validation — capabilities that far exceed conventional manual or script-based QA.

In addition to defect prevention, the SQT framework incorporates a proactive Process Optimisation Advisory service whereby AI-agent outputs are analysed to identify workflow inefficiencies, configuration anomalies, and data-model improvement opportunities within each Customer's deployment. These insights are delivered as actionable recommendations during Quarterly Service Reviews (§3.9).

5.2 Scope

The SQT framework applies to all software artefacts deployed to Customer environments under this Framework, including but not limited to:

(a) Releases/Updates (v11.xx) — incremental client-specific changes delivered via 3-day Agile sprints (§4.7).

(b) Upgrades (v11 → v12) — major-version product-wide changes delivered approximately annually (§4.8).

(c) Configuration changes — module activation, workflow customisation, report templates, role and permission adjustments.

(d) Data migration artefacts — import transformations, ETL scripts, schema migration patches.

(e) Integration interfaces — API endpoints, webhook handlers, third-party connector adaptors.

(f) Infrastructure changes — database engine updates, middleware version upgrades, TLS certificate rotations.

The SQT framework covers both the Provider's internal testing (§5.4–§5.7) performed prior to Customer UAT, and the Customer's Universal User Acceptance Testing (§5.8) that serves as the formal production-readiness gate.

5.3 AI-Augmented Testing Framework

5.3.1 Architecture Overview

The Provider employs a purpose-built AI testing platform comprising three core layers:

Layer	Component	Function
Orchestration	AI Testing Framework AI Agents	Custom AI agents that interpret test specifications, generate test scenarios, execute test sequences, and evaluate results autonomously.
Integration	secure API integration layer	Open-standard protocol enabling AI Testing Agents to interface with ProjectVIEW ERP APIs, database endpoints, and UI automation hooks in a structured, auditable manner.
Execution	Per-Client Test Environments	Dedicated Dev/Sandbox environments (§2.3.1) provisioned per Customer, populated with anonymised production-equivalent data to ensure test fidelity.

5.3.2 AI Testing Agents

Each Customer's ProjectVIEW ERP instance is paired with one or more custom AI Testing Agents, configured with domain-specific knowledge of the Customer's:

- **Module Configuration:** Activated modules (e.g., Project-Management, Contract-Management, Quality-Management) and their interdependencies.
- **Business Rules:** Approval workflows, escalation matrices, notification rules, and calculation formulae specific to the Customer's operational requirements.
- **Data Schema:** Custom fields, lookup tables, coded value domains, and relational integrity constraints configured in the Customer's instance.
- **Role Taxonomy:** User roles, permission sets, and segregation-of-duties rules applicable to the Customer's organisation.
- **Integration Map:** Connected third-party systems (accounting, HR, document management, BI) and their data-exchange contracts.

AI agents are version-controlled alongside the application codebase using the Provider's Git branching strategy (Master → Client → Working branches, §4.7.2) ensuring that test configurations evolve in lockstep with the software they validate.

5.3.3 Secure API Integration

The secure API integration layer provides the structured communication layer between AI Testing Agents and ProjectVIEW ERP, enabling:

(a) **API Invocation:** Agents invoke ProjectVIEW REST/GraphQL APIs to create, read, update, and delete records, simulating real user transactions without UI dependency.

(b) **Database Inspection:** Read-only access to the Customer's Dev/Sandbox database to validate data-integrity constraints, referential consistency, and computed fields post-transaction.

(c) **UI Automation Hooks:** Where business logic is tightly coupled to the front-end (e.g., conditional field visibility, dynamic form validation), the integration layer routes agent instructions through a headless browser interface that faithfully renders the ProjectVIEW UI.

(d) **Event Capture:** All agent-ERP interactions are logged to an immutable audit trail, including request payloads, response codes, timing metrics, and assertion results.

API connections are authenticated using short-lived, scoped API tokens that grant only the permissions required for the current test suite. Tokens are rotated automatically per test session and cannot be used against Production environments.

5.4 Testing Methodology

5.4.1 Test Levels

The Provider's testing lifecycle encompasses five progressive levels, each with defined entry criteria, exit criteria, and accountability:

Level	Name	Scope	Method	Exit Criteria
L1	Unit Testing	Individual functions, methods, stored procedures	Automated — developer-authored tests run in CI/CD pipeline	100% of new/modified units pass; code coverage ≥ 80%
L2	Integration Testing	Inter-module data flows, API contracts, event propagation	AI Agent — AI Testing Agents exercise cross-module transactions via the secure API integration layer	All integration scenarios pass; no data leakage between modules
L3	System Testing	End-to-end business processes within the full application stack	AI Agent — agents simulate complete user journeys (e.g., project creation → procurement → invoicing → reporting)	All critical-path scenarios pass; performance within SLO thresholds
L4	Regression Testing	Previously validated functionality after code changes	AI Agent — agents re-execute the full regression suite against the Customer's configuration	Zero regression failures; no degradation in response times > 10%
L5	User Acceptance Testing (UAT)	Business-process validation by Customer stakeholders	Customer-executed — supported by Provider via test-case templates, data preparation, and defect triage	Written UAT sign-off by Customer authorised representative (§5.8)

5.4.2 Test Environments

All Provider-side testing (L1–L4) is executed exclusively in the Customer's dedicated Dev/Sandbox environment (§2.3.1). This environment is:

- Architecturally identical to Production — same database engine version, middleware stack, and application build.
- Populated with anonymised production-equivalent data — sufficient volume and variety to exercise realistic edge cases without exposing personal data.

- Isolated — no network connectivity to Production; separate DNS namespace and authentication realm.
- Resettable — snapshot/restore capability enables repeatable test runs from a known-good baseline.

Post Go-Live, the Dev/Sandbox environment transitions to a **Staging** role (§2.3.2), retaining all of the above properties while additionally serving as the UAT environment for the Customer.

5.5 End-to-End Data-Flow Simulation

5.5.1 Simulation Objectives

AI agents simulate realistic, end-to-end data flows that traverse the full lifecycle of a business transaction within ProjectVIEW ERP. The objectives are:

(e) Validate that data created in one module is correctly propagated, transformed, and available in all downstream modules.

(f) Confirm that business rules (approval chains, notifications, calculations) fire correctly at each stage.

(g) Verify that concurrent user actions do not cause race conditions, deadlocks, or data corruption.

(h) Measure transaction latency and throughput against defined SLO thresholds (§3.3).

5.5.2 Simulation Scenarios

The Provider maintains a library of parameterised simulation scenarios, each mapped to a core ProjectVIEW business process. The following table illustrates representative scenarios — the full library is tailored per Customer based on their activated modules and configuration:

Scenario ID	Business Process	Modules Traversed	Key Assertions
SIM-001	Project Initiation → Budget Approval → Procurement	Project-Management, Budget-Management, Procurement-Management	Budget ceiling enforced; PO auto-linked to budget line; approval workflow fires for amounts > threshold
SIM-002	Timesheet Entry → Cost Allocation → Invoice Generation	Resource-Management, Cost-Management, Invoicing	Hours correctly costed at contractual rates; invoice line items reconcile to approved timesheets
SIM-003	Change Order → Variation → Budget Revision → Client Billing	Contract-Management, Change-Management, Budget-Management, Invoicing	Variation value propagates to budget; client billing reflects approved variation amount
SIM-004	Quality Inspection → Non-Conformance → Corrective Action → Close-Out	Quality-Management, Document-Management	NCR auto-generated; corrective action tracked to closure; document trail complete

SIM-005	Subcontractor Onboarding → Insurance Verification → Work Assignment	Subcontractor-Management, Compliance, Resource-Management	Expired insurance blocks assignment; notification sent to subcontractor and PM

5.5.3 Data Seeding & Scenario Execution

Prior to each simulation run, AI agents autonomously:

(a) **Seed prerequisite data:** Create master records (projects, vendors, users, cost codes) required as inputs to the scenario under test.

(b) **Execute the transaction chain:** Invoke ProjectVIEW APIs via the secure API integration layer to perform each step of the business process in the correct sequence, with realistic data values and timing intervals.

(c) **Assert at each checkpoint:** After each step, the agent queries the database and/or API to confirm that the expected state change has occurred (record created/updated, workflow advanced, notification dispatched).

(d) **Capture evidence:** Every API call, database query, assertion result, and timing measurement is logged to an immutable test-evidence repository linked to the deployment ticket.

(e) **Clean up:** On completion, the agent restores the environment to baseline using the snapshot/restore capability, ensuring no test artefacts contaminate subsequent runs.

5.6 User-Interaction Simulation

5.6.1 Purpose

While API-level testing (§5.5) validates backend logic, User-Interaction Simulation validates that the ProjectVIEW user interface behaves correctly when operated by human users. AI agents replicate realistic user interactions including:

- Form completion with valid, invalid, and boundary-value data.
- Navigation through multi-step workflows (wizards, approval chains, document-upload sequences).
- Role-based access enforcement — agents impersonate users across different role/permission sets to confirm that UI elements are correctly shown/hidden, enabled/disabled.
- Responsive behaviour — testing across desktop and tablet viewport sizes to confirm layout integrity.
- Accessibility compliance — verifying that keyboard navigation, ARIA attributes, and contrast ratios meet WCAG 2.1 AA requirements.

5.6.2 Interaction Scenarios

User-interaction simulations are structured around persona-based test scripts:

Persona	Role	Key Interactions Tested
Project Manager	PM	Project creation, team assignment, budget entry, milestone tracking, report generation, change-order initiation

Site Engineer	Field User	Daily log entry, quality inspection, photo upload, safety checklist, timesheet submission
Procurement Officer	Buyer	Purchase requisition, vendor comparison, PO approval, goods receipt, invoice matching
Finance Controller	Finance	Cost review, budget variance analysis, invoice approval, payment certification, period-end close
Contract Administrator	Contracts	Contract registration, variation processing, claim management, subcontractor compliance checks
Executive / Client	Read-Only / Approver	Dashboard views, KPI drill-down, document review, approval actions on mobile

5.6.3 Defect Classification

Defects identified during user-interaction simulation are classified using the same severity taxonomy as operational incidents (§4.3):

Severity	Definition (UI Context)	Example	Action
P1 — Critical	Application crash, data loss, security bypass	Form submission deletes unrelated records; admin panel accessible without authentication	Immediate fix; blocks deployment
P2 — High	Core workflow broken, no workaround	Approval button unresponsive; mandatory field validation missing	Fix before UAT release
P3 — Medium	Functionality degraded but workaround available	Sort order incorrect on list view; date picker defaults to wrong timezone	Fix in current sprint if capacity permits
P4 — Low	Cosmetic or minor usability issue	Misaligned label; truncated tooltip text	Queued to backlog

5.7 Data Integrity Validation

5.7.1 Scope

Data integrity is validated at three levels after every test run and prior to any deployment promotion:

Level	Validation	Method
Referential	All foreign-key relationships are intact; no orphaned records exist	AI agent executes referential-integrity SQL queries against the full schema
Computational	Calculated fields, aggregations, and rollup values are mathematically correct	Agent compares computed values against independently calculated expected results
Temporal	Audit trails are complete; every record has valid created/modified timestamps and user attribution	Agent verifies audit-log completeness and chronological consistency

5.7.2 Integrity Assertions

The AI agent executes the following integrity assertions at the conclusion of each simulation scenario:

(a) **Zero Orphans:** SELECT queries across all junction and child tables confirm no records reference non-existent parent records.

(b) **Balance Verification:** For financial modules — total debits equal total credits within each cost centre; budget committed + actual + remaining equals budget total.

(c) **Sequence Integrity:** Auto-numbered sequences (document numbers, transaction IDs) contain no gaps and no duplicates.

(d) **Concurrency Safety:** Parallel agent threads executing conflicting updates produce deterministic, correct outcomes with appropriate optimistic-locking responses.

(e) **Encryption at Rest:** Sensitive fields (PII, financial data) are stored encrypted in the database; plaintext is only available through the application's decryption layer.

5.7.3 Data-Integrity Report

Each test cycle produces an automated Data-Integrity Report containing:

- Total assertions executed and pass/fail count.
- Detailed failure records with table, column, record ID, expected value, and actual value.
- Trend analysis comparing integrity scores across the last ten test cycles to identify degradation patterns.
- Remediation actions taken (auto-corrected vs. escalated to development).

Data-Integrity Reports are attached to the deployment ticket and included in the UAT evidence pack provided to the Customer.

5.8 Universal User Acceptance Testing (UAT)

5.8.1 UAT Prerequisites

The Provider shall not invite the Customer to commence UAT until the following prerequisites are satisfied:

(a) All L1–L4 test levels have been completed with zero P1/P2 defects outstanding.

(b) The Data-Integrity Report (§5.7.3) shows a 100% assertion pass rate.

(c) The Customer's Staging environment has been refreshed with the candidate build.

(d) Test-case templates, test data, and user credentials have been prepared and communicated to the Customer's designated UAT lead.

5.8.2 UAT Execution

UAT is executed by the Customer's designated representatives using the Staging environment. The Provider shall:

- Provide structured test-case templates aligned to the Customer's business processes.
- Prepare realistic test data that mirrors production scenarios without exposing personal data.
- Make the Service Desk available for defect logging, triage, and resolution during the UAT window.

- Assign a dedicated Provider QA resource as the UAT liaison, available for real-time support via the shared WhatsApp Business group (§4.4) and Embedded Ticketing System (§4.1).

5.8.3 UAT Sign-Off

No deployment to Production shall proceed without a written UAT sign-off from the Customer's authorised representative. The sign-off document shall confirm that the Customer has validated the release against their acceptance criteria and authorises promotion to Production.

If the Customer does not provide sign-off or rejection within ten (10) Business Days of the UAT start date, the Provider shall issue a written reminder. If no response is received within a further five (5) Business Days, the release shall be deemed accepted by the Customer.

5.8.4 UAT Defect Handling

Defects identified during UAT are managed through the Embedded Ticketing System (§4.1) and classified per the severity taxonomy in §5.6.3. The following rules apply:

- **P1/P2 defects:** Block UAT sign-off. The Provider shall remediate and re-present the affected functionality within the current sprint cycle.
- **P3 defects:** Do not block sign-off. The Provider shall remediate in the subsequent sprint and confirm resolution to the Customer.
- **P4 defects:** Logged to the backlog. Remediation is scheduled based on capacity and Customer priority input.

5.9 Process Optimisation Advisory

5.9.1 Overview

A unique capability enabled by the Provider's AI-augmented testing framework is the ability to generate actionable process-optimisation insights derived from the analysis of test execution data. This service transforms testing from a purely defensive quality gate into a proactive value-creation activity for the Customer.

5.9.2 Insight Generation

During test execution, AI agents continuously capture and analyse:

(a) **Transaction Latency Patterns:** Identifying workflow steps that consistently consume disproportionate processing time, indicating potential bottlenecks in business rules or data-access patterns.

(b) **Exception Frequencies:** Cataloguing validation failures, business-rule rejections, and approval denials to surface process friction points that may indicate misconfigured rules or unclear user guidance.

(c) **Data-Quality Anomalies:** Detecting patterns of incomplete records, default-value overuse, or systematic data-entry errors that suggest form redesign or mandatory-field adjustments.

(d) **Permission Conflicts:** Identifying role/permission combinations that create unnecessary approval bottlenecks or, conversely, segregation-of-duties gaps.

(e) **Underutilised Features:** Flagging activated modules or features that are configured but not exercised in realistic test scenarios, indicating potential training gaps or unnecessary licensing costs.

5.9.3 5.9.3 Recommendation Delivery

Process-optimisation recommendations are:

- **Compiled:** Into a structured Process Optimisation Report following each major test cycle (Sprint Release or Upgrade).
- **Classified:** By impact (High/Medium/Low), effort (configuration change, minor development, major development), and risk (no risk, low risk, requires UAT).
- **Presented:** To the Customer during the Quarterly Service Review (§3.9) by the Service Delivery Manager.
- **Tracked:** As action items in the Continuous Service Improvement (CSI) register (§4.10) with agreed timelines and ownership.

5.9.4 Scope Limitations

The Process Optimisation Advisory is provided on an informational basis. Implementation of any recommendation constitutes a configuration change or development request governed by the applicable change-management and sprint-planning processes (§4.6, §4.7). The Provider shall not implement optimisation changes without Customer approval and, where applicable, a formal Scope Change Request (§2.7).

5.10 Test Governance & Reporting

5.10.1 Test Evidence Repository

The Provider shall maintain a centralised, immutable test-evidence repository for each Customer, containing:

- Test plans and test-case specifications for each deployment.
- AI-agent execution logs (full API interaction traces, timestamps, assertion results).
- Data-integrity reports (§5.7.3).
- Process-optimisation reports (§5.9.3).
- UAT evidence packs (test-case results, defect logs, sign-off documents).
- Regression-suite evolution history (added/modified/deprecated test cases).

Test evidence is retained for the duration of the Framework plus twelve (12) months, or as required by applicable data-protection regulation (GDPR Art. 5(1)(e); UAE PDPL Art. 5), whichever is longer.

5.10.2 Quality Metrics

The Provider shall track and report the following quality metrics, included in the Quarterly Service Review (§3.9):

Metric	Definition	Target
Defect Escape Rate	Number of defects found in Production that should have been caught in testing, as a percentage of total deployment defects	< 2%

Test Coverage	Percentage of configured business processes covered by automated AI-agent test scenarios	≥ 90%
Regression Pass Rate	Percentage of regression test cases that pass without modification on each new build	≥ 98%
Mean Time to Defect Resolution	Average elapsed time from defect identification (L1–L4) to verified fix	≤ 4 hours (P1/P2); ≤ 2 Business Days (P3)
Data Integrity Score	Percentage of integrity assertions (§5.7.2) that pass in each test cycle	100%
UAT First-Pass Rate	Percentage of releases that achieve Customer UAT sign-off without re-submission	≥ 85%
Optimisation Insights per Cycle	Number of actionable process-optimisation recommendations generated per major test cycle	≥ 3

5.10.3 Continuous Improvement

The SQT framework is subject to continuous improvement in line with the Deming Cycle (Plan-Do-Check-Act):

(a) **Plan:** Test strategy and AI-agent configurations are reviewed and updated at the start of each quarter based on quality-metric trends and Customer feedback.

(b) **Do:** Updated test suites and agent configurations are deployed to the Customer's Staging environment.

(c) **Check:** Quality metrics (§5.10.2) are evaluated against targets; root-cause analysis is performed on any target misses.

(d) **Act:** Corrective and preventive actions are logged in the CSI register (§4.10) and executed in subsequent sprint cycles.

5.11 Security & Compliance

5.11.1 Test-Data Protection

All test data used in the SQT process is subject to the data-protection obligations of this Framework (Chapter [Data Protection — future chapter reference]). Specifically:

- Production data shall be anonymised or pseudonymised before use in non-production environments, in accordance with GDPR Art. 89(1) and UAE PDPL Art. 5.
- AI agents do not store Customer data beyond the test session. All data processed by AI Testing Agents is ephemeral and purged upon session termination.
- API tokens are scoped to the minimum permissions required, time-limited, and automatically revoked at session end.
- Test-evidence logs are encrypted at rest (AES-256) and in transit (TLS 1.3).

5.11.2 Agent Governance

The Provider's use of AI agents in the SQT framework is governed by:

- **EU AI Act Compliance:** AI agents used for software testing are classified as minimal-risk under the EU AI Act (Regulation (EU) 2024/1689), as they operate on non-production data within a controlled environment and do not make autonomous decisions affecting natural persons.

- **NIST AI RMF:** The Provider's AI testing methodology aligns with the NIST AI Risk Management Framework (AI RMF 1.0) principles of validity, reliability, and accountability.
- **Human Oversight:** AI agents operate under human supervision. All test results, optimisation recommendations, and deployment decisions require human review and approval before action is taken.
- **Transparency:** The Provider shall, upon Customer request, provide documentation of AI-agent configurations, decision logic, and interaction logs for any test cycle.

EU AI Act — Regulation (EU) 2024/1689

NIST AI Risk Management Framework 1.0

5.12 Process Register

5.12.1 Process Registry

Ref	Process	Trigger	Handler	Approver	Expected Outcome	Cross-Ref
P-5.01	AI Agent Configuration	New Customer onboarding or module activation	Provider QA Lead	SDM	Customer-specific AI agent configured, tested, and version-controlled	§2.4, §5.3.2
P-5.02	End-to-End Data-Flow Simulation	New build ready for L2/L3 testing	AI Testing Agent	Provider QA Lead	All simulation scenarios pass; evidence logged to test repository	§5.5, §4.7
P-5.03	User-Interaction Simulation	New build ready for L3 testing	AI Testing Agent	Provider QA Lead	All persona-based interaction scripts pass; defects classified	§5.6, §4.3
P-5.04	Data Integrity Validation	Completion of L2/L3 test run	AI Testing Agent	Provider QA Lead	100% integrity assertions pass; Data-Integrity Report generated	§5.7
P-5.05	Regression Suite Execution	Code change merged to Client branch	AI Testing Agent	Provider QA Lead	Full regression suite passes; no regressions detected	§5.4.1 L4, §4.7.2
P-5.06	UAT Preparation & Handover	L1–L4 testing complete with zero P1/P2	Provider QA Lead	SDM	Staging environment refreshed; test cases and data prepared; Customer notified	§5.8.1, §2.3.2
P-5.07	UAT Defect Resolution	Customer logs defect during UAT	Provider Dev Team	Provider QA Lead	Defect resolved per severity SLA; fix verified and re-presented	§5.8.4, §4.3

P-5.08	UAT Sign-Off	Customer completes UAT	Customer UAT Lead	Customer Authorised Representative	Written sign-off received; deployment to Production authorised	§5.8.3, §4.7.3
P-5.09	Process Optimisation Analysis	Completion of major test cycle	AI Testing Agent	SDM	Process Optimisation Report generated with classified recommendations	§5.9, §3.9
P-5.10	Test Governance Review	Quarterly cadence	Provider QA Lead	SC	Quality metrics reviewed; test strategy updated; CSI actions logged	§5.10, §4.10

5.12.2 RACI Matrix

R = Responsible | A = Accountable | C = Consulted | I = Informed

Process	Provider QA	AI Agent	Dev Team	Customer	SDM
P-5.01 AI Agent Configuration	R	—	C	I	A
P-5.02 Data-Flow Simulation	A	R	C	I	I
P-5.03 User-Interaction Simulation	A	R	C	I	I
P-5.04 Data Integrity Validation	A	R	I	I	I
P-5.05 Regression Suite Execution	A	R	C	I	I
P-5.06 UAT Preparation & Handover	R	C	C	I	A
P-5.07 UAT Defect Resolution	A	C	R	I	I
P-5.08 UAT Sign-Off	I	—	I	R/A	I
P-5.09 Process Optimisation	C	R	C	I	A
P-5.10 Test Governance Review	R	I	C	C	A

5.12.3 5.12.3 Process Flow — Software Quality & Testing Lifecycle

Stage	Activity	Role	Output
① Configure	Provision per-Client AI agent with module config, business rules, data schema, role taxonomy, and integration map	Provider QA Lead	Versioned AI Agent config in Git
② Simulate	Execute end-to-end data-flow and user-interaction simulations via the secure API integration layer against Dev/Sandbox	AI Testing Agent	Test execution logs + assertion results
③ Validate	Run data-integrity assertions (referential, computational, temporal) across full schema	AI Testing Agent	Data-Integrity Report
④ Regress	Execute full regression suite against Customer's configuration to confirm zero regressions	AI Testing Agent	Regression Pass/Fail report
⑤ Optimise	Analyse test data to generate process-optimisation insights and recommendations	AI Testing Agent	Process Optimisation Report
⑥ Prepare	Refresh Staging, prepare test cases, seed UAT data, notify Customer	Provider QA Lead + SDM	UAT evidence pack + Customer notification
⑦ Accept	Customer executes UAT against acceptance criteria; logs defects if any	Customer UAT Lead	UAT test results + defect tickets
⑧ Authorise	Customer provides written UAT sign-off; Provider promotes build to Production	Customer Auth. Rep. + Provider	Signed UAT document + Production deployment

6 Training & Knowledge Transfer

6.1 6.1 Overview & Purpose

This chapter defines the **Training & Knowledge Transfer (TKT) framework** governing how the Provider equips the Customer's personnel with the skills, knowledge, and operational competence required to maximise the value derived from ProjectVIEW ERP throughout the Subscription Term.

Effective training is a **critical success factor** for enterprise SaaS adoption. Industry data consistently demonstrates that inadequate end-user training is the primary cause of ERP under-utilisation, shadow processes, and avoidable support-ticket volume. The Provider's TKT framework is therefore designed not as a one-time implementation activity, but as a **continuous enablement programme** that evolves with the Customer's organisational maturity and the Platform's feature roadmap.

The framework encompasses **both online and hands-on training delivery**, self-paced digital learning, contextual in-application guidance, train-the-trainer certification, and a per-Client knowledge wiki — all calibrated to the Customer's activated modules, role taxonomy, and operational workflows.

Each Customer is provisioned with a dedicated, AI-enhanced documentation wiki at **https://docs.projectview.wiki/[client]** containing personalised training materials, recorded session transcripts, role-specific manuals, video libraries, and curriculum plans. All implementation training sessions are recorded and processed through AI transcription to generate personalised, searchable training content unique to each Customer's configuration, terminology, and operational context.

6.2 Scope

The TKT framework covers:

(a) **Implementation Training:** Structured training delivered during the implementation phase (§2.4) prior to Go-Live, covering all activated modules and customer-specific configurations.

(b) **Post Go-Live Enablement:** Ongoing training delivered after Go-Live to address new features introduced via Releases/Updates (§4.7), Upgrades (§4.8), and organisational changes (new hires, role changes, departmental expansion).

(c) **Train-the-Trainer Programme:** Certification of Customer-designated Super Users who assume responsibility for first-line internal training and support within their organisation.

(d) **Knowledge Base & Documentation:** Maintenance and delivery of comprehensive platform documentation, process guides, video tutorials, and release notes accessible through the the Platform's integrated release management module and the Customer's dedicated wiki at https://docs.projectview.wiki/[client].

(e) **Per-Client Training Wiki:** A dedicated, AI-enhanced documentation portal provisioned for each Customer, hosting personalised training materials, recorded session libraries, role-specific manuals, training plans and curricula, and AI-generated transcripts.

(f) **AI-Assisted Learning:** Integration of AI-driven contextual help, guided workflows, and intelligent search within the ProjectVIEW ERP interface to provide just-in-time assistance during daily operations.

(g) **Session Recording & AI Transcription:** All onboarding and training sessions are recorded and processed through AI transcription to produce personalised, searchable training material per

Client and per role, creating a unique knowledge asset that compounds over the lifecycle of the engagement.

(h) **DANAOS ProjectVIEW ERP Champions Programme:** A specialised training and examination programme for Customer-designated Champions who serve as Level 1 support contacts for intranet and extranet users and as the primary communication channel with the Provider from Go-Live onwards (§6.6).

(i) **GAP Analysis & Feedback:** A structured mechanism for attendees to register qualms, configuration requirements, and change requests during training, consolidated into a GAP Analysis Document for Customer approval (§6.4.6).

6.3 Training Delivery Model

6.3.1 Delivery Channels

The Provider delivers training through a blended model combining **online (virtual instructor-led and self-paced) and hands-on (on-site instructor-led)** delivery, comprising five complementary channels:

Channel	Format	Audience	When	Duration
Hands-On ILT (On-Site)	In-person instructor-led sessions at the Customer's premises with live system access	Customer project team, end users, management	Implementation phase; complex modules; Go-Live readiness	4–8 hours per module
Online ILT (Virtual)	Live virtual sessions via MS Teams / Zoom with shared-screen system access	Distributed teams, remote users, post Go-Live refreshers	Implementation phase + post Go-Live on request	2–4 hours per module
Self-Paced Digital Learning	Pre-recorded video modules, interactive walkthroughs, quizzes — hosted on Client wiki	All Authorised Users	Available continuously via https://docs.projectview.wiki/[client]	15–45 minutes per module
In-Application Guidance	Contextual tooltips, guided tours, embedded help panels within ProjectVIEW UI	All Authorised Users during daily operations	Always-on within the ProjectVIEW UI	N/A — on-demand
Train-the-Trainer (T3)	Intensive certification programme — virtual or on-site	Customer Super Users (max 3 per module)	Implementation phase; refreshed annually	2–3 days per certification track

6.3.2 Training Environment

All hands-on training is conducted exclusively in the Customer's dedicated Dev/Sandbox environment (§2.3.1), which:

- Contains anonymised production-equivalent data sufficient for realistic training scenarios.
- Is architecturally identical to Production, ensuring that trained workflows translate directly to live operations.
- Can be reset to a known-good baseline between training sessions to ensure consistent starting conditions.
- Is isolated from Production — trainees cannot inadvertently affect live data or active user sessions.

Post Go-Live, the Staging environment (§2.3.2) serves the same training function, with the additional benefit of reflecting the latest production configuration.

6.4 Implementation Training Programme

6.4.1 Training Needs Assessment

Prior to the commencement of implementation training, the Provider shall conduct a Training Needs Assessment (TNA) in collaboration with the Customer's Project Manager. The TNA identifies:

(a) The Customer's activated modules and their interdependencies.

(b) The organisational role taxonomy and the mapping of roles to ProjectVIEW permission sets.

(c) The number of users per role requiring training, and their current proficiency levels with ERP systems.

(d) Customer-specific business processes, approval workflows, and reporting requirements that training must address.

(e) Language requirements — all standard training materials are provided in English; translation requirements are identified during the TNA.

(f) Preferred training schedule, considering the Customer's operational calendar, time zones, and availability constraints.

6.4.2 Training Plan

Based on the TNA, the Provider shall deliver a structured **Training Plan** for each role-based track. **A physical or digital copy of the Training Plan is handed to each attendee at the start of their first onboarding session**, providing full visibility into the curriculum, schedule, and expected outcomes. The Training Plan contains:

Component	Description
Training Calendar	Date/time schedule for all ILT sessions, aligned to the implementation project plan milestones.
Module Curriculum	Per-module syllabus covering learning objectives, hands-on exercises, and assessment criteria.
Role-Based Tracks	Training paths tailored to each role (PM, Finance, Procurement, Site, Executive) ensuring users learn only what is relevant to their function.

Prerequisite Map	Dependencies between modules (e.g., Budget-Management training requires completion of Project-Management training).
Assessment Strategy	Competency evaluation approach — practical exercises, scenario-based assessments, knowledge checks.
Resource Allocation	Named Provider trainers assigned to each track; Customer attendee lists confirmed.
Materials Package	Training manuals, quick-reference cards, exercise workbooks, and video recordings delivered prior to each session.

6.4.3 Module Training Curriculum

The following table outlines the standard training curriculum mapped to the DANAOS ProjectVIEW ERP module suite, based on the Comprehensive Training Plans with Module Interdependencies & Data Flow Mapping. Customer-specific sessions are added based on the TNA (§6.4.1).

Total programme duration: 136 hours across 29 sessions plus the cross-modular Site Operations domain.

Code	Module	Target Roles	Duration	Sessions
PV_00	ProjectVIEW ERP Core	Digital Transformation Mgr (D20), Project Mgr (D11), IT Mgr (D21), Champion, C-Level (D22)	8 hrs	2
PV_01	Budget Estimation – Bidding	Cost Estimator (D3), Commercial/BD Mgr (D2), Bidding Mgr (D1), Planner (D6), QS (D5), Champion	12 hrs	3
PV_02	Cost Control	Cost Controller (D4), Construction Mgr (D10), Cost Estimator (D3), Planner (D6), PM (D11), QS (D5), Champion	12 hrs	3
PV_03	Subcontractors Management	Contract Mgr (D7), QS (D5), Cost Controller (D4), Procurement Mgr (D8), PM (D11), Champion	12 hrs	3
PV_04	Procurement & Purchasing	Procurement Mgr (D8), Store/Warehouse Mgr (D9), Cost Controller (D4), PM (D11), Champion	12 hrs	3
PV_05	Materials & Production Management	Store/Warehouse Mgr (D9), Procurement Mgr (D8), Production Mgr (D17), Site Engineer (D12), Champion	12 hrs	2
PV_06	Machinery Management	Plant/Fleet Mgr (D15), Site Engineer (D12), PM (D11), Maintenance Mgr, Champion	12 hrs	2
PV_07	HRMS – Payroll	HR Manager (D16), Payroll Officer, PM (D11), Cost Controller (D4), Champion	12 hrs	2
PV_08	Accounting – Finance Management	Chief Accountant (D18), Finance Mgr (D19), Cost Controller (D4), PM (D11), Champion	16 hrs	3

PV_09	Suppliers Account Payables	Accounts Payable Officer, Chief Accountant (D18), Procurement Mgr (D8), Champion	8 hrs	2
PV_10	Customers Account Receivables	Contract Mgr (D7), QS (D5), Chief Accountant (D18), Commercial Mgr (D2), Champion	12 hrs	2
PV_A	Site Operations & Labour Productivity	Site Engineer (D12), Foreman (D13), Safety Officer (D14), PM (D11), Champion	8 hrs	2

Prerequisite Chain: PV_00 (Core) is mandatory for all personnel before any module training. Module prerequisites follow the trilateral data-flow architecture: PV_01 → PV_02 → PV_03 (estimation → cost control → subcontractors); PV_00 → PV_04 → PV_05 (core → procurement → materials); PV_08 is required before PV_09/PV_10 (accounting before AP/AR). The cross-modular domain PV_A requires PV_02 + PV_06 + PV_07.

6.4.4 Session Breakdown per Module

Each module is delivered across focused sessions of 50–75 minutes, structured to accommodate the Customer's operational workload (§6.4.5). The detailed session breakdown, including per-topic time estimates, knowledge area descriptions, integration touchpoints, and hands-on exercises, is documented in the Provider's Comprehensive Training Plans document and personalised per Customer. The following provides the session index:

Code	Session	Session Title	Duration
PV_00	1	System Architecture & Company Setup	75 min
PV_00	2	Master Data & Integration Setup	75 min
PV_01	1	BoQ Import & Structure	60 min
PV_01	2	Cost Recipes & Budget Creation	70 min
PV_01	3	Bid Preparation & Submission	60 min
PV_02	1	Budget Setup & Cost Code Assignment	50 min
PV_02	2	Daily Transactions & Site Data Entry	50 min
PV_02	3	Cost Reports & Earned Value Analysis	60 min
PV_03	1	Contract Creation from Procurement	60 min
PV_03	2	Certifications, Deductions & Cost Codes	50 min
PV_03	3	Accounting Transfer, Variations & Reports	55 min
PV_04	1	MRF to Requisition	50 min
PV_04	2	Supplier Quotation & Evaluation	60 min
PV_04	3	Order Creation & Purchase Order	55 min
PV_05	1	Warehouse Setup & Goods Receipt	50 min
PV_05	2	Issuance, Invoicing, Production & Reports	70 min
PV_06	1	Fleet Setup, Allocation & Transactions	45 min

PV_06	2	Maintenance, Insurance & Reports	55 min
PV_07	1	Employee Management & Timesheets	60 min
PV_07	2	Payroll Processing & Labour Productivity	60 min
PV_08	1	Chart of Accounts & General Ledger	55 min
PV_08	2	Suppliers AP & Customers AR	60 min
PV_08	3	Financial Statements & Reporting	60 min
PV_09	1	Invoice Processing & Payment Scheduling	50 min
PV_09	2	AP Reports, Aging & Reconciliation	50 min
PV_10	1	Customer Contract & Certifications	50 min
PV_10	2	Claims, Variations, AR & Revenue Recognition	60 min
PV_A	1	Daily Transactions & Progress Entry	60 min
PV_A	2	Productivity Analysis & Site Reporting	60 min

Each session includes hands-on practice exercises, Q&A, and a consolidation review. All sessions are recorded (§6.9) and AI-transcribed to produce personalised reference material for each Customer's wiki (§6.8). **The Comprehensive Training Plans document with full per-topic breakdowns, master data checklists, attendee sign-off sheets, and GAP Analysis sections is handed to each attendee at the start of training (§6.4.2).**

6.4.5 Training Completion Criteria

Implementation training for each role-based track is deemed complete when:

(a) All scheduled ILT sessions for the track have been delivered.

(b) At least 80% of nominated attendees have participated in each session (attendance is recorded).

(c) Practical assessment exercises have been completed with a minimum competency score of 70%.

(d) The Customer's Project Manager has signed a Training Completion Certificate confirming satisfaction with the training delivered.

Training completion is a prerequisite for UAT commencement (§5.8.1). The Provider shall not invite the Customer to begin UAT until the applicable role-based training tracks have been completed to the satisfaction of both Parties.

6.4.6 Attendance Tracking & Schedule Accommodation

The Provider maintains a **formal attendance register for every training session**, recording the attendee name, role, knowledge area covered, session date, and duration. Attendance records are published to the Customer's dedicated wiki (§6.7.1) and included in the Training Completion Certificate (§6.4.4).

Recognising that Customer personnel cannot be fully withdrawn from their operational responsibilities during the onboarding phase, **training sessions are deliberately structured and scheduled to accommodate the Customer's daily workload**. Sessions are:

- **Modular:** Broken into focused sessions of 45–75 minutes (§6.4.3.1) rather than full-day marathons, enabling attendees to fulfil operational duties between sessions.
- **Flexible:** Scheduled around the Customer's operational peaks, project deadlines, and time-zone constraints — the Provider adjusts the training calendar in collaboration with the Customer's Training Coordinator.
- **Scrambled:** Sessions across different modules and role tracks are interleaved (not delivered sequentially by module), allowing team members to attend the sessions relevant to their role without blocking colleagues from attending other tracks simultaneously.
- **Repeatable:** Critical sessions are offered on multiple dates/times to accommodate shift patterns, site-based personnel, and absentees. All sessions are recorded (§6.8) for asynchronous review.

6.4.7 Training Feedback, Change Requests & GAP Analysis

Under each Training Plan, the Provider establishes a structured feedback mechanism that enables attendees to register **qualms, configuration requirements, and change requests** encountered during training sessions. This captures:

(a) **Qualms:** Concerns, uncertainties, or objections raised by users regarding workflows, UI design, or business-rule implementation that may indicate misalignment between the system configuration and the Customer's operational expectations.

(b) **Configuration Requirements:** Requests for field-label changes, additional dropdown values, custom report layouts, modified approval hierarchies, or other configuration adjustments identified during hands-on training exercises.

(c) **Change Requests:** Formal requests for workflow modifications, new functionality, or integration enhancements that go beyond configuration and require development effort, logged in accordance with the Change Management process (§4.5).

At the conclusion of the implementation training phase, the Provider consolidates all registered items into a **GAP Analysis Document** — a structured report that categorises every qualm, configuration requirement, and change request by module, severity, and recommended resolution.

The GAP Analysis Document is **formally presented to the Customer for review and written approval** before the Provider proceeds with any remediation, configuration adjustment, or change-request implementation.

The approved GAP Analysis Document forms a binding addendum to the Implementation Plan (§2.4) and its resolution status is tracked through to closure.

6.5 Train-the-Trainer (T3) Programme

6.5.1 Objective

The T3 programme creates a cadre of Customer-designated Super Users who are certified to deliver first-line training within their organisation, reducing dependency on the Provider for routine enablement activities and accelerating the onboarding of new hires.

6.5.2 Eligibility & Selection

Super User candidates must:

- Have completed the full implementation training curriculum for their assigned module(s).

- Demonstrate advanced proficiency through a practical assessment administered by the Provider.
- Be nominated by the Customer's Project Manager and committed to the T3 programme for a minimum of twelve (12) months.
- Have sufficient organisational authority to conduct training sessions and enforce adoption standards.

The Provider recommends a minimum of two (2) and a maximum of three (3) Super Users per activated module to ensure coverage for absence, attrition, and workload distribution.

6.5.3 Certification Curriculum

The T3 certification programme covers:

(a) **Advanced Module Mastery:** Deep-dive into module configuration, edge cases, and advanced workflows beyond standard end-user training.

(b) **Training Delivery Skills:** Principles of adult learning, session planning, facilitation techniques, and competency assessment — enabling Super Users to deliver effective training sessions.

(c) **First-Line Troubleshooting:** Common user errors, misconfiguration diagnosis, escalation procedures, and effective use of the Provider Service Desk (§4.2).

(d) **Knowledge Base Navigation:** Proficiency in using the Platform's integrated knowledge base to find answers, update internal documentation, and contribute to the Customer's internal wiki.

(e) **Release Readiness:** How to interpret release notes, assess training impact of new features, and prepare internal communications for Release/Update and Upgrade deployments (§4.7, §4.8).

6.5.4 Certification & Renewal

Super Users who complete the T3 curriculum and pass the certification assessment receive a DANAOS Certified Super User credential, valid for twelve (12) months. Renewal requires:

- Completion of the annual Release Readiness update training.
- Demonstrated continued activity — delivery of at least two (2) internal training sessions during the certification period.
- Passing a refresher assessment covering any new features or workflow changes introduced since the last certification.

6.6 DANAOS ProjectVIEW ERP Champions Programme

6.6.1 Overview

Beyond the Super User / Train-the-Trainer cadre (§6.5), each Customer is required to designate **DANAOS ProjectVIEW ERP Champions** — senior power users who serve as the Customer's primary operational interface with the Provider from Go-Live onwards. Champions undergo a **specialised training programme with formal examinations** and assume an elevated role encompassing Level 1 support, user advocacy, and strategic communication with the Provider.

6.6.2 Minimum Requirement & Selection

Each Customer must designate a minimum of two (2) Champions: one (1) Main Champion and one (1) Deputy Champion. The dual-Champion requirement ensures continuity of coverage during leave,

travel, or attrition. The Provider recommends that larger organisations (>50 Authorised Users) designate additional Champions to cover distinct functional domains (e.g., Finance Champion, Project Champion).

Champion candidates must:

- Have completed the full implementation training curriculum for their assigned module(s) with a minimum assessment score of 80% (above the standard 70% threshold).
- Hold the DANAOS Certified Super User credential (§6.5.4) or be concurrently enrolled in the T3 programme.
- Demonstrate cross-module awareness — Champions must understand the inter-module data flows and dependencies, not just their primary module.
- Be nominated by the Customer's senior management and committed to the Champion role for a minimum of twelve (12) months.
- Have direct access to the Customer's executive sponsor for escalation purposes.

6.6.3 Champions Training & Examination

Champion candidates undergo a **specialised training programme** that extends beyond the standard Super User certification and covers:

(a) **Cross-Module Integration Mastery:** End-to-end data-flow understanding across all activated modules, including inter-module triggers, cascading approvals, and consolidated reporting — mirroring the simulation scenarios defined in §5.5.2.

(b) **Intranet & Extranet Support:** Configuration and operational knowledge for both the internal company portal (intranet users) and the external stakeholder portal (extranet/portal users), including access management, permission troubleshooting, and data-visibility controls.

(c) **Escalation & Communication Protocol:** Formal procedures for triaging user issues, determining Level 1 vs. Level 2 classification, raising Service Requests and Incidents via the Provider Service Desk (§4.2), and communicating system updates to internal stakeholders.

(d) **Process Optimisation Awareness:** Understanding of the AI-generated process-optimisation reports (§5.9) and the ability to interpret and advocate for recommended workflow improvements within the Customer's organisation.

(e) **GAP Analysis Facilitation:** Skills to collect, categorise, and prioritise user qualms, configuration requirements, and change requests during training and operational use, contributing to the ongoing GAP Analysis process (§6.4.6).

Champions training concludes with a **formal examination** comprising:

- **Written Assessment:** A multiple-choice and short-answer examination covering cross-module knowledge, support protocols, and escalation procedures. Minimum pass mark: 80%.
- **Practical Scenario Assessment:** Live troubleshooting scenarios conducted in the Dev/Sandbox environment, where the candidate must diagnose, resolve, or correctly escalate simulated user issues within defined time constraints.
- **Communication Exercise:** Preparation and delivery of a mock stakeholder communication (e.g., system-update briefing, incident notification) evaluated for clarity, accuracy, and professionalism.

Candidates who pass all three examination components receive the **DANAOS ProjectVIEW ERP Champion** credential, valid for twelve (12) months and renewable via the same process as Super User recertification (§6.5.4), with the addition of a refresher examination.

6.6.4 Champion Responsibilities

Upon certification, Champions assume the following responsibilities:

(a) **Level 1 Support — Intranet Users:** Serve as the first point of contact for all internal company users (intranet) encountering operational issues, answering how-to questions, resolving configuration queries, and guiding users through standard workflows before any issue is escalated to the Provider Service Desk.

(b) **Level 1 Support — Extranet/Portal Users:** Provide equivalent first-line support for external stakeholder users accessing the Customer's ProjectVIEW portal (extranet), including subcontractors, joint-venture partners, and client representatives, addressing access issues, data-visibility queries, and document-sharing workflows.

(c) **Provider Communication Channel:** Act as the Customer's designated communication channel with the Provider from Go-Live onwards. Champions raise Service Requests and Incidents (§4.2), participate in the WhatsApp Business support group (§4.3), attend Quarterly Service Reviews (§3.9), and relay Provider communications (release notes, maintenance windows, service advisories) to the Customer's user base.

(d) **Adoption & Compliance Monitoring:** Monitor user adoption patterns, identify under-utilised features, flag shadow processes or workaround behaviours, and advocate for system-native workflows in alignment with the training curriculum.

(e) **Continuous Improvement Input:** Provide structured feedback to the Provider during Quarterly Service Reviews, contribute to the CSI register (§4.10), and facilitate user-feedback collection for process-optimisation recommendations (§5.9).

(f) **Knowledge Transfer:** Maintain and curate the Customer's internal wiki content, ensure new hires are onboarded using the personalised training materials (§6.8.3), and conduct ad-hoc refresher sessions for their user community.

6.7 Post Go-Live Enablement

6.7.1 Ongoing Training Triggers

The Provider shall deliver additional training sessions post Go-Live when triggered by any of the following events:

Trigger	Training Response	Delivery Channel	Lead Time
Release/Update (v11.xx)	Release-specific training covering new/changed features relevant to the Customer	Self-paced video + optional live Q&A	Delivered with or before release deployment
Upgrade (v11 → v12)	Comprehensive upgrade training covering all material changes to UI, workflows, and functionality	ILT (virtual or on-site) + self-paced modules	Minimum 10 Business Days before upgrade Go-Live
New User Onboarding	Role-based training for newly activated Authorised Users	Self-paced modules + Super User guided session	Within 5 Business Days of user activation
Role Change	Incremental training for users transitioning to a new role with different module access	Super User guided session + self-paced modules	Within 5 Business Days of role change
Process Change	Training on reconfigured workflows, new approval chains, or modified business rules	ILT (virtual) + updated documentation	Prior to process-change activation in Production
Support Ticket Pattern	Targeted remedial training when ticket analytics identify recurring user-error clusters	ILT or self-paced — at Provider's recommendation	Within 10 Business Days of pattern identification
Customer Request	Ad-hoc training on any module or process area requested by the Customer	ILT (virtual or on-site) as agreed	Scheduled within 15 Business Days of request

6.7.2 Release Training Protocol

For each Release/Update and Upgrade, the Provider shall:

(a) Publish detailed release notes within the Platform at least five (5) Business Days prior to deployment.

(b) Classify each change as Training Impact: High (new workflow/UI), Medium (modified behaviour), or Low (bug fix / cosmetic).

(c) Produce updated self-paced video modules for all High-impact changes.

(d) Conduct a live Release Briefing session (30–60 minutes) for Customer Super Users, covering all High and Medium-impact changes.

(e) Update all affected knowledge-base articles, quick-reference cards, and process guides.

(f) Notify all Authorised Users of available training materials via in-application notification.

6.8 Per-Client Training Wiki & Knowledge Base

6.8.1 Per-Client Training Wiki

Each Customer is provisioned with a **dedicated, AI-enhanced training wiki** at **https://docs.projectview.wiki/[client]**, accessible to all Authorised Users via single sign-on (SSO). The wiki serves as the Customer's central repository for all personalised training and knowledge-transfer assets, including:

- **Recorded Training Sessions:** Full video recordings of every instructor-led training session delivered during onboarding and post Go-Live, organised by module and role.
- **AI-Generated Transcripts:** Automated transcriptions of every recorded session, processed through AI to produce searchable, timestamped text with speaker identification, key-topic indexing, and action-item extraction.
- **Role-Specific Manuals:** Personalised user manuals generated per role, incorporating the Customer's specific module configuration, field labels, workflow names, and approval hierarchies.
- **Training Plans & Curricula:** The agreed Training Plan, module curricula, assessment criteria, and completion records for each training track.
- **Quick-Reference Cards:** Printable, one-page summaries for common tasks (e.g., "How to Create a Purchase Order"), auto-generated from the Customer's configured workflows.
- **Video Library:** Curated feature walkthroughs, quick-tip videos (2–5 minutes), and guided demonstrations maintained by the Provider and supplemented by the Customer's own recorded sessions.
- **FAQ & Troubleshooting:** Common issues, workarounds, and diagnostic steps — continuously updated based on the Customer's support-ticket patterns and AI analysis.
- **Release Notes:** Customer-specific release notes highlighting changes relevant to the Customer's activated modules and configuration.

ProjectVIEW Client Wiki — https://docs.projectview.wiki

6.8.2 Platform Release Centre

In addition to the per-Client wiki, the Provider might maintain a central Help Knowledge Base as part of the Platform containing platform-wide documentation organised into the following tiers:

Tier	Content Type	Audience	Update Frequency
Tier 1 — Platform Guides	Module-by-module functional documentation, screenshots, step-by-step workflows	All Authorised Users	Updated with each Release/Update

Tier 2 — Administration Guides	System configuration, user management, role/permission setup, integration configuration	Customer IT / Super Users	Updated with each Release/Update
Tier 3 — API & Integration Documentation	REST/GraphQL API reference, webhook specifications, third-party connector guides	Customer IT / Integration developers	Updated with each Release/Update
Tier 4 — Video Library	Recorded training sessions, feature walkthroughs, quick-tip videos (2–5 min)	All Authorised Users	New videos per Release; library curated quarterly
Tier 5 — Release Notes Archive	Detailed release notes for every Release/Update and Upgrade, with change classification	Super Users, Customer IT, Management	Published per Release/Update
Tier 6 — FAQ & Troubleshooting	Common issues, known limitations, workarounds, diagnostic steps	All Authorised Users / Super Users	Continuously updated based on ticket patterns

6.8.3 Documentation Standards

All Provider-authored documentation — whether published on the per-Client wiki or the central Knowledge Base — shall comply with the following quality standards:

- **Accuracy:** Documentation reflects the current production version of ProjectVIEW ERP. Outdated content is archived within five (5) Business Days of a superseding release.
- **Completeness:** Every activated module has corresponding Tier 1 and Tier 2 documentation. No feature is deployed without accompanying documentation.
- **Clarity:** Written in clear, jargon-minimised English. Screenshots are annotated with numbered callouts. Procedures use numbered steps with expected outcomes.
- **Searchability:** All articles are tagged with module names, role tags, and feature keywords. Full-text search and AI-powered semantic search are available across both the wiki and the central Knowledge Base.
- **Version Control:** Documentation is version-controlled in line with the application release it describes. Historical versions are retained for reference.
- **Personalisation:** Per-Client wiki content reflects the Customer's specific configuration, field labels, workflow names, and organisational terminology — not generic platform documentation.

6.9 Session Recording & AI Transcription

6.9.1 Recording Policy

All instructor-led training sessions delivered during the onboarding and implementation phase are recorded by the Provider as standard practice. Post Go-Live training sessions (§6.6) are also recorded unless the Customer explicitly opts out. Recordings are captured in high-definition audio/video format and stored on the Customer's dedicated wiki.

Recordings are organised by:

- Module (e.g., Project-Management, Procurement-Management).

- Role track (e.g., PM track, Finance track, Site Engineer track).
- Date and trainer, enabling rapid navigation to specific sessions.

6.9.2 AI Transcription & Content Generation

Each recorded session is processed through the Provider's AI transcription pipeline to generate:

(a) **Timestamped Transcript:** Full text of the session with speaker identification, searchable by keyword, topic, or module area. Users can click any transcript segment to jump to the corresponding video timestamp.

(b) **Key-Topic Index:** AI-extracted topic headings and subheadings that provide a structured table of contents for each session, enabling users to navigate directly to the subject matter relevant to their role.

(c) **Action Items & Follow-Ups:** Automatically extracted action items, questions raised, and follow-up commitments made during the session, linked to the relevant timestamp and assigned to the appropriate party.

(d) **Role-Specific Summaries:** AI-generated session summaries tailored to each role — for example, a Finance user viewing a Project-Management session receives a summary focused on the budget and cost implications discussed, rather than the full project-scheduling content.

(e) **Glossary Enrichment:** Customer-specific terminology, abbreviations, and project names mentioned during training are automatically extracted and added to the wiki's glossary, ensuring that AI-powered search understands the Customer's internal language.

6.9.3 Personalised Training Material Generation

The combination of recorded sessions, AI transcripts, and the Customer's configuration metadata enables the Provider to generate highly personalised training assets:

- **Per-Role Training Digest:** A consolidated document for each role (e.g., "Project Manager Onboarding Guide") that assembles relevant segments from multiple training sessions, supplemented with screenshots from the Customer's actual configuration.
- **Scenario-Based Quick Guides:** Step-by-step guides generated from real training demonstrations (e.g., "How to Process a Variation Order at [Customer Name]"), using the Customer's field names, approval workflows, and terminology.
- **New-Hire Onboarding Pack:** A curated selection of recorded sessions, transcripts, and quick-reference cards automatically assembled based on the new hire's assigned role, providing a self-service onboarding experience that mirrors the original implementation training.
- **Refresher Micro-Modules:** AI-generated short video clips (2–5 minutes) extracted from longer training sessions, focusing on single tasks or concepts, ideal for just-in-time refresher viewing.

This capability creates a unique, compounding knowledge asset for each Customer — every training interaction enriches the wiki, making subsequent onboarding faster, support-ticket volume lower, and user proficiency higher. No two Customers' training libraries are the same, because no two Customers' configurations, terminology, or operational contexts are the same.

6.10 AI-Assisted Learning

6.10.1 In-Application AI Guidance

The Provider leverages AI capabilities to provide intelligent, contextual learning experiences directly within the ProjectVIEW ERP interface:

(a) **Contextual Help Panel:** An AI-driven help panel that detects the user's current screen and task, and surfaces the most relevant knowledge-base articles, video clips, and step-by-step guides without the user needing to leave the application.

(b) **Guided Walkthroughs:** Interactive, step-by-step overlays that guide first-time users through complex workflows (e.g., creating a project, raising a purchase order, generating a report), highlighting each UI element in sequence.

(c) **Intelligent Search:** Natural-language search across the knowledge base and training library, powered by semantic understanding rather than keyword matching, enabling users to find answers using plain-language questions.

(d) **Proactive Suggestions:** AI-generated suggestions surfaced when the system detects common error patterns (e.g., incomplete form submissions, repeated navigation to incorrect screens), offering corrective guidance before a support ticket is raised.

6.10.2 Learning Analytics

The AI-assisted learning system generates anonymised usage analytics that inform the continuous improvement of training materials:

- Most-accessed help topics — indicating areas of user uncertainty or complexity.
- Search queries with no results — identifying documentation gaps.
- Guided walkthrough completion rates — highlighting workflows that may need simplification.
- Time-to-proficiency metrics by role and module — benchmarking the effectiveness of the training programme.

Learning analytics are included in the Quarterly Service Review (§3.9) and used to prioritise knowledge-base improvements in the CSI register (§4.10).

6.11 Customer Responsibilities

To ensure the effectiveness of the TKT framework, the Customer shall:

(a) Consent to the recording of instructor-led training sessions for the purpose of generating personalised training materials on the Customer's dedicated wiki; or provide written notice of opt-out prior to each session.

(b) Nominate a Training Coordinator who serves as the single point of contact for all training logistics, scheduling, and feedback.

(c) Ensure nominated attendees are released from operational duties for the duration of scheduled training sessions.

(d) Provide the Provider with timely notification of new-user activations, role changes, and organisational restructuring that may trigger training needs.

(e) Nominate and support Super User candidates for the T3 programme, including allocation of time for certification activities and internal training delivery.

(f) Distribute Provider-supplied training materials and release notes to relevant personnel within their organisation.

(g) Provide feedback on training quality, relevance, and effectiveness through the post-session evaluation forms supplied by the Provider.

(h) Maintain internal documentation (e.g., organisation-specific process guides, work instructions) that supplements the Provider's standard training materials.

(i) **Champion Designation:** Designate a minimum of two (2) DANAOS ProjectVIEW ERP Champions (Main and Deputy) in accordance with §6.6, and ensure Champion availability for Level 1 support duties and Provider communication from Go-Live onwards.

(j) **GAP Analysis Participation:** Review and provide written approval of the consolidated GAP Analysis Document (§6.4.6) within ten (10) Business Days of receipt; unreasonable delay in GAP Analysis approval may impact the implementation timeline.

6.12 Training Governance & Metrics

6.12.1 Training Metrics

The Provider shall track and report the following training metrics, included in the Quarterly Service Review (§3.9):

Metric	Definition	Target
Training Completion Rate	Percentage of nominated users who complete their assigned training tracks	≥ 90% within 30 days of nomination
Assessment Pass Rate	Percentage of trainees achieving the minimum competency score (70%)	≥ 85%
T3 Certification Rate	Percentage of nominated Super Users who achieve certification	≥ 90%
Time-to-Proficiency	Average elapsed days from user activation to independent operational use (no support escalation)	≤ 15 Business Days
Training Satisfaction Score	Average post-session evaluation rating (1–5 scale)	≥ 4.0
Training-Related Ticket Ratio	Percentage of support tickets attributable to training gaps (tagged “user error / training”)	< 10% of total ticket volume
Knowledge Base Utilisation	Average monthly unique knowledge-base sessions per Authorised User	≥ 2.0
Documentation Currency	Percentage of knowledge-base articles updated within 5 Business Days of a superseding release	100%
Champion Certification Rate	Percentage of designated Champion candidates who pass the Champion examination (§6.6.3)	≥ 100% (mandatory)
GAP Analysis Turnaround	Elapsed Business Days from training completion to approved GAP Analysis Document	≤ 15 Business Days

6.12.2 Training Review Cadence

The training programme is reviewed and updated on the following cadence:

- **Per Release:** Training impact assessment, material updates, and Super User briefing (§6.7.2).
- **Quarterly:** Training metrics review during QSR (§3.9); CSI actions logged for training improvements.
- **Annually:** Full TNA refresh; T3 recertification; curriculum review against the Platform roadmap and Customer’s organisational evolution.

6.13 Intellectual Property & Licensing

All training materials, knowledge-base content, video recordings, and documentation produced by the Provider remain the Intellectual Property of the Provider (§1.4 — Intellectual Property Rights).

The Customer is granted a non-exclusive, non-transferable licence to use such materials solely for the purpose of internal training and knowledge transfer in connection with the Customer's licensed use of ProjectVIEW ERP.

The Customer shall not:

- Reproduce, distribute, or make available any Provider training materials to third parties without the Provider's prior written consent.
- Use Provider training materials for the purpose of training personnel of any entity other than the Customer named in this Framework.
- Modify, adapt, or create derivative works from Provider training materials without the Provider's prior written consent.

Customer-authored internal documentation (e.g., organisation-specific process guides, work instructions) remains the Intellectual Property of the Customer.

6.14 Process Register

6.14.1 Process Registry

Ref	Process	Trigger	Handler	Approver	Expected Outcome	Cross-Ref
P-6.01	Training Needs Assessment	New Customer onboarding or annual review	Provider Training Lead	Customer PM + SDM	TNA document completed; Training Plan agreed	§2.4, §6.4.1
P-6.02	Implementation Training Delivery	Training Plan schedule	Provider Trainer	Customer PM	All ILT sessions delivered; attendance recorded; assessments completed	§6.4.2, §6.4.3
P-6.03	Training Completion Certification	All track sessions delivered + assessments passed	Provider Training Lead	Customer PM	Training Completion Certificate signed; UAT prerequisite met	§6.4.4, §5.8.1
P-6.04	T3 Candidate Nomination	Customer PM nomination	Customer PM	SDM	Super User candidates confirmed; T3 schedule agreed	§6.5.2

P-6.05	T3 Certification	Completion of T3 curriculum + assessment	Provider Training Lead	SDM	DANAOS Certified Super User credential issued	§6.5.3, §6.5.4
P-6.06	Release Training	New Release/Update or Upgrade deployed	Provider Training Lead	SDM	Updated materials published; Super User briefing delivered; users notified	§6.7.2, §4.7, §4.8
P-6.07	New User Onboarding Training	New Authorised User activated	Super User + Champion + Provider	Customer Training Coordinator	New user completes role-based training within 5 Business Days	§6.7.1, §3.7
P-6.08	Knowledge Base Update	Release deployment or ticket pattern analysis	Provider Documentation Team	Provider Training Lead	All affected articles updated within 5 Business Days	§6.8.1, §6.8.2
P-6.09	Training Gap Remediation	Support ticket pattern identifies training gap	Provider Training Lead	SDM	Targeted remedial training delivered within 10 Business Days	§6.7.1, §4.10
P-6.10	Annual TNA Refresh & Curriculum Review	12-month anniversary of last TNA	Provider Training Lead + Customer PM	SC	Updated TNA; revised Training Plan; T3/Champion recertification scheduled	§6.12.2
P-6.11	Session Recording & AI Transcription	Completion of any ILT session	Provider Training Lead	SDM	Recording published to Client wiki; AI transcript generated with topic index, action items, and role-specific summaries	§6.9
P-6.12	Client Wiki Content Curation	New release, training session, or quarterly cycle	Provider Documentation Team	Provider Training Lead	Wiki updated with new materials; personalised role manuals regenerated; FAQ enriched	§6.8

					from ticket patterns	
P-6.13	Champion Certification & Examination	Completion of Champion training programme	Provider Training Lead	SDM + Customer PM	Champion examination administered; DANAOS ProjectVIEW ERP Champion credential issued to passing candidates	§6.6.3
P-6.14	GAP Analysis Generation & Approval	Conclusion of implementation training phase	Provider Training Lead	Customer PM + SDM	Consolidated GAP Analysis Document delivered; Customer written approval obtained; remediation plan agreed	§6.4.6

6.14.2 RACI Matrix

R = Responsible | A = Accountable | C = Consulted | I = Informed

Process	Provider Training	Super User	Champion	Customer PM	SDM	Customer Users
P-6.01 TNA	R	—	C	R/A	A	I
P-6.02 Impl. Training	R	C	C	A	I	I
P-6.03 Training Cert.	R	I	I	A	I	I
P-6.04 T3 Nomination	C	—	—	R	A	I
P-6.05 T3 Certification	R	R	I	I	A	I
P-6.06 Release Training	R	C	C	I	A	I
P-6.07 New User Onboarding	C	R	R	A	I	I
P-6.08 KB Update	R	I	I	I	A	I
P-6.09 Gap Remediation	R	C	C	C	A	I
P-6.10 Annual TNA Refresh	R	C	C	R	A	C
P-6.11 Session Recording	R	I	I	I	A	I
P-6.12 Wiki Curation	R	C	C	I	A	I
P-6.13 Champion Cert.	R	I	R	A	A	I
P-6.14 GAP Analysis	R	C	R	A	A	I

6.14.3 Process Flow — Training & Knowledge Transfer Lifecycle

Stage	Activity	Role	Output
① Assess	Conduct Training Needs Assessment; map roles to modules; identify proficiency gaps	Provider Training Lead + Customer PM	TNA Document + Training Plan
② Design	Develop role-based curricula; prepare materials, exercises, and assessments; hand training plans to attendees	Provider Training Lead	Module Syllabi + Training Materials + Attendee Plans
③ Deliver	Execute ILT sessions (hands-on + online); record attendance per session and knowledge area; scramble schedule around client workload; collect qualms, configurations, and change requests	Provider Trainer + Champion	Session Records + Assessment Results + Feedback Register
④ Analyse	Consolidate registered qualms, configuration requirements, and change requests into GAP Analysis Document; present to Customer for written approval	Provider Training Lead	Approved GAP Analysis Document
⑤ Certify	Evaluate training completion; issue Training Completion Certificate; certify T3 Super Users; administer Champion examinations and issue Champion credentials	Provider Training Lead + Customer PM	Signed Certificate + T3 Credentials + Champion Credentials
⑥ Enable	Activate in-application guidance; publish knowledge base; release self-paced modules; publish recorded sessions and AI transcripts to Client wiki	Provider Documentation Team	Live Knowledge Base + Video Library + AI Transcripts
⑦ Sustain	Deliver release training; onboard new users; conduct remedial sessions per ticket patterns; Champions provide Level 1 support for intranet and extranet users	Provider Training + Super Users + Champions	Updated Materials + Onboarding Records + L1 Support Logs
⑧ Measure	Track training metrics; analyse learning analytics; identify improvement areas; review Champion effectiveness	Provider Training Lead + SDM	Training Metrics Report + Champion Performance Report
⑨ Improve	Refresh TNA annually; update curricula; recertify Super Users and Champions; log CSI actions	Provider Training Lead + SC	Revised Training Plan + CSI Actions

7 Chapter 7 — Data Protection & Privacy

7.1 Overview & Purpose

This chapter defines the data-protection and privacy obligations that govern the processing of Personal Data within and by the ProjectVIEW ERP Platform throughout the Subscription Term. It establishes the regulatory baseline, allocates Controller and Processor responsibilities, sets out the technical and organisational safeguards applied to Personal Data, and specifies the breach-notification and data-subject-rights procedures that both Parties shall follow.

The Provider operates under a **dual-jurisdiction compliance model**, maintaining concurrent alignment with:

(a) the European Union's General Data Protection Regulation (EU) 2016/679 ("GDPR"), including all adopted opinions and guidelines of the European Data Protection Board (EDPB); and

(b) (ii) the United Arab Emirates' Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data ("UAE PDPL") and its implementing regulations. Where a Customer operates in additional jurisdictions, supplementary data-processing addenda may be executed pursuant to §7.14.

DANAOS Projects Software Solutions LLC has established as a major objective the adoption of data-protection principles and the permeation of all daily business operations with an acute data-protection mentality. The Provider has consistently achieved compliance with the existing legal framework regarding data protection and has undertaken the actions derived from the repealing of Directive 95/46/EC, the establishment of GDPR (EU) 2016/679, and the enactment of the UAE PDPL.

This chapter, together with the Data Processing Agreement ("DPA") annexed to this Framework (§7.5), constitutes the **binding contractual framework** required under GDPR Article 28 and UAE PDPL Article 29 for the lawful processing of Personal Data by a Data Processor on behalf of a Data Controller.

7.2 Scope

This chapter applies to all Personal Data processed by the Provider in connection with the delivery of the Platform and related services, including but not limited to:

(a) **Customer Employee Data:** Personnel records, payroll data, timesheets, attendance, labour-productivity records, and identity information processed within modules PV_07 (HRMS–Payroll) and PV_A (Site Operations & Labour Productivity).

(b) **Customer Contacts & Counterparties:** Names, email addresses, telephone numbers, and commercial correspondence of subcontractors, suppliers, clients, and other third parties managed within modules PV_03, PV_04, PV_09, and PV_10.

(c) **End-User Credentials & Activity Logs:** User-account credentials, authentication tokens, session logs, IP addresses, browser fingerprints, and audit-trail data generated by the Platform's Users & Roles Management module (STY).

(d) **Support & Communication Data:** Personal Data contained within support tickets, WhatsApp Business group messages, training recordings, AI-transcribed session content, and any other communication exchanged through the Provider's omnichannel support model (§4.2).

(e) **Project & Financial Data:** Where project records, procurement data, accounting entries, or cost-control records contain identifiable natural-person information (e.g., named workers, consultant invoices), such data falls within scope.

(f) **Configuration & Master Data:** Master-data elements that reference identifiable individuals, including personnel registers, organisational hierarchies, approval matrices, and signatory authorities.

7.3 Regulatory Framework

The Provider's data-protection programme is built on the following regulatory instruments, standards, and guidance:

Ref	Instrument / Standard	Relevance
RF-01	GDPR (EU) 2016/679	Primary regulation for EEA-origin Personal Data; defines Controller/Processor obligations, data-subject rights, breach notification, and cross-border transfer rules.
RF-02	UAE Federal Decree-Law No. 45 of 2021 (PDPL)	Primary regulation for UAE-resident Personal Data; mirrors GDPR in substance with UAE-specific provisions on data localisation, Emirati data sovereignty, and UAE Data Office oversight.
RF-03	EDPB Guidelines & Adopted Opinions	Interpretive guidance on GDPR application, including SCCs, data transfers, legitimate interest, and DPIA methodology.
RF-04	EU Standard Contractual Clauses (SCCs) — Commission Implementing Decision (EU) 2021/914	Approved mechanism for Controller-to-Processor and Controller-to-Controller cross-border transfers of Personal Data outside the EEA.
RF-05	ISO/IEC 27701:2019	Extension to ISO 27001 establishing a Privacy Information Management System (PIMS); used as the organisational baseline for Processor privacy controls.
RF-06	ISO/IEC 27001:2022	Information Security Management System standard; foundational for the technical and organisational measures described in §7.8.
RF-07	NIST Privacy Framework 1.0	Voluntary framework used to align privacy risk assessment with enterprise risk management (§7.10).
RF-08	EU AI Act — Regulation (EU) 2024/1689	Regulates AI systems; relevant to the Provider's use of AI-assisted transcription, AIOps, and contextual in-app guidance (§5.3, §6.2).
RF-09	NIST AI Risk Management Framework (AI RMF 1.0)	Voluntary framework for identifying and mitigating risks in AI systems; applied alongside the EU AI Act for governance of AI components.

GDPR Full Text — EUR-Lex

UAE PDPL — Federal Decree-Law No. 45 of 2021

EU Standard Contractual Clauses (2021/914)

ISO/IEC 27701:2019 — PIMS

EU AI Act — Regulation (EU) 2024/1689

7.4 Roles & Responsibilities

7.4.1 Controller–Processor Allocation

By nature of its business operations, the Provider's role under applicable data-protection law is determined as follows:

(a) **Data Processor:** The Provider acts as a Data Processor regarding any Personal Data processing activity conducted on behalf of the Customer within the Platform. The Customer, as Data Controller, determines the purposes and means of processing; the Provider processes Personal Data solely on the Controller's documented instructions (§7.5).

(b) **Data Controller (limited scope):** The Provider acts as an independent Data Controller regarding processing activities conducted on its own employees' Personal Data (e.g., Provider staff assigned to the Customer's account), business-contact data for commercial relationship management, and anonymised/aggregated analytics that cannot be re-identified to any natural person.

(c) **Sub-Processor engagement:** The Provider shall not engage any Sub-Processor to process Personal Data without the prior specific or general written authorisation of the Controller. Where general authorisation is given, the Provider shall notify the Controller of any intended additions or replacements of Sub-Processors, giving the Controller the opportunity to object (§7.6).

7.4.2 Data Protection Officer

The Provider has designated a Data Protection Officer (DPO) in accordance with GDPR Articles 37–39 and UAE PDPL Article 10. The DPO is responsible for: (i) monitoring compliance with applicable data-protection legislation; (ii) advising on Data Protection Impact Assessments (§7.10); (iii) serving as the contact point for supervisory authorities; and (iv) handling data-subject inquiries.

Data subjects and Customer contacts may reach the DPO at: **admin@danaos-projects.com**

DANAOS employees may contact the DPO for any clarification regarding data-protection principles and request guidelines to perform data processing optimally and avoid potential infringement of the legislation.

7.4.3 RACI Matrix — Data Protection

Activity	Provider DPO	Provider Ops	Customer DPO / Privacy Lead	Customer PM	Champion	Supervisory Authority
Define processing purposes & lawful basis	C	I	A/R	I	I	I
Maintain Record of Processing Activities (RoPA)	A/R	C	R	I	I	I
Conduct Data Protection Impact Assessment	A/R	C	R	C	I	I
Implement technical & organisational measures	C	A/R	I	I	I	I

Respond to Data Subject Access Requests	C	R	A/R	I	I	I
Detect & classify Personal Data breach	C	A/R	I	I	I	I
Notify Controller of breach (≤72 hrs)	A/R	R	I	I	I	I
Notify Supervisory Authority (≤72 hrs)	C	I	A/R	I	I	R
Notify affected Data Subjects	C	I	A/R	C	C	I
Approve Sub-Processor engagements	C	R	A	I	I	I
Annual privacy audit & compliance review	A/R	C	R	I	I	I
Cross-border transfer impact assessment	A/R	C	R	I	I	I

Legend: R = Responsible (does the work) | A = Accountable (owns the outcome) | C = Consulted | I = Informed

7.5 Data Processing Agreement (DPA)

The Parties might execute a Data Processing Agreement ("DPA") which constitutes the **Article 28 contract** required under GDPR and the equivalent processor agreement required under UAE PDPL Article 29. The DPA shall, at a minimum, specify:

(a) **Subject matter & duration:** The DPA covers all Personal Data processing performed by the Provider in delivering the Platform throughout the Subscription Term plus any post-termination data-retention or return period (§7.13).

(b) **Nature & purpose of processing:** Hosting, storing, transmitting, backing-up, and computing Personal Data within the Customer's dedicated private sovereign environment for the purpose of enabling the Customer's construction project management, financial management, human-resources management, and procurement operations.

(c) **Categories of Data Subjects:** Customer employees, subcontractor personnel, supplier contacts, client contacts, site workers, and any other natural persons whose data the Customer inputs into the Platform.

(d) **Types of Personal Data:** Identification data (names, national IDs, passport numbers), contact data (email, phone, address), employment data (role, salary, attendance, leave), financial data (bank details for payroll), project-assignment data, access credentials, and audit-trail metadata.

(e) **Documented instructions:** The Provider shall process Personal Data only on documented instructions from the Controller, including with regard to transfers to third countries, unless required to do so by Union or Member State law to which the Provider is subject (GDPR Art. 28(3)(a)).

(f) **Confidentiality:** All Provider personnel authorised to process Personal Data have committed to confidentiality or are under an appropriate statutory obligation of confidentiality (GDPR Art. 28(3)(b)).

(g) **Deletion or return:** Upon termination, the Provider shall, at the Controller's election, delete or return all Personal Data and delete existing copies unless Union or Member State law requires storage (§7.13).

(h) **Audit rights:** The Provider shall make available to the Controller all information necessary to demonstrate compliance, and shall allow for and contribute to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller (§7.11).

7.6 Sub-Processor Management

The Provider engages a limited number of Sub-Processors to deliver components of the Platform and associated services. The following Sub-Processor governance applies:

(a) **Authorisation model:** The Customer grants general authorisation for Sub-Processor engagement subject to the Provider's obligation to: (i) maintain a current register of Sub-Processors; (ii) notify the Customer of any intended additions or replacements no fewer than thirty (30) calendar days before the new Sub-Processor commences processing; and (iii) provide sufficient information to enable the Customer to exercise its right of objection.

(b) **Right of objection:** If the Customer reasonably objects to a new Sub-Processor on legitimate data-protection grounds, the Provider shall either: (i) refrain from engaging the Sub-Processor and offer an alternative; or (ii) if no alternative is feasible, either Party may terminate the affected services without penalty, subject to a reasonable wind-down period.

(c) **Flow-down obligations:** The Provider shall impose on each Sub-Processor, by way of contract, the same data-protection obligations as set out in the DPA (§7.5), in particular providing sufficient guarantees to implement appropriate technical and organisational measures such that the processing meets GDPR and UAE PDPL requirements.

(d) **Liability:** The Provider remains fully liable to the Customer for the performance of the Sub-Processor's obligations under the DPA. Where a Sub-Processor fails to fulfil its data-protection obligations, the Provider shall be liable for the acts and omissions of the Sub-Processor as if they were the Provider's own acts or omissions.

7.6.1 Sub-Processor Register

The following table lists the Sub-Processors engaged by the Provider as at the Effective Date. The register is maintained and updated pursuant to §7.6(a).

Sub-Processor	Processing Activity	Location	Safeguard
Microsoft Azure	IaaS hosting of Customer's dedicated private sovereign environment (compute, storage, networking)	Region selected per Customer DPA (default: UAE North / West Europe)	EU SCCs + Microsoft DPA
Microsoft 365	Email communication, collaboration tools used by Provider operations team	EEA / UAE (per licence configuration)	EU SCCs + Microsoft DPA
WhatsApp (Meta Platforms)	Expedient informal communication via shared WhatsApp Business groups (§4.2)	EEA (Meta Ireland)	EU SCCs + Meta DPA
AI Transcription Service	Processing of recorded training-session audio for AI-generated transcripts (§6.2)	EEA / UAE (per Provider configuration)	EU SCCs + Provider-assessed DPA

Note: *The Customer's Platform data resides in a dedicated private sovereign environment; no customer data is co-mingled across tenants. The hosting region is selected per the Customer's DPA and may be restricted to a specific Azure region to satisfy data-localisation requirements under the UAE PDPL or other applicable law.*

7.7 Data Protection Principles

Any Personal Data processing activity conducted by the Provider, either as Data Controller or Data Processor, shall be characterised by the following principles, aligned with GDPR Article 5 and UAE PDPL Article 4:

Principle	GDPR Art.	UAE PDPL Art.	Provider Implementation
Lawfulness, fairness & transparency	5(1)(a)	4(1)	Processing is based on at least one lawful basis (Art. 6); data subjects are informed in a concise, transparent, intelligible manner via the Customer's privacy notices; Provider assists Customer in maintaining transparency.
Purpose limitation	5(1)(b)	4(2)	Personal Data is processed exclusively for the documented purposes specified in the DPA (§7.5). The Provider does not process Customer data for its own purposes (e.g., analytics, marketing, profiling) unless explicitly authorised in writing.
Data minimisation	5(1)(c)	4(3)	The Platform's module design collects only data elements required for the activated business functions. Master-data checklists (§6.4.3) define the minimum viable dataset per module.
Accuracy	5(1)(d)	4(4)	The Platform provides data-validation rules, duplicate-detection, and referential-integrity checks. The Customer retains responsibility for the accuracy of input data; the Provider provides tools to maintain it.
Storage limitation	5(1)(e)	4(5)	Data-retention policies (§7.12) ensure Personal Data is deleted or anonymised when no longer necessary. Automated retention-period enforcement is configurable per Customer.
Integrity & confidentiality	5(1)(f)	4(6)	Technical and organisational measures (§7.8) ensure Personal Data is protected against unauthorised or unlawful processing, accidental loss, destruction, or damage.
Accountability	5(2)	4(7)	The Provider maintains Records of Processing Activities (RoPA), conducts DPIAs where required, and makes compliance evidence available for audit (§7.11).

7.8 Technical & Organisational Measures (TOMs)

The Provider implements and maintains the following technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with GDPR Article 32 and UAE PDPL Article 28. These measures are aligned with ISO/IEC 27001:2022 and ISO/IEC 27701:2019 control objectives. The Provider's Information Security Management System (ISMS) is maintained by the IT Department.

7.8.1 Access Control & Authentication

(a) **Password complexity:** Minimum length, character-class requirements, and prohibition of common/breached passwords enforced at the application layer.

(b) **Password expiration:** Configurable password-rotation policy; default rotation period aligned with NIST SP 800-63B guidance.

(c) **Failed-authentication lockout:** Account lockout after a configurable number of consecutive failed attempts; lockout duration escalates with repeated violations.

(d) **Password history:** The system prevents reuse of the last N passwords (configurable per Customer policy).

(e) **Multi-factor authentication (MFA):** Second-factor authentication is supported and recommended for all administrative and privileged accounts. MFA methods include TOTP (time-based one-time password), push notification, and FIDO2 hardware keys.

(f) **Single Sign-On (SSO):** The Platform supports integration with enterprise identity providers via SAML 2.0 and OpenID Connect, enabling centralised credential management and reducing the attack surface associated with password proliferation.

(g) **Session management:** Away-from-keyboard auto-lock mechanism; configurable idle-session timeout; session invalidation on password change or account suspension.

(h) **Role-based access control (RBAC):** The Users & Roles Management module (STY) enforces granular, role-based access control at the module, function, field, and record level. Segregation of duties is enforced through conflicting-role detection.

(i) **Restricted remote access:** Remote administrative access to the Provider's infrastructure is restricted to authorised personnel via encrypted VPN tunnels with MFA; all remote sessions are logged and auditable.

7.8.2 Encryption

(a) **Data in transit:** All client–server communication is encrypted using TLS 1.2 or higher. End-to-end data-transmission encryption is enforced across all Platform interfaces, APIs, and integration endpoints.

(b) **Data at rest:** Transparent Data Encryption (TDE) is applied to all database instances. Database backups are encrypted using AES-256 encryption. Encryption keys are managed through the cloud provider's Key Management Service with customer-managed key (CMK) options available.

(c) **Key management:** Encryption keys are rotated according to a defined schedule. Key-management procedures follow ISO 27001 Annex A.10 controls. Hardware Security Modules (HSMs) are used for root key protection where available.

7.8.3 Database Security

(a) **Database connections:** Connections to database instances are controlled, monitored, and restricted to authorised application-layer services and designated DBA personnel only.

(b) **Default accounts:** Default system accounts are secured by the DBA; all default passwords are changed immediately upon provisioning; unnecessary default accounts are disabled.

(c) **Minimum privilege:** Database user accounts are provisioned with minimum permissions and roles necessary for their function. System privileges are removed unless explicitly required and approved.

(d) **Audit logging:** Database audit logging captures all DDL operations, privileged-user activity, failed authentication attempts, and data-export operations. Logs are retained for a minimum of twelve (12) months and are tamper-evident.

(e) **DBA remote access:** Remote database administration is restricted to named individuals via encrypted channels with multi-factor authentication. All DBA sessions are logged with full command-level audit trail.

7.8.4 Network Security

(a) **Perimeter defence:** Next-generation firewalls, Web Application Firewalls (WAF), and DDoS-protection services guard the platform perimeter. Network segmentation isolates the Customer's private sovereign environment from other Provider infrastructure.

(b) **Intrusion detection & monitoring:** Cloud-native SIEM and network-monitoring tools provide real-time alerting on anomalous traffic patterns, port-scan attempts, and lateral-movement indicators.

(c) **Vulnerability management:** Regular vulnerability scans and annual penetration tests are conducted. Critical and high-severity vulnerabilities are remediated within the timeframes specified in §3.5 (Incident Priority Classification).

7.8.5 Organisational Measures

(a) **Confidentiality agreements:** All Provider personnel authorised to process Personal Data have signed confidentiality/non-disclosure agreements and are under an appropriate statutory obligation of confidentiality.

(b) **Training & awareness:** Provider personnel receive annual data-protection training covering GDPR, UAE PDPL, breach reporting, social engineering, and secure-coding practices.

(c) **Clean desk & clear screen:** Clean-desk and clear-screen policies are enforced in all Provider facilities to prevent inadvertent exposure of Personal Data.

(d) **Asset-use policy:** All hardware and software assets are used exclusively for business purposes and the implementation of tasks respective to each employee's job description.

7.9 Data Subject Rights

The Provider recognises the rights of Data Subjects as defined in GDPR Chapter III (Articles 12–23) and UAE PDPL Articles 12–18, and shall assist the Customer in fulfilling its obligation to respond to Data Subject requests in accordance with GDPR Article 28(3)(e) and UAE PDPL Article 29. The Provider shall:

(a) Promptly notify the Customer upon receipt of a Data Subject request related to Customer data, without responding to the Data Subject directly unless instructed by the Customer.

(b) Provide the Customer with the technical capability to extract, rectify, restrict, port, or delete Personal Data through Platform functionality or, where not available through the UI, through Provider-executed database operations within the timeframes required by law.

(c) Maintain audit trails of all Data Subject request fulfilment actions for a minimum of twenty-four (24) months.

7.9.1 Rights Fulfilment Matrix

Right	GDPR Art.	UAE PDPL Art.	Platform Capability	Response SLA
Right of access	15	13	Data-export function generates structured report of all Personal Data associated with a Data Subject's identity	≤30 calendar days

Right to rectification	16	14	In-app record editing with full audit trail; batch-correction support for bulk updates	≤30 calendar days
Right to erasure ('right to be forgotten')	17	15	Erasure workflow anonymises or deletes all instances of a Data Subject's Personal Data across modules, backups, and logs (subject to legal-hold exceptions)	≤30 calendar days
Right to restriction of processing	18	16	Record-level processing-restriction flag; restricted data remains stored but is excluded from active processing, reporting, and API responses	≤72 hours (flag)
Right to data portability	20	17	Machine-readable export in CSV, JSON, and XML formats; API-based extraction available	≤30 calendar days
Right to object	21	18	Processing-objection flag triggers review; Provider ceases processing pending assessment of compelling legitimate grounds	≤72 hours (flag)

Legal-hold override: Where erasure or restriction conflicts with a legal obligation (e.g., statutory record-retention, pending litigation, regulatory investigation), the Provider shall inform the Customer and the Data Subject of the legal basis for continued processing, and shall restrict processing to the minimum necessary for compliance.

7.10 Data Protection Impact Assessment (DPIA)

Where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons, the Customer (as Controller) shall carry out a Data Protection Impact Assessment in accordance with GDPR Article 35 and UAE PDPL Article 23. The Provider shall:

(a) Provide the Customer with all information necessary to conduct the DPIA, including documentation of the Platform's data flows, retention policies, access-control model, and cross-border transfer mechanisms.

(b) Assist the Customer in conducting the DPIA where requested, including by providing a pre-completed DPIA template covering the standard processing operations performed by the Platform.

(c) Notify the Customer if, in the Provider's opinion, a new feature, module activation, integration, or change in processing operations triggers the need for a new or updated DPIA.

(d) **AI-specific DPIA:** Where the Platform's AI components (e.g., AI-assisted transcription, AIOps anomaly detection, contextual in-app guidance) process Personal Data, a supplementary AI-specific DPIA shall be conducted addressing algorithmic bias, automated decision-making transparency, data-minimisation in training sets, and the rights of Data Subjects under GDPR Article 22 (automated individual decision-making). This assessment shall also consider obligations under the EU AI Act (Regulation (EU) 2024/1689) and the NIST AI Risk Management Framework.

7.11 Audit & Compliance

7.11.1 Provider Obligations

The Provider shall:

(d) Maintain a Record of Processing Activities (RoPA) in accordance with GDPR Article 30, covering all processing operations performed on behalf of the Customer.

(e) Make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in GDPR Article 28 and UAE PDPL Article 29.

(f) Allow for and contribute to audits, including inspections, conducted by the Customer or an auditor mandated by the Customer, subject to: (i) reasonable advance notice of not less than thirty (30) calendar days; (ii) audit scope limited to the processing activities covered by the DPA; (iii) the auditor's execution of a non-disclosure agreement acceptable to the Provider; and (iv) audits being conducted during normal business hours in a manner that minimises disruption.

(g) Immediately inform the Customer if, in the Provider's opinion, an instruction from the Customer infringes GDPR, UAE PDPL, or other applicable data-protection law (GDPR Art. 28(3)(h)).

7.11.2 Audit Frequency & Scope

The following audit schedule applies:

Audit Type	Frequency	Scope	Output
Provider self-assessment	Quarterly	RoPA completeness, TOM effectiveness, Sub-Processor compliance, incident log review	Internal compliance report shared with Customer DPO
Customer-initiated audit	Annually (or upon material breach)	Full DPA compliance, technical controls inspection, personnel-training records, breach-response drill	Audit findings report with remediation timeline
Third-party certification audit	Annually	ISO 27001:2022 / ISO 27701:2019 scope — ISMS and PIMS controls	Certificate and Statement of Applicability
Regulatory authority audit	As required	Full regulatory scope as directed by the supervisory authority	Cooperation and documentation provision per GDPR Art. 58

7.12 Data Retention & Destruction

Personal Data shall not be retained for longer than is necessary for the purposes for which it was collected. The following retention framework applies:

(a) **Active processing:** Personal Data is actively processed for the duration of the Subscription Term and any post-termination wind-down period agreed under the DPA.

(b) **Retention periods:** Where specific retention periods are mandated by applicable law (e.g., labour-law record retention, tax-authority requirements, regulatory preservation orders), the Provider shall retain the minimum necessary data for the prescribed period, clearly segregated and access-restricted.

(c) **Automated enforcement:** The Platform supports configurable data-retention policies that automatically flag, archive, or purge records that exceed their defined retention period. The Customer defines the retention rules; the Provider implements the technical enforcement.

(d) **Secure destruction:** When Personal Data is deleted, the Provider shall ensure secure destruction through: (i) cryptographic erasure for encrypted data (rendering the encryption

key irrecoverable); (ii) multi-pass overwrite for unencrypted media; and (iii) deletion confirmation certificates provided to the Customer upon request.

(e) **Backup retention:** Backup copies containing Personal Data are subject to the same retention and destruction policies. The Provider shall ensure that deleted Personal Data is purged from all backup cycles within ninety (90) calendar days of the deletion instruction, unless a shorter period is specified in the DPA.

NIST SP 800-88 Rev. 1 — Guidelines for Media Sanitization

7.13 Data Return & Portability on Termination

Upon termination or expiry of the Framework, the following data-return and portability provisions apply:

(a) **Data-return period:** The Customer shall have a period of sixty (60) calendar days from the effective date of termination to request the return of all Personal Data and Customer Data in a structured, commonly used, machine-readable format (CSV, JSON, XML, or SQL dump).

(b) **Format options:** The Provider shall offer data export in at least three machine-readable formats. The export shall include: (i) all transactional data across activated modules; (ii) master-data registers; (iii) document attachments; (iv) audit logs; and (v) configuration metadata sufficient to reconstruct the Customer's operational setup in a successor system.

(c) **Deletion after return:** Upon confirmation that the Customer has received and verified the exported data, or upon expiry of the sixty (60) day data-return period (whichever is earlier), the Provider shall securely delete all Personal Data from all systems, including production databases, staging environments, backups, and disaster-recovery replicas.

(d) **Deletion certificate:** The Provider shall issue a written certificate of deletion within thirty (30) calendar days of completing the secure-destruction process, confirming that all Personal Data has been irreversibly destroyed from all Provider-controlled systems and media.

(e) **Residual obligations:** Data-protection obligations under this chapter survive termination with respect to any Personal Data retained by the Provider pursuant to a legal obligation, until such data is securely destroyed.

7.14 Cross-Border Data Transfers

Where the processing of Personal Data involves or may involve the transfer of Personal Data to a third country or international organisation, the following provisions apply:

(a) **EEA-origin data:** Transfers of Personal Data originating from the European Economic Area to countries not covered by an adequacy decision under GDPR Article 45 shall be governed by the EU Standard Contractual Clauses (SCCs) adopted under Commission Implementing Decision (EU) 2021/914, supplemented by a Transfer Impact Assessment (TIA) where required by EDPB Recommendations 01/2020.

(b) **UAE-origin data:** Transfers of Personal Data originating from the UAE to countries outside the UAE shall comply with UAE PDPL Article 22 (cross-border transfer provisions), including any data-localisation requirements imposed by the UAE Data Office or sector-specific regulators.

(c) **Data-localisation options:** The Provider's dedicated private sovereign environment model enables the Customer to select the geographic region (Azure Region) in which all Customer Data resides and is processed. Where the Customer requires data to remain within a specific jurisdiction (e.g., UAE for government contracts, EEA for EU-regulated entities), the Provider shall ensure that no data leaves the designated region, including for backup and disaster-recovery purposes.

(d) **Transfer Impact Assessment:** Prior to initiating any new cross-border transfer mechanism, the Provider shall conduct and document a Transfer Impact Assessment evaluating: (i) the legal framework of the recipient country; (ii) the supplementary measures in place; and (iii) the practical enforceability of Data Subject rights in the recipient jurisdiction.

7.15 Personal Data Breach Management

7.15.1 Breach Detection & Classification

The Provider has established procedures, governed by the IT Department, to detect, classify, and respond to Personal Data breaches. The Provider's SIEM and AIOps tooling provides automated anomaly detection; all alerts classified as potential Personal Data breaches are immediately escalated to the DPO.

Breaches are classified by severity:

Severity	Criteria	Notification Timeline	Example
Critical	High risk to rights and freedoms of Data Subjects; large-scale breach; sensitive data categories affected	Provider → Controller: ≤24 hrs Controller → Authority: ≤72 hrs Controller → Data Subjects: without undue delay	Database exfiltration; ransomware encrypting HR/payroll data; credential compromise of admin accounts
High	Material risk to rights and freedoms; limited-scale breach; standard Personal Data categories	Provider → Controller: ≤48 hrs Controller → Authority: ≤72 hrs	Unauthorised access to project-contact data; email misdirection containing Personal Data
Medium	Low risk; containment achieved quickly; limited data exposure	Provider → Controller: ≤72 hrs Controller → Authority: at Controller's discretion	Failed brute-force attempt contained by lockout; exposure of non-sensitive metadata
Low	Negligible risk; no actual exposure of Personal Data	Provider → Controller: monthly summary report	Anomalous login pattern with no data access; policy-violation alert triggered by false positive

7.15.2 Breach Notification Procedure

The Provider shall notify the Customer (as Controller) of any confirmed or suspected Personal Data breach as follows:

(a) **Initial notification:** Within the timeframes specified in §7.15.1, the Provider shall notify the Customer's designated DPO/privacy lead via the primary communication channel (email to designated address, followed by telephone confirmation for Critical and High severity breaches). The initial notification shall include: (i) nature of the breach; (ii) categories and approximate number of Data Subjects affected; (iii) categories and approximate number of records concerned; (iv) likely consequences; and (v) measures taken or proposed to mitigate adverse effects.

(b) **Follow-up reporting:** Where the full details are not available at the time of the initial notification, the Provider shall provide information in phases without undue delay as it becomes available (GDPR Art. 33(4)).

(c) **Root-cause analysis:** The Provider shall deliver a full root-cause analysis report to the Customer within fifteen (15) business days of breach containment, including: timeline of events, affected systems and data, root cause, containment actions, remediation measures, and recommendations to prevent recurrence.

(d) **Regulatory cooperation:** The Provider shall assist the Customer in: (i) notifying the competent supervisory authority (GDPR Art. 33, UAE PDPL Art. 28); and (ii) communicating the breach to affected Data Subjects where required (GDPR Art. 34). The Provider shall not communicate directly with the supervisory authority or Data Subjects regarding Customer data without the Customer's prior written consent, unless required by law.

7.15.3 Breach Response Drill

The Provider and Customer shall conduct a joint Personal Data breach-response drill at least **annually**, simulating a Critical-severity breach scenario. The drill shall test: (i) detection-to-notification timelines; (ii) communication-channel effectiveness; (iii) containment-procedure execution; and (iv) regulatory-notification readiness. Findings from each drill shall be documented and incorporated into process improvements.

7.16 AI-Specific Data Protection

The Provider's use of artificial-intelligence components within the Platform (including AI-assisted transcription, AIOps, predictive analytics, and contextual in-app guidance) is subject to the following data-protection controls, aligned with the EU AI Act (Regulation (EU) 2024/1689) and the NIST AI RMF:

(a) **No cross-tenant training:** Customer data is never used to train AI models that serve other customers or improve the Provider's general-purpose AI capabilities. Each Customer's AI-generated outputs (e.g., transcription models, predictive analytics) are trained and scoped exclusively to that Customer's data within their dedicated sovereign environment.

(b) **Data minimisation in AI:** AI components process the minimum Personal Data necessary to deliver their function. Where possible, data is pseudonymised or anonymised before AI processing.

(c) **Automated decision-making:** The Platform does not make decisions based solely on automated processing that produce legal effects or similarly significant effects on Data Subjects (GDPR Art. 22) unless: (i) the Customer explicitly configures such processing; (ii) the Customer ensures a lawful basis (consent, contract necessity, or Member State law); and (iii) human review is available.

(d) **AI transparency:** The Provider documents the purpose, data inputs, logic, and output scope of each AI component in the Platform's technical documentation. This documentation is available to the Customer for DPIA purposes (§7.10) and regulatory inspection.

(e) **Bias monitoring:** Where AI components process Personal Data that includes special categories (e.g., ethnicity, nationality in HRMS modules), the Provider implements bias-monitoring checks and reports findings to the Customer as part of the quarterly self-assessment (§7.11.2).

7.17 Process Register

The following table enumerates the contractual and operational processes governed by this chapter. Each process is assigned a unique identifier, trigger condition, responsible handler, approver, expected outcome, and cross-reference to the governing section.

Proc-ID	Process Name	Trigger	Handler	Approver	Outcome	Section
P-7.01	DPA Execution	Agreement signing or renewal	Provider DPO	Customer DPO	Signed DPA annexing Art. 28 obligations	§7.5
P-7.02	Sub-Processor Notification	New or replacement Sub-Processor identified	Provider Ops	Customer DPO	30-day advance notice with objection window	§7.6
P-7.03	Sub-Processor Objection Resolution	Customer objects to Sub-Processor	Provider DPO	Both Parties	Alternative Sub-Processor or service termination option	§7.6(b)
P-7.04	Data Subject Access Request (DSAR)	Data Subject submits request to Controller	Customer DPO	Customer DPO	Structured report delivered within 30 days	§7.9
P-7.05	Data Subject Erasure Request	Data Subject exercises right to erasure	Provider Ops + Customer DPO	Customer DPO	Anonymisation/deletion with legal-hold check	§7.9
P-7.06	DPIA Initiation	New module, feature, or processing change triggers high-risk threshold	Provider DPO	Customer DPO	Completed DPIA with risk register	§7.10
P-7.07	AI-Specific DPIA	AI component processes Personal Data	Provider DPO	Customer DPO	AI DPIA covering bias, transparency, Art. 22	§7.10
P-7.08	Breach Detection	SIEM/AIOps alert or manual detection of suspected breach	Provider Ops	Provider DPO	Classified breach record; containment initiated	§7.15.1
P-7.09	Breach Notification (Controller)	Confirmed/suspected breach classified ≥ Medium	Provider DPO	Provider DPO	Notification to Customer within SLA timeline	§7.15.2
P-7.10	Breach Notification (Authority)	Controller determines authority notification required	Customer DPO	Customer DPO	≤72-hour notification to supervisory authority	§7.15.2
P-7.11	Root-Cause Analysis	Breach containment completed	Provider Ops	Provider DPO + Customer DPO	RCA report within 15 business days	§7.15.2(c)

P-7.12	Breach Response Drill	Annual schedule or ad-hoc trigger	Provider DPO + Customer DPO	Both Parties	Drill report with improvement actions	§7.15.3
P-7.13	Data Return on Termination	Agreement termination/expiry	Provider Ops	Customer PM	Data exported in machine-readable format within 60 days	§7.13
P-7.14	Secure Data Destruction	Data-return period expires or deletion requested	Provider Ops	Provider DPO	Deletion certificate issued within 30 days	§7.12
P-7.15	Cross-Border Transfer Assessment	New transfer mechanism or destination identified	Provider DPO	Customer DPO	Documented TIA with supplementary measures	§7.14
P-7.16	Privacy Audit (Internal)	Quarterly schedule	Provider DPO	Provider DPO	Compliance report shared with Customer	§7.11.2
P-7.17	Privacy Audit (Customer)	Annual schedule or material breach trigger	Customer Auditor	Customer DPO	Findings report with remediation timeline	§7.11.2
P-7.18	Retention Policy Review	Annual schedule or regulatory change	Provider DPO + Customer DPO	Customer DPO	Updated retention schedule and automated enforcement rules	§7.12

7.18 Process-Flow Schematic

The following diagram illustrates the data-protection lifecycle from DPA execution through ongoing compliance monitoring, breach response, and data return on termination.

Feedback loop: Stage ⑨ (Data Return/Destruction) feeds back into Stage ② (RoPA) for record-keeping of destruction activities and Stage ⑧ (Audit) for post-termination compliance verification. Stages ④–⑦ operate continuously throughout the Subscription Term with quarterly self-assessment checkpoints (§7.11.2).

8 Information Security & Confidentiality

8.1 8.1 Overview & Purpose

This chapter defines the information-security and confidentiality obligations governing the Provider's delivery of the ProjectVIEW ERP Platform. It establishes the security architecture, authentication controls, encryption standards, network defences, vulnerability management procedures, and confidentiality provisions that protect Customer Data, Platform integrity, and the Provider's proprietary intellectual property throughout the Subscription Term.

The Provider's Information Security Management System (ISMS) is maintained by the IT Department and is aligned with **ISO/IEC 27001:2022**. This chapter addresses the **technical security controls** that complement the privacy-specific measures described in Chapter 7 (Data Protection & Privacy) and the operational-support security measures described in Chapter 4 (Service Support & Operations).

DANAOS Web Enterprise incorporates security mechanisms at every layer of the application stack — from the presentation tier (web browser) through the application tier (application server) to the data tier (database server) — ensuring that confidentiality, integrity, and availability (the C.I.A. triad) are enforced end-to-end within each Customer's dedicated private sovereign environment.

8.2 Scope

This chapter covers:

(a) **Platform application security:** Authentication, authorisation, session management, input validation, and secure-coding practices embedded within the DANAOS Web Framework.

(b) **Infrastructure security:** Network segmentation, firewall configuration, intrusion detection, DDoS protection, and Web Application Firewall (WAF) controls applied to each Customer's Azure-hosted sovereign environment.

(c) **Database security:** Access control, encryption (at rest and in transit), audit logging, privilege management, and connection monitoring for SQL Server database instances.

(d) **Operational security:** Vulnerability management, penetration testing, patch management, change-tracking, and security-incident response (non-personal-data incidents; Personal Data breaches are governed by §7.15).

(e) **Source-code security:** Intellectual-property protection, secure-development lifecycle, Git-based version control, and code-review practices governing the Provider's proprietary codebase.

(f) **Confidentiality obligations:** Mutual confidentiality undertakings, information classification, disclosure restrictions, and survival provisions.

8.3 Security Standards & Frameworks

The Provider's security programme is built on the following standards, frameworks, and guidance:

Ref	Standard / Framework	Application

SF-01	ISO/IEC 27001:2022	Foundation for the ISMS; defines the management system, risk assessment methodology, Statement of Applicability (SoA), and continuous improvement cycle.
SF-02	ISO/IEC 27002:2022	Reference control set; provides implementation guidance for the Annex A controls selected in the SoA.
SF-03	NIST Cybersecurity Framework (CSF) 2.0	Used to structure the Provider's security functions: Identify, Protect, Detect, Respond, Recover, and Govern.
SF-04	OWASP Top 10 (2021)	Baseline for web-application security; integrated into the Provider's secure-development lifecycle and penetration-testing scope.
SF-05	OWASP Application Security Verification Standard (ASVS) 4.0	Used for Level 2 verification of authentication, session management, access control, and input-validation controls.
SF-06	CIS Microsoft Azure Foundations Benchmark v2.1	Hardening baseline for Azure infrastructure; applied to NSGs, storage accounts, key vaults, and identity configuration.
SF-07	CIS Microsoft SQL Server 2022 Benchmark	Hardening baseline for SQL Server database instances; applied to authentication, authorisation, auditing, and encryption settings.
SF-08	NIST SP 800-63B	Digital identity guideline for authentication assurance levels; informs password-policy and MFA requirements.
SF-09	Microsoft Azure Well-Architected Framework — Security Pillar	Cloud-native security design principles: zero-trust, defence-in-depth, and least-privilege.

ISO/IEC 27001:2022

NIST CSF 2.0

OWASP Top 10 (2021)

CIS Azure Foundations Benchmark

NIST SP 800-63B

Azure Well-Architected Framework

8.4 Application Security

DANAOS ProjectVIEW ERP platform incorporates the following security mechanisms at the application layer to ensure system confidentiality and integrity. These controls are enforced for every Customer instance and are configurable by the Customer's system administrators through the STY (Users & Roles Management) module.

8.4.1 Authentication Controls

Control	Description	Configurable	Reference
Password complexity	Inherits Microsoft LDAP authentication password-value requirements. Enforces minimum character-class diversity (uppercase, lowercase, numeric, special characters) and prohibits common/breached passwords.	Yes — complexity rules defined by Customer admin	NIST SP 800-63B §5.1.1

Password expiration	System administrators define a mandatory rotation period after which users must alter their password. Default: 90 days; configurable per Customer policy.	Yes — rotation period in days	ISO 27002 §8.5
Failed-authentication lockout	System administrators define the maximum number of consecutive failed login attempts per account, after which the account is locked for a configurable duration.	Yes — attempt threshold + lockout duration	OWASP ASVS 2.2.1
Password history	Prevents users from reusing any password value used in the past. System administrators configure the number of historical passwords retained.	Yes — history depth (N passwords)	NIST SP 800-63B
Minimum password length	System administrators define the minimum length of the password value users may utilise.	Yes — minimum characters	NIST SP 800-63B §5.1.1
Idle-session lock	System administrators define the number of minutes of inactivity after which the application demands re-authentication (away-from-keyboard lock screen).	Yes — timeout in minutes	ISO 27002 §8.1
Multi-factor authentication (MFA)	Incorporated Google Authenticator OTP (TOTP) authentication mandated when login requests originate outside the intranet. System administrators define network/IP ranges considered ‘external’ that trigger MFA.	Yes — network/IP ranges, MFA method	NIST SP 800-63B AAL2
Single Sign-On (SSO)	Supports SSO via Active Directory (SAML 2.0, OpenID Connect). Enables centralised credential management and reduces password proliferation.	Yes — IdP integration configuration	ISO 27002 §8.5

8.4.2 Authorisation & Access Control

The Platform’s **Users & Roles Management module (STY)** enforces granular, role-based access control (RBAC) at multiple levels:

(a) **Module level:** Users are granted or denied access to entire modules (e.g., PV_07 HRMS–Payroll, PV_08 Accounting) based on their role assignment.

(b) **Function level:** Within a module, individual functions (e.g., create purchase order, approve invoice, view salary) are independently permissioned.

(c) **Field level:** Sensitive fields within a record (e.g., salary amount, bank account, national ID) can be hidden or read-only for specific roles.

(d) **Record level:** Row-level security restricts visibility based on organisational hierarchy (e.g., project managers see only their assigned projects; regional managers see their region).

(e) **Segregation of duties:** Conflicting-role detection prevents a single user from holding roles that create separation-of-duties conflicts (e.g., requisition creator and approval authority). The STY module alerts administrators to detected conflicts and enforces policy-based restrictions.

(f) **Unique user IDs:** Every user account is assigned a unique identifier. Shared/generic accounts are prohibited. All actions are traceable to an individual user through the audit trail.

(g) **Restricted remote access:** System administrators control remote access per user via the administrator console; access can be allowed or revoked at any time.

8.4.3 Session Security

(a) **Session tokens:** Cryptographically random session tokens are generated upon authentication. Tokens are bound to the user's IP address and user-agent string to prevent session hijacking.

(b) **Session invalidation:** Sessions are invalidated upon: password change, account suspension, explicit logout, or idle-timeout expiry.

(c) **Concurrent-session control:** Configurable limits on concurrent active sessions per user account. Default: single active session per user (last-login-wins policy).

8.4.4 Input Validation & Output Encoding

(a) **Server-side validation:** All user-supplied input is validated on the server side using whitelist-based validation. Client-side validation is treated as a usability enhancement only, never as a security control.

(b) **Parameterised queries:** All database interactions use parameterised queries (prepared statements) to prevent SQL injection. Dynamic SQL construction from user input is prohibited by the Provider's secure-coding standard.

(c) **Output encoding:** All data rendered to the browser is contextually encoded (HTML, JavaScript, URL, CSS encoding as appropriate) to prevent cross-site scripting (XSS).

(d) **Content Security Policy (CSP):** HTTP response headers include a strict Content Security Policy to mitigate XSS and data-injection attacks.

8.5 Infrastructure Security

Each Customer's ProjectVIEW ERP instance is deployed within a **dedicated private sovereign environment** on Microsoft Azure. The infrastructure security controls described below are applied per-tenant and are aligned with the CIS Azure Foundations Benchmark and the Azure Well-Architected Security Pillar.

8.5.1 Network Security

(a) **Network Security Groups (NSGs):** Each virtual machine is protected by NSGs that provide stateful firewall functionality with explicit allow/deny rules. Default policy: deny-all inbound; allow only required service ports.

(b) **Web Application Firewall (WAF):** Azure WAF is deployed in front of the application tier to protect against OWASP Top 10 threats, including SQL injection, XSS, CSRF, and request-smuggling attacks.

(c) **DDoS Protection:** Azure DDoS Protection Standard is enabled for all Customer environments, providing volumetric, protocol, and application-layer attack mitigation with automatic detection and inline remediation.

(d) **Network segmentation:** The data tier, application tier, and management tier are deployed in separate subnets with inter-tier traffic controlled by NSG rules. The database subnet is not directly accessible from the internet.

(e) **VPN & private connectivity:** Where the Customer requires site-to-site connectivity (e.g., integration with on-premises Active Directory), Azure VPN Gateway or ExpressRoute is provisioned with IPSec/IKEv2 encryption.

(f) **DNS security:** Azure Private DNS zones are used to prevent DNS-based data exfiltration. Public DNS records are protected with DNSSEC where supported by the registrar.

8.5.2 Compute Security

(a) **Operating system hardening:** All virtual machines run Microsoft Windows Server 2022, hardened per CIS Windows Server 2022 Benchmark. Unnecessary services, ports, and features are disabled.

(b) **Patch management:** Security patches are applied within: (i) seventy-two (72) hours for Critical/High CVEs; (ii) thirty (30) calendar days for Medium CVEs; (iii) next maintenance window for Low CVEs. Patches are tested in the Staging Environment before production deployment.

(c) **Anti-malware:** Cloud-native endpoint protection (Microsoft Defender for Cloud) is enabled on all virtual machines with real-time scanning, behavioural analysis, and automatic remediation.

(d) **Host-based intrusion detection:** Azure Security Centre monitors file-integrity, suspicious process execution, and anomalous system calls on all VMs.

8.5.3 Identity & Secrets Management

(a) **Azure Key Vault:** All cryptographic keys, certificates, connection strings, and service credentials are stored in Azure Key Vault with access controlled by Azure RBAC and Key Vault access policies.

(b) **Managed identities:** Azure Managed Identities are used for service-to-service authentication where possible, eliminating the need for stored credentials in application configuration.

(c) **Secret rotation:** Automated secret-rotation policies are enforced for all service-account credentials and API keys. Maximum rotation period: ninety (90) calendar days.

8.6 Database Security

The Platform's data tier runs on **Microsoft SQL Server 2022 (Standard or Enterprise Edition)** deployed on Microsoft Windows Server 2022. The following database-specific security controls are applied, aligned with the CIS SQL Server 2022 Benchmark:

8.6.1 Access & Authentication

(a) **Database authentication:** SQL Server uses Windows Authentication mode (integrated with Active Directory) as the primary authentication method. Mixed-mode authentication is disabled unless explicitly required and approved by the Customer.

(b) **Application passwords:** Application-level database credentials use strong passwords compliant with the password-composition policy and are rotated per the secret-rotation schedule (§8.5.3).

(c) **Default accounts:** All default system accounts (e.g., 'sa') are properly secured by the DBA: default passwords are changed immediately upon provisioning; unnecessary default accounts are disabled or dropped.

(d) **Connection control:** Connections to the database instances are controlled and monitored. Only authorised application-layer services and designated DBA personnel may establish connections. Connection strings are stored in Azure Key Vault (§8.5.3).

(e) **Ability to connect:** Network-level controls restrict database connectivity to the application-tier subnet and authorised management endpoints only. Direct internet connectivity to the database is prohibited.

8.6.2 Privilege Management

(a) **Minimum permissions & roles:** Database user accounts are provisioned with the minimum permissions and roles necessary for their function. The principle of least privilege is enforced and periodically reviewed.

(b) **System privileges:** All 'system' privileges are removed from user accounts unless explicitly required and approved. Privileged operations require a separate, dedicated DBA account with MFA.

(c) **Segregation of duties:** Database administration privileges are segregated from application-development privileges. Developers do not have production database access.

(d) **Privilege review:** Quarterly review of database privilege assignments; unused or excessive privileges are revoked. Review results are documented and available for audit (§7.11).

8.6.3 Encryption

(a) **Transparent Data Encryption (TDE):** TDE is enabled on all production and staging database instances, encrypting data files, log files, and tempdb using AES-256 encryption. TDE certificates are backed up and stored in Azure Key Vault.

(b) **Backup encryption:** All database backups (full, differential, and transaction-log) are encrypted using AES-256 with Customer-specific encryption keys managed through Azure Key Vault.

(c) **Column-level encryption:** Where required by the Customer's data-classification policy, column-level encryption (Always Encrypted) is available for highly sensitive fields (e.g., national IDs, bank account numbers).

8.6.4 Auditing & Logging

(a) **Audit logging:** SQL Server Audit captures: (i) all DDL operations (schema changes); (ii) privileged-user activity; (iii) failed authentication attempts; (iv) data-export and bulk-copy operations; (v) permission changes. Audit logs are written to a tamper-evident store.

(b) **Logging retention:** Database audit logs are retained for a minimum of twelve (12) months online and twenty-four (24) months in archival storage. Retention meets regulatory requirements under GDPR, UAE PDPL, and applicable industry standards.

(c) **Change tracking:** SQL Server Change Tracking and Change Data Capture (CDC) are enabled to provide a complete inventory of data modifications for compliance and audit purposes.

(d) **DBA remote access:** Remote database administration is restricted to named individuals via encrypted channels with multi-factor authentication. All DBA sessions are logged with full command-level audit trail (§7.8.3).

8.7 Vulnerability Management

The Provider operates a continuous vulnerability management programme aligned with NIST CSF Identify (ID.RA) and Protect (PR.IP) functions:

8.7.1 Assessment Schedule

Assessment Type	Frequency	Scope	Standard / Tool
Automated vulnerability scan (infrastructure)	Weekly	All Azure VMs, NSGs, storage accounts, Key Vaults	Microsoft Defender for Cloud + third-party scanner
Automated vulnerability scan (application)	Weekly (on every build)	DANAOS Web Framework codebase; OWASP Top 10 + SANS CWE 25	SAST + DAST integrated into CI/CD pipeline
Dependency / supply-chain scan	On every build + daily	Third-party libraries, NuGet/npm packages, container images	Software Composition Analysis (SCA) tool

Penetration test (external)	Annually	Public-facing attack surface; authentication bypass, privilege escalation, data exfiltration	Certified third-party penetration-testing firm
Penetration test (internal / red team)	Annually	Lateral movement, privilege escalation, insider-threat scenarios	Provider security team or certified third party
Configuration compliance scan	Monthly	CIS Benchmark compliance for Azure, Windows Server, SQL Server	CIS-CAT Pro or equivalent

8.7.2 Remediation Timelines

CVSS Severity	Score Range	Remediation SLA	Escalation
Critical	9.0–10.0	≤72 hours	Immediate escalation to CISO; Customer notification within 24 hours if Customer-facing
High	7.0–8.9	≤30 calendar days	Escalation to security lead; included in next patch cycle
Medium	4.0–6.9	≤90 calendar days	Tracked in vulnerability register; scheduled remediation
Low	0.1–3.9	Next major release	Documented; remediated as part of ongoing hardening

Zero-day vulnerabilities: For actively exploited zero-day vulnerabilities affecting the Platform's technology stack, the Provider shall apply emergency mitigation measures (e.g., WAF rules, network isolation, virtual patching) within twenty-four (24) hours, with a permanent patch following the Critical remediation SLA.

8.8 Security Monitoring & Incident Response

8.8.1 Monitoring

The Provider operates a 24/7 security-monitoring capability using the following components:

(a) **SIEM:** Cloud-native Security Information and Event Management (Microsoft Sentinel) aggregates logs from all infrastructure, application, and database layers. Correlation rules and machine-learning detections identify anomalous patterns.

(b) **AIOps:** AI-driven operations tooling provides predictive anomaly detection on performance metrics, authentication patterns, and data-access volumes, enabling early identification of security-relevant deviations before they escalate to incidents.

(c) **Threat intelligence:** SIEM integrates real-time threat-intelligence feeds (Microsoft Threat Intelligence, industry-specific IOCs) to detect known attack signatures and indicators of compromise.

(d) **User and Entity Behaviour Analytics (UEBA):** Baseline behaviour profiles are established for users and service accounts. Deviations (e.g., anomalous login locations, unusual data-access patterns, privilege-escalation attempts) trigger automated alerts.

8.8.2 Security Incident Response

Security incidents that do not involve Personal Data are managed under this section. Personal Data breaches are governed by §7.15. Where an incident is later classified as involving Personal Data, the §7.15 breach-notification procedures apply **in addition to** the measures below.

Phase	Activities	Timeline
Detection & Triage	SIEM/AIOps alert triggered → SOC analyst validates → incident classified by severity → assigned to responder	Real-time
Containment	Isolate affected systems; block IOCs at perimeter; revoke compromised credentials; preserve forensic evidence	≤60 minutes (Critical); ≤4 hours (High)
Eradication	Remove threat actor presence; patch exploited vulnerability; rebuild compromised components from known-good images	Concurrent with containment
Recovery	Restore services from clean backups; validate integrity; re-enable network connectivity; confirm no residual indicators	Per RTO targets (§3.4)
Post-Incident Review	Root-cause analysis; lessons-learned documentation; control improvements; Customer notification (if applicable)	≤15 business days post-containment

8.8.3 Customer Notification

The Provider shall notify the Customer of security incidents that: (i) result in actual or suspected unauthorised access to Customer Data; (ii) materially affect Platform availability or integrity; or (iii) involve law-enforcement engagement related to the Customer's environment. Notification shall occur within the timelines aligned with the incident severity and the breach-notification SLAs defined in §7.15.1.

8.9 Secure Development Lifecycle (SDLC)

The Provider follows a secure SDLC aligned with OWASP's Software Assurance Maturity Model (SAMM) and Microsoft's Security Development Lifecycle (SDL):

(a) **Threat modelling:** New features and significant changes undergo threat modelling during design. STRIDE methodology is used to identify threats; DREAD is used to prioritise risk.

(b) **Secure-coding standards:** Developers follow the Provider's secure-coding standard (based on OWASP Secure Coding Practices) covering input validation, output encoding, authentication, session management, error handling, and cryptography.

(c) **Static Application Security Testing (SAST):** Automated SAST runs on every code commit. Findings of High/Critical severity block the build until resolved.

(d) **Dynamic Application Security Testing (DAST):** DAST is executed against the Staging Environment before every production deployment. The scan targets the OWASP Top 10 and ASVS Level 2 controls.

(e) **Software Composition Analysis (SCA):** All third-party dependencies are scanned for known vulnerabilities (CVEs) and licence compliance on every build. Components with unpatched Critical/High CVEs are blocked.

(f) **Code review:** All production code changes require peer review and approval before merge to the Master branch. Security-sensitive changes (authentication, cryptography, access-control logic) require review by a designated security champion.

(g) **Version control:** Git-based version control with Master/Client/Working branch model (§4.7). All commits are signed and traceable to individual developers. Force-push to Master is prohibited.

8.10 Source Code Protection

The Provider's source code constitutes **proprietary intellectual property** and is subject to the following protections:

(a) **Access restriction:** Source code repositories are accessible only to authorised Provider development personnel. Customer personnel do not have access to source code unless a separate source-code escrow agreement is executed.

(b) **Source-code escrow:** Upon Customer request, the Provider shall enter into a source-code escrow agreement with a reputable third-party escrow agent. Release conditions typically include: Provider insolvency, material breach of this Framework, or discontinuation of the Platform without an adequate successor product.

(c) **Thin-client architecture:** The Platform operates as a thin-client web application. No proprietary source code, compiled binaries, or application logic is distributed to Client devices. All application processing occurs server-side within the Customer's sovereign environment.

(d) **Obfuscation:** Client-side JavaScript and CSS delivered to the browser are minified and obfuscated. Source maps are not exposed in production deployments.

(e) **No open-source obligation:** The Provider ensures that the use of open-source components does not create an obligation to disclose proprietary source code (e.g., copyleft licence contamination). All open-source components are vetted for licence compatibility before adoption.

8.11 Confidentiality Obligations

8.11.1 Information Classification

All information exchanged between the Parties is classified according to the following scheme:

Classification	Definition	Handling Requirements
STRICTLY CONFIDENTIAL	Customer Data, source code, security configurations, encryption keys, penetration-test reports, vulnerability reports	Encrypted at rest and in transit; access restricted to named individuals on a need-to-know basis; no disclosure to third parties

		without written consent; deletion/return on termination (§7.13)
CONFIDENTIAL	Commercial terms, pricing, project plans, architectural diagrams, process documentation, training materials	Protected from unauthorised disclosure; shared only with authorised personnel; marked 'CONFIDENTIAL' when distributed; encrypted in transit
INTERNAL	Provider internal procedures, non-sensitive operational documentation	Not shared externally; standard access controls; no public disclosure
PUBLIC	Marketing materials, published product documentation, publicly available certifications	No handling restrictions; may be freely distributed

8.11.2 Mutual Confidentiality Undertakings

Each Party undertakes to the other that it shall:

(a) Keep confidential all Confidential Information of the disclosing Party and not disclose it to any third party without the prior written consent of the disclosing Party.

(b) Use the Confidential Information solely for the purpose of performing its obligations or exercising its rights under this Framework.

(c) Restrict disclosure of Confidential Information to those of its employees, agents, or sub-processors who need to know the information for the purposes of this Framework and who are bound by confidentiality obligations no less restrictive than those contained herein.

(d) Apply the same degree of care to protect the Confidential Information of the disclosing Party as it applies to its own confidential information, but in no event less than reasonable care.

(e) Promptly notify the disclosing Party of any actual or suspected unauthorised disclosure or use of Confidential Information.

8.11.3 Exclusions

The confidentiality obligations shall not apply to information that:

(a) Is or becomes publicly available through no fault of the receiving Party.

(b) Was already known to the receiving Party at the time of disclosure, as demonstrated by written records.

(c) Is independently developed by the receiving Party without reference to the Confidential Information.

(d) Is lawfully obtained from a third party without restriction on disclosure.

(e) Is required to be disclosed by applicable law, regulation, or court order, provided that the receiving Party gives prompt written notice to the disclosing Party (to the extent legally permissible) and cooperates in any effort to obtain protective treatment.

8.11.4 Survival

The confidentiality obligations set out in this section shall survive termination or expiry of this Framework for a period of **five (5) years**, except with respect to trade secrets, which shall be protected for as long as they remain trade secrets under applicable law.

8.12 Access Removal

8.12.1 Systems Access Removal

When a Provider employee's role changes or their employment terminates, all systems access is removed within:

(a) **Involuntary termination or security concern:** Immediate revocation (within 1 hour) of all system credentials, VPN access, Key Vault permissions, and physical-facility access.

(b) **Planned departure:** Access is revoked on the last working day. All Provider-owned devices are returned and wiped.

(c) **Role change:** Access is adjusted within one (1) business day to reflect the new role's privilege requirements. Excess privileges from the prior role are removed.

8.12.2 Application Access Removal

When a Customer end-user's role changes or they leave the Customer's organisation:

(a) **Customer responsibility:** The Customer's system administrator (or Champion) is responsible for disabling or modifying user accounts within the STY module.

(b) **Provider support:** Where the Customer requires Provider assistance (e.g., bulk-deactivation, emergency lockout), a P2 service request (§4.3) shall be raised and processed within the applicable SLA.

(c) **Dormant-account detection:** The Platform flags accounts with no login activity for more than ninety (90) calendar days. Flagged accounts are reported to the Customer administrator for review and potential deactivation.

8.13 Process Register

The following table enumerates the contractual and operational processes governed by this chapter. Each process is assigned a unique identifier, trigger condition, responsible handler, approver, expected outcome, and cross-reference to the governing section.

Proc-ID	Process Name	Trigger	Handler	Approver	Outcome	Section
P-8.01	ISMS Risk Assessment	Annual schedule or significant change	Provider CISO / IT Dept	Provider Management	Updated risk register and SoA	§8.3
P-8.02	Authentication Policy Update	Regulatory change, security incident, or annual review	Provider IT Dept	Provider CISO	Updated authentication controls in STY module	§8.4.1
P-8.03	Access-Control Review	Quarterly schedule	Provider IT Dept + Customer Admin	Customer PM	Privilege reconciliation report; excess privileges revoked	§8.4.2

P-8.04	NSG / Firewall Rule Change	Change request or security incident	Provider Cloud Ops	Provider CISO	Updated firewall rules; change-log entry; rollback capability	§8.5.1
P-8.05	Patch Deployment	Vendor patch release or zero-day disclosure	Provider Cloud Ops	Provider CISO	Patched systems within remediation SLA; test evidence	§8.5.2
P-8.06	Database Privilege Review	Quarterly schedule	Provider DBA	Provider CISO	Reviewed privilege assignments; revoked excess	§8.6.2
P-8.07	Encryption Key Rotation	Rotation schedule (max 90 days) or key compromise	Provider Cloud Ops	Provider CISO	Rotated keys; updated Key Vault references	§8.5.3
P-8.08	Vulnerability Scan (Infrastructure)	Weekly schedule	Provider Cloud Ops	Provider CISO	Scan report; new findings triaged and prioritised	§8.7.1
P-8.09	Vulnerability Scan (Application)	Every build + weekly	Provider Dev / Security	Provider CISO	SAST/DAST/SCA findings; Critical/High blocked	§8.7.1
P-8.10	Penetration Test	Annual schedule	Third-party tester	Provider CISO + Customer PM	Pen-test report with findings and remediation plan	§8.7.1
P-8.11	Vulnerability Remediation	New finding classified ≥ Medium	Provider Dev / Cloud Ops	Provider CISO	Remediation within CVSS-based SLA	§8.7.2
P-8.12	Security Incident Response	SIEM/AIOps alert or manual detection	Provider SOC	Provider CISO	Incident contained; RCA delivered within 15 BDs	§8.8.2
P-8.13	Threat-Model Review	New feature or significant change	Provider Security Champion	Provider CISO	Updated threat model; identified risks mitigated	§8.9
P-8.14	Code Security Review	Pull request targeting Master branch	Peer reviewer + Security Champion	Provider Dev Lead	Approved merge; SAST findings resolved	§8.9
P-8.15	Source-Code Escrow Update	New major release or Customer request	Provider Legal / Dev	Customer PM	Updated escrow deposit with current release	§8.10
P-8.16	Information Classification Review	Annual schedule or new information type	Provider DPO + CISO	Provider Management	Updated classification register	§8.11.1

P-8.17	Provider Staff Access Removal	Employment termination or role change	Provider HR + IT Dept	Provider CISO	Access revoked within SLA; device wiped	§8.12.1
P-8.18	Dormant Account Review	90-day inactivity flag	Customer Admin / Champion	Customer PM	Account deactivated or exception documented	§8.12.2

8.14 Process-Flow Schematic

The following diagram illustrates the information-security lifecycle from risk assessment through continuous monitoring and incident response.

① ISMS Risk Assessment → ② Security Architecture & Controls → ③ Secure Development & Deployment

|

▼

④ Vulnerability Management → ⑤ Continuous Monitoring (SIEM / AIOps) → ⑥ Access Control & Reviews

|

▼

⑦ Incident Detection & Response → ⑧ Post-Incident Review & Improvement → ⑨ Compliance Audit & Certification

Continuous loop: Stage ⑨ (Audit & Certification) feeds back into Stage ① (Risk Assessment) through the ISMS continuous improvement cycle (Plan–Do–Check–Act). Stages ④–⑦ operate continuously with weekly automated scans and real-time SIEM monitoring. Annual penetration tests and certification audits provide independent assurance.

9 Business Continuity & Disaster Recovery

9.1 Overview & Purpose

This chapter defines the **business-continuity and disaster-recovery (BCDR)** obligations governing the Provider's delivery of the ProjectVIEW ERP Platform. It establishes the backup strategy, replication architecture, failover procedures, recovery-time objectives, data-redundancy commitments, and continuity-planning requirements that ensure Customer Data remains available, durable, and recoverable throughout the Subscription Term.

The Provider's Business Continuity Management System (BCMS) is aligned with **ISO 22301:2019** (Security and Resilience — Business Continuity Management Systems) and draws upon the **NIST SP 800-34 Rev. 1** (Contingency Planning Guide for Federal Information Systems) and the **Microsoft Cloud Enterprise Business Continuity Management (EBCM) Programme**. This chapter complements the availability commitments defined in Chapter 3 (Service Level Agreement), the infrastructure-security controls described in Chapter 8 (Information Security & Confidentiality), and the data-protection provisions of Chapter 7 (Data Protection & Privacy).

Each Customer's dedicated private sovereign environment is provisioned with defence-in-depth continuity controls spanning compute, database, storage, and network tiers — ensuring that no single point of failure can result in data loss or extended service interruption beyond the contracted Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

9.2 Scope

This chapter covers:

(a) **Recovery objectives:** Contractually binding RPO and RTO commitments for all tiers of the Platform.

(b) **Backup management:** Backup schedules, retention periods, integrity verification, and restoration procedures for virtual machines, databases, and application artefacts.

(c) **Data redundancy & replication:** Azure Storage replication options (LRS, ZRS, GRS), database read-replicas, and geo-redundant failover architecture.

(d) **Disaster recovery:** Failover procedures, secondary-region activation, communication protocols, and service-restoration workflows.

(e) **Business continuity planning:** Business Impact Analysis (BIA), continuity plan maintenance, DR drill schedules, and post-incident review procedures.

(f) **Data ownership & portability:** Customer data-ownership rights, data-export mechanisms, records-management obligations, and e-discovery support.

(g) **Roles & responsibilities:** RACI allocation across Provider and Customer organisations for all BCDR activities.

This chapter does not cover application-level security controls (see Chapter 8), personal-data processing (see Chapter 7), or operational-support workflows (see Chapter 4).

9.3 Standards & Framework Alignment

The Provider's BCDR programme is aligned with the following internationally recognised standards and frameworks:

Standard / Framework	Scope of Alignment	Reference
ISO 22301:2019	Business Continuity Management Systems — requirements for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving a BCMS.	https://www.iso.org/standard/75106.html
ISO 27031:2011	Guidelines for Information and Communication Technology Readiness for Business Continuity (IRBC) — extending ISO 22301 to ICT services.	https://www.iso.org/standard/44374.html
NIST SP 800-34 Rev. 1	Contingency Planning Guide for Federal Information Systems — BIA methodology, recovery strategies, plan testing, and maintenance.	https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final
Azure EBCM Programme	Microsoft's Enterprise Business Continuity Management programme governing Azure platform resilience, availability zones, and geo-redundant infrastructure.	https://learn.microsoft.com/en-us/compliance/assurance/assurance-bcdr
Azure Well-Architected Framework — Reliability Pillar	Design principles for resilient cloud workloads: redundancy, fault isolation, self-healing, and graceful degradation.	https://learn.microsoft.com/en-us/azure/well-architected/reliability/
ITIL 4 — Service Continuity Management	IT Service Continuity Management (ITSCM) practice ensuring agreed service-continuity levels during and after a disaster.	https://www.axelos.com/certifications/itil-service-management

9.4 Recovery Objectives

The following **contractually binding** recovery objectives apply to each Customer's dedicated private sovereign environment. These objectives define the maximum tolerable data loss (RPO) and the maximum tolerable downtime (RTO) for each tier of the Platform:

Recovery Metric	Tier	Objective	Measurement
Recovery Point Objective (RPO)	Database Tier (SQL Server 2022)	15 minutes	Maximum data loss measured from the point of failure to the most recent successful backup or replication checkpoint.
Recovery Point Objective (RPO)	Virtual Machine Tier	24 hours	Maximum data loss for VM-level state (OS, application binaries,

			configuration). Daily snapshots ensure RPO ≤ 24h.
Recovery Point Objective (RPO)	File / Blob Storage Tier	Near-zero (GRS)	Geo-redundant Storage replication provides asynchronous cross-region replication with near-zero RPO under normal conditions.
Recovery Time Objective (RTO)	Database Tier (SQL Server 2022)	4 hours	Maximum elapsed time from incident declaration to restored database availability, including failover to read-replica if provisioned.
Recovery Time Objective (RTO)	Full Platform (End-to-End)	8 hours	Maximum elapsed time from incident declaration to full Platform operational status, including compute, database, networking, and application verification.
Recovery Time Objective (RTO)	Secondary Region Failover	24 hours	Maximum elapsed time for complete failover to secondary Azure region when primary region is declared unrecoverable.

Where the Customer has elected the **Enhanced DR Option** (secondary server with read-only database replicas and high-frequency replication at up to 15-minute intervals), the database-tier RTO is reduced to **1 hour** as the secondary VM assumes the primary role with minimal data and time loss. The Enhanced DR Option is subject to additional subscription fees as set out in the applicable Commercial Contract.

Azure SQL Database Business Continuity Overview

9.5 Backup Management

The Provider maintains a comprehensive backup regime covering all components of each Customer's dedicated private sovereign environment. Backup operations are performed using Azure Backup and native SQL Server backup capabilities.

9.5.1 Backup Schedule & Retention

Component	Backup Type	Frequency	Retention	Storage Redundancy
SQL Server 2022 Databases	Full database backup	Daily	7 days (default); extended retention available on request	Geo-Redundant Storage (GRS)
SQL Server 2022 Databases	Transaction log backup	Every 15 minutes (Enhanced DR)	72 hours rolling	Geo-Redundant Storage (GRS)
Virtual Machines (Windows Server 2022)	Azure Backup VM snapshot	Daily	14 days (default); customisable up to 99 years via Azure policy	Geo-Redundant Storage (GRS)

Application Artefacts & Configuration	Git repository (Master + Client branches)	Continuous (on every commit)	Indefinite (full version history)	Azure DevOps geo-redundant storage
Blob / File Storage	Azure Storage replication	Continuous (synchronous within region)	As per Customer retention policy	GRS (6 copies across 2 regions)
Azure Key Vault Secrets & Keys	Azure-managed replication	Continuous	Indefinite (soft-delete + purge protection enabled)	Geo-redundant by default

Customised higher-frequency backups may be provisioned upon Customer request subject to additional subscription fees. All backup frequencies and retention periods are documented in the applicable **Backup Schedule Addendum** annexed to the Commercial Contract.

Azure Backup Overview

SQL Server Backup to Azure

9.5.2 Backup Integrity Verification

The Provider shall perform the following backup-integrity verification procedures:

(a) **Automated checksum validation:** Every backup operation generates a cryptographic checksum (SHA-256). The checksum is verified automatically upon completion and logged in the backup audit trail.

(b) **Monthly restore test:** At least once per calendar month, the Provider shall perform a test restoration of a randomly selected database backup to an isolated environment, verifying data completeness, referential integrity, and application-layer functionality.

(c) **Quarterly full-stack restore drill:** At least once per calendar quarter, the Provider shall perform a complete platform restoration (VM + database + application + configuration) to an isolated environment, simulating a full disaster-recovery scenario. Results are documented in the DR Drill Report.

(d) **Backup monitoring & alerting:** Azure Monitor alerts are configured to notify the Provider's Cloud Operations team within 15 minutes of any backup failure, timeout, or integrity-check failure. Failed backups trigger an automatic retry within 1 hour.

9.6 Data Redundancy & Replication

Each Customer's dedicated private sovereign environment leverages Azure's multi-layered data-redundancy architecture to protect against hardware failure, facility failure, and regional disaster:

Replication Option	Copies	Regions	Durability	Use Case
Locally Redundant Storage (LRS)	3 copies	1 region, 1 facility	11 nines (99.999999999%)	Default for non-critical temporary storage within a single data-centre.
Zone-Redundant Storage (ZRS)	3 copies	1 region, 2–3 availability zones	12 nines	Protection against single availability-zone failure within a region. Used for application configuration stores.

Geo-Redundant Storage (GRS)	6 copies	2 regions (primary + secondary, hundreds of km apart)	16 nines	Default for all Customer Data. Provides cross-region durability with automatic failover capability.
Read-Access Geo-Redundant Storage (RA-GRS)	6 copies	2 regions with read access to secondary	16 nines	Available upon Customer election for read-only access to replicated data during primary-region outage.

By default, each Customer's Azure Storage account is provisioned with **Geo-Redundant Storage (GRS)**, maintaining six copies of Customer Data — three within the primary Azure region and three within a geographically paired secondary region. In the event of a primary-region failure, Azure Storage automatically fails over to the secondary region, ensuring data durability without manual intervention.

Azure Storage Redundancy

9.6.1 Database Replication

SQL Server 2022 databases within each Customer's environment support the following replication configurations:

(a) **Standard configuration:** Daily full backups with 7-day retention, stored in GRS. Transaction logs are backed up according to the configured schedule (default: hourly; Enhanced DR: every 15 minutes).

(b) **Enhanced DR configuration (optional):** A secondary SQL Server instance is provisioned with read-only replicas of all Customer databases. High-frequency log shipping (up to 15-minute intervals) ensures near-real-time data synchronisation. In the event of a primary-server failure, the secondary server automatically assumes the primary role, providing continuity with minimal data loss (RPO ≤ 15 minutes) and rapid recovery (RTO ≤ 1 hour).

(c) **Data residency compliance:** Data replication is constrained to the Customer's selected geographic region unless the Customer explicitly authorises cross-region replication in writing. Data cannot be transmitted outside the selected geographic area without Customer consent, in compliance with GDPR Article 44 and UAE PDPL Article 22 cross-border transfer requirements (see Chapter 7, §7.14).

9.7 Disaster Recovery Procedures

The Provider maintains documented disaster-recovery procedures for each tier of the Platform. These procedures are tested at least quarterly and updated following any material change to the Platform architecture, Azure service capabilities, or Customer environment configuration.

9.7.1 Incident Classification & Escalation

Disaster-recovery events are classified according to the following severity taxonomy:

DR Severity	Description	Example Scenarios	Escalation
DR-1: Critical	Complete loss of primary environment — compute, database, and/or networking fully unavailable. No workaround exists.	Azure region-wide outage; primary VM and all backups corrupted; data-centre destruction.	Immediate: CTO + Cloud Ops Lead + Customer Account Manager. Customer notified within 30 minutes.

DR-2: Major	Partial loss of a critical tier — service is degraded but partially functional, or a single-tier failure with workaround available.	Primary database server failure (read-replica available); VM failure (backup restorable); storage account degradation.	Within 1 hour: Cloud Ops Lead + DBA. Customer notified within 2 hours.
DR-3: Moderate	Non-critical component failure or performance degradation that does not impact core transactional processing.	Backup job failure; monitoring agent offline; secondary-region replication lag exceeding threshold.	Within 4 hours: Cloud Ops team. Customer notified in next scheduled status update.
DR-4: Minor	Precautionary alert or near-miss event requiring investigation but no immediate service impact.	Azure health advisory for planned maintenance; storage latency spike resolved automatically; failed DR drill component.	Logged and investigated. Customer notified only if escalated to DR-3 or above.

9.7.2 Failover Procedures

The following failover procedures are executed in sequence upon declaration of a DR-1 or DR-2 event:

Phase	Activity	Owner	Target Duration	Success Criteria
1. Detection	Azure Monitor / SIEM alert received and acknowledged by Cloud Operations on-call engineer.	Cloud Ops (On-Call)	< 15 minutes	Alert acknowledged; incident ticket created; severity classified.
2. Assessment	Determine scope of failure: affected tier(s), data integrity status, availability of read-replicas and recent backups.	Cloud Ops Lead + DBA	< 30 minutes	Root-cause hypothesis documented; recovery path selected.
3. Customer Notification	Notify Customer Account Manager and designated Customer contacts via agreed communication channel.	Account Manager	< 30 min (DR-1) < 2 hr (DR-2)	Customer acknowledges receipt; Incident Bridge convened for DR-1.
4. Database Recovery	Activate read-replica failover (Enhanced DR) or restore most recent database backup to replacement VM.	DBA + Cloud Ops	< 1 hr (Enhanced DR) < 4 hr (Standard)	Database online; referential-integrity check passed; RPO verified.
5. Compute Recovery	Restore VM from Azure Backup snapshot or provision new VM from baseline image + apply latest configuration.	Cloud Ops	< 4 hours	VM operational; application services responding; health-check passed.

6. Application Verification	Execute automated smoke tests and manual validation of core transactional workflows (login, data entry, reporting).	QA / Cloud Ops	< 1 hour	All critical paths pass; no data corruption detected.
7. DNS / Network Cutover	Update DNS records and/or Azure Traffic Manager to route traffic to restored environment. Verify SSL/TLS certificates.	Cloud Ops	< 30 minutes	End-users can connect; HTTPS verified; latency within SLA.
8. Service Restoration	Declare service restored. Resume SLA clock. Begin post-incident monitoring (heightened alerting for 72 hours).	Cloud Ops Lead	N/A	Service restored; SLA metrics resume; monitoring confirmed.
9. Post-Incident Review	Conduct Root Cause Analysis (RCA) within 5 Business Days. Publish Post-Incident Report (PIR) to Customer.	CTO + Cloud Ops Lead	5 Business Days	PIR delivered; corrective actions assigned; BCDR plan updated.

9.7.3 Secondary-Region Failover

Where the primary Azure region is declared unrecoverable by Microsoft or by the Provider's CTO, the Provider shall execute a **full secondary-region failover** to the geographically paired Azure region. This procedure includes:

(a) **GRS failover initiation:** Azure Storage automatically fails over to the secondary region. RA-GRS accounts provide immediate read access to replicated data.

(b) **VM re-provisioning:** New virtual machines are provisioned in the secondary region from the most recent Azure Backup vault (cross-region restore enabled).

(c) **Database restoration:** SQL Server databases are restored from geo-redundant backups or, where Enhanced DR is provisioned, from the secondary read-replica server in the paired region.

(d) **DNS reconfiguration:** Azure Traffic Manager or DNS records are updated to route all Customer traffic to the secondary-region endpoints.

(e) **Validation & declaration:** Full application-verification suite is executed prior to declaring service restored from the secondary region.

The target RTO for a complete secondary-region failover is **24 hours** from the point of primary-region declaration. The Customer shall be kept informed at minimum every 2 hours during the failover procedure via the agreed communication channel.

Azure Cross-Region Disaster Recovery

9.8 Business Continuity Planning

9.8.1 Business Impact Analysis (BIA)

The Provider maintains a Business Impact Analysis for the ProjectVIEW ERP Platform that identifies critical business processes, maps their dependencies on Platform components, and quantifies the impact of service disruption. The BIA is reviewed and updated:

(a) At least annually as part of the BCMS management review cycle.

(b) Following any material change to the Platform architecture, Azure region configuration, or Customer deployment topology.

(c) Following any DR-1 or DR-2 incident that reveals gaps in the existing BIA.

The BIA informs the recovery-objective calibration (RPO/RTO), backup-frequency decisions, and replication-architecture design for each Customer environment.

9.8.2 Business Continuity Plan (BCP)

The Provider's Business Continuity Plan documents the procedures, roles, communication protocols, and resource allocations required to maintain or restore Platform services during a disruption. The BCP includes:

(a) **Crisis Management Team (CMT) composition:** CTO (Incident Commander), Cloud Operations Lead, DBA Lead, Customer Account Manager, and Communications Lead.

(b) **Communication plan:** Predefined templates for Customer notification (initial alert, progress update, resolution notice, PIR distribution), internal escalation matrices, and vendor-contact registers (Microsoft Azure Support, domain registrars, SSL providers).

(c) **Resource inventory:** Documented inventory of all Azure resources per Customer environment (VMs, SQL instances, storage accounts, networking components, Key Vault secrets), maintained in the CMDB and validated quarterly.

(d) **Alternate-site procedures:** Step-by-step procedures for activating the secondary Azure region, including pre-provisioned infrastructure templates (Azure Resource Manager / Bicep) and automated deployment scripts.

(e) **Supplier continuity:** Assessment of critical third-party dependencies (Microsoft Azure SLA commitments, domain registrars, certificate authorities) and contingency measures for each.

9.8.3 DR Drill Programme

The Provider shall conduct regular DR drills to validate the effectiveness of the BCDR plan and ensure operational readiness:

Drill Type	Frequency	Scope	Participants	Output
Tabletop Exercise	Quarterly	Walk-through of a hypothetical DR scenario with the CMT to validate decision-making, communication, and escalation procedures.	CMT + Customer representative (optional)	Tabletop Exercise Report with findings and corrective actions.
Component Recovery Test	Monthly	Isolated restore of a single backup component (database, VM, or storage) to verify recoverability.	Cloud Ops + DBA	Recovery Test Log with RPO/RTO achieved vs. target.

Full-Stack DR Drill	Semi-annually	End-to-end platform recovery in an isolated environment simulating a DR-1 event, including database failover, VM restoration, and application verification.	CMT + QA + DBA + Cloud Ops	DR Drill Report with measured RPO/RTO, deviations, and improvement actions.
Secondary-Region Failover Drill	Annually	Complete failover to the paired secondary Azure region with live traffic redirection (during a pre-agreed maintenance window).	CMT + Customer + Cloud Ops	Regional Failover Report with measured RTO and Customer sign-off.

All drill results are documented, retained for a minimum of three (3) years, and made available to the Customer upon written request. Where a drill reveals a deviation from contracted RPO/RTO objectives, the Provider shall implement corrective actions within thirty (30) calendar days and repeat the relevant drill to confirm remediation.

9.9 Customer Data Ownership & Portability

The Customer retains **sole and exclusive ownership** of all Customer Data processed, stored, or generated within the Platform. The Provider does not inspect, approve, monitor, or claim any ownership right over Customer Data at any time, whether during the Subscription Term or following its expiration or termination.

Microsoft, as the underlying infrastructure provider, does not know what kind of data Customers choose to store in Azure and does not claim data ownership over Customer information entered into Azure services.

9.9.1 Data Export & Portability

The Provider shall make Customer Data available for export in the following manner:

(a) **On-demand export:** The Customer may request a full or partial export of Customer Data at any time during the Subscription Term. The Provider shall deliver the export within two (2) Business Days of receiving a valid written request, in a machine-readable, industry-standard format (SQL backup file, CSV, JSON, or XML as agreed).

(b) **Termination export:** Upon expiration or termination of the Framework, the Provider shall make all Customer Data available for export within two (2) Business Days of the Customer's written request, in accordance with the data-return provisions of Chapter 7, §7.13 (Data Return on Termination). The overall export window shall remain open for a minimum of sixty (60) calendar days from the effective date of termination.

(c) **Audit & compliance export:** The Customer may request audit logs, access logs, and change-tracking records for compliance purposes. Such exports are provided within two (2) Business Days of the written request.

9.9.2 Records Management

The Customer is responsible for identifying its own record-retention requirements in accordance with applicable law and industry regulation. The Provider supports Customer records-management obligations by:

(a) **Configurable retention policies:** The Platform supports configurable data-retention rules at the application level, allowing the Customer to define retention periods for different record categories.

(b) **Audit-trail preservation:** Azure Storage retention policies and SQL Server change tracking provide an immutable audit trail for all data modifications. Audit records are retained for a minimum period agreed in the Commercial Contract (default: seven years).

(c) **Export for external archival:** The Customer may export data and audit reports for external archival at any time during the Subscription Term. The Provider shall facilitate bulk export in standard formats upon written request.

9.9.3 Electronic Discovery (e-Discovery)

The Customer is responsible for complying with e-discovery requirements in its use of the Platform. The Provider shall support Customer e-discovery obligations by:

(a) **Data preservation holds:** Upon written request from the Customer citing a litigation-hold or regulatory-investigation requirement, the Provider shall place a preservation hold on specified Customer Data, suspending all automated deletion and retention-policy enforcement for the affected data sets.

(b) **Data export for e-discovery:** The Provider shall export and deliver the specified data sets in a format suitable for e-discovery review (including metadata and audit trails) within two (2) Business Days of the preservation-hold request.

(c) **Chain-of-custody documentation:** The Provider shall provide chain-of-custody documentation for all e-discovery exports, certifying the completeness and integrity of the exported data.

9.10 Azure Platform Resilience

The Provider leverages the following Azure-native resilience capabilities within each Customer's dedicated private sovereign environment:

(a) **Availability Zones:** Where available in the Customer's selected Azure region, critical resources (VMs, managed disks, load balancers) are deployed across multiple Availability Zones to protect against single-zone failure.

(b) **Azure Resource Health:** Monitors VM health and checks whether resources are running as expected, detecting known Azure platform problems that affect existing resources. Alerts are routed to the Cloud Operations team via Azure Monitor.

(c) **Azure Backup Vault:** Centralised backup management with cross-region restore capability, soft-delete protection (14 days), and multi-user authorisation for critical backup-deletion operations.

(d) **Azure Resource Locks:** CanNotDelete and ReadOnly locks are applied to all production resources to prevent accidental or malicious deletion or modification of critical infrastructure components.

(e) **Azure DDoS Protection:** Standard-tier DDoS protection is enabled on all Customer virtual networks, providing automatic attack mitigation with real-time telemetry and post-attack reporting.

(f) **Azure Key Vault:** Encryption keys, secrets, and certificates are stored in Azure Key Vault with soft-delete and purge-protection enabled, ensuring cryptographic material is recoverable even in the event of accidental deletion.

Azure Availability Zones Overview

Azure Resource Health Overview

Azure Backup Architecture

9.11 Customer Responsibilities

The Customer acknowledges and agrees to the following responsibilities in support of the BCDR programme:

(a) **Contact designation:** The Customer shall designate and maintain at least two (2) authorised contacts for DR-related communications, including after-hours emergency contact details. Contact details shall be updated within five (5) Business Days of any personnel change.

(b) **DR drill participation:** The Customer shall make reasonable efforts to participate in annual Secondary-Region Failover Drills and quarterly Tabletop Exercises, providing feedback on communication effectiveness and business-impact accuracy.

(c) **Retention-policy specification:** The Customer shall specify its data-retention requirements in writing during onboarding and update them as needed. The Provider shall configure the Platform retention policies accordingly.

(d) **Data-export validation:** Following any data-export operation (on-demand or termination), the Customer shall verify the completeness and integrity of the exported data within the agreed validation window. Failure to raise a data-completeness objection within the validation window shall constitute acceptance of the export.

(e) **End-user continuity planning:** The Customer is responsible for its own internal business-continuity planning, including end-user communication, manual-process fallbacks, and internal-systems dependencies that are outside the scope of the Platform.

9.12 Continuous Improvement

The Provider's BCDR programme is subject to a continuous-improvement cycle aligned with the Plan-Do-Check-Act (PDCA) methodology prescribed by ISO 22301:2019:

(a) **Plan:** Annual BIA review, recovery-objective calibration, and BCDR plan update based on changes to the Platform, Azure capabilities, and Customer requirements.

(b) **Do:** Execution of backup schedules, replication configurations, and DR drill programme as defined in this chapter.

(c) **Check:** Monitoring of backup success rates, DR drill results (measured RPO/RTO vs. target), post-incident reviews, and Customer feedback.

(d) **Act:** Implementation of corrective actions, architecture improvements, and procedure refinements identified through the Check phase. All improvements are tracked in the BCDR Improvement Register and reported in the quarterly Service Review meeting (see Chapter 4, §4.12).

9.13 Lifetime Software Warranty

The Provider warrants that the Platform shall, for the **entire duration of the Subscription Term and any renewal thereof** (the "**Warranty Period**"):

(a) **Conformance:** perform materially in accordance with the specifications, functionality, and service levels described in this Framework and the applicable Commercial Contract;

(b) **Defect Remediation:** be free from material defects that prevent the Customer from using the Platform for its intended business purposes. Any confirmed defect shall be remediated by the Provider at no additional cost to the Customer within the applicable SLA response and resolution targets defined in Chapter 3;

(c) **Version Currency:** remain on a currently supported and maintained technology stack. The Provider shall proactively upgrade all underlying COTS components (database engine, application framework, operating system, middleware) to vendor-supported versions within the release cycle defined in Section 4.7;

(d) **Security Maintenance:** receive continuous security patching throughout the Warranty Period, including Critical and High vulnerability remediation within the timelines specified in Chapter 8;

(e) **No Degradation:** maintain performance characteristics that meet or exceed the SLO and recovery-objective targets (RPO/RTO) defined in this Framework. The Provider shall not introduce changes that materially degrade Platform performance without Customer approval.

This warranty is a **lifetime warranty** co-extensive with the Customer's active Subscription. It does not expire, reduce in scope, or require separate renewal. The warranty survives version transitions under Chapter 10 and applies equally to the successor version from its General Availability date.

Exclusions: The warranty does not cover defects arising from (i) Customer modifications to the Platform outside the Provider's change management process; (ii) use of the Platform in a manner inconsistent with its documentation; (iii) third-party software or hardware not supplied or approved by the Provider; or (iv) Force Majeure Events.

9.14 Source Code Escrow

To provide the Customer with long-term continuity assurance, the Provider shall maintain a **source code escrow arrangement** as follows:

9.14.1 Escrow Deposit

(a) **Escrow Agent:** The Provider shall appoint a reputable, independent third-party escrow agent (the "Escrow Agent") to hold the Platform's source code. The identity of the Escrow Agent shall be disclosed to the Customer upon request.

(b) **Deposit Contents:** The escrow deposit shall include: (i) the complete source code of the Platform; (ii) build scripts and compilation instructions; (iii) database schemas and migration scripts; (iv) third-party dependency manifests and licence documentation; (v) system architecture documentation; and (vi) deployment procedures sufficient to enable a competent software professional to compile, deploy, and operate the Platform.

(c) **Update Frequency:** The escrow deposit shall be updated within thirty (30) days of each major version release (Upgrade) and at least once per calendar quarter for incremental releases (Updates).

(d) **Verification:** The Escrow Agent shall perform an annual verification of the deposit to confirm completeness and buildability. A summary verification certificate shall be provided to the Customer upon request.

9.14.2 Release Conditions

The Escrow Agent shall release the escrowed source code to the Customer upon the occurrence of any of the following release conditions:

(a) **Insolvency:** The Provider enters into liquidation, administration, receivership, or any analogous insolvency proceeding in any jurisdiction;

(b) **Cessation of Business:** The Provider ceases to carry on business or substantially all of its business;

(c) **Material Breach:** The Provider commits a material breach of this Framework that remains unremedied for sixty (60) days following written notice from the Customer;

(d) **Discontinuation:** The Provider permanently discontinues the Platform without providing a commercially reasonable successor product or transition path.

9.14.3 Customer Rights Upon Release

Upon release of the escrowed source code, the Customer shall be granted a **non-exclusive, non-transferable, irrevocable licence** to use, compile, modify, and deploy the source code solely for the purpose of continuing to operate the Platform for the Customer's own internal business purposes. This licence shall not include the right to redistribute, sublicense, or commercially exploit the source code.

9.14.4 Costs

The costs of establishing and maintaining the escrow arrangement, including the Escrow Agent's fees, deposit updates, and annual verification, shall be borne by the Customer. The Provider shall facilitate the initial set-up with the Escrow Agent and shall co-operate with all deposit and verification activities, but the Customer shall be solely responsible for the Escrow Agent's fees and any associated costs throughout the Subscription Term.

9.15 Roles & Responsibilities (RACI Matrix)

The following RACI matrix allocates responsibilities for key BCDR activities across Provider and Customer roles:

Activity	CTO	Cloud Ops Lead	DBA Lead	Account Mgr	Customer IT Lead	Customer CISO
BIA review & update	A	R	C	I	C	C
BCP maintenance	A	R	C	I	I	I
Backup schedule configuration	I	R	R	I	C	I
Backup integrity verification	I	R	R	I	I	I
DR drill planning & execution	A	R	R	C	C	C
DR drill reporting	A	R	C	R	I	I
Incident detection & classification	I	R	R	I	I	I
Incident communication to Customer	I	I	I	R	I	I

Database failover execution	I	C	R	I	I	I
VM restoration execution	I	R	C	I	I	I
Secondary-region failover	A	R	R	C	I	I
Post-incident review (PIR)	A	R	R	C	C	C
Data-export fulfilment	I	R	R	C	R	I
e-Discovery hold management	A	R	R	C	R	C
Retention-policy configuration	I	C	R	I	R	C
BCDR improvement tracking	A	R	C	I	I	I
Warranty defect remediation	A	R	R	C	C	I
Escrow deposit & update	A	R	C	I	I	I
Escrow verification (annual)	I	C	I	I	I	I
Escrow release adjudication	C	I	I	I	R	C

Legend: **R** = Responsible (executes the activity) · **A** = Accountable (ultimate decision authority) · **C** = Consulted (provides input before decision) · **I** = Informed (notified after decision).

9.16 Process Register

The following process register catalogues all formal processes defined in this chapter. Each process is assigned a unique identifier, trigger condition, responsible handler, accountable approver, expected outcome, and cross-reference to the governing section.

Process ID	Process Name	Trigger	Handler	Approver	Outcome	Section Ref.
P-9.01	BIA Review	Annual management review cycle or material architecture change	Cloud Ops Lead	CTO	Updated BIA document with revised impact ratings and recovery-priority rankings.	§9.8.1
P-9.02	BCP Update	BIA revision, post-incident review findings, or Azure capability change	Cloud Ops Lead	CTO	Updated Business Continuity Plan approved and	§9.8.2

					distributed to CMT.	
P-9.03	Backup Configuration	New Customer onboarding, environment provisioning, or backup-policy change request	DBA + Cloud Ops	Cloud Ops Lead	Backup schedules, retention periods, and storage redundancy configured and documented.	§9.5.1
P-9.04	Backup Integrity Verification	Completion of each backup operation; scheduled monthly/quarterly drill	Cloud Ops + DBA	Cloud Ops Lead	Checksum validated; restore test passed; results logged in backup audit trail.	§9.5.2
P-9.05	Backup Failure Remediation	Azure Monitor alert for backup failure, timeout, or integrity-check failure	Cloud Ops (On-Call)	Cloud Ops Lead	Automatic retry within 1 hour; manual investigation if retry fails; root-cause documented.	§9.5.2
P-9.06	DR Incident Detection	Azure Monitor / SIEM alert indicating potential service disruption	Cloud Ops (On-Call)	Cloud Ops Lead	Alert acknowledged within 15 min; incident ticket created; severity classified (DR-1 to DR-4).	§9.7.1
P-9.07	DR Incident Assessment	DR incident detected and classified as DR-1 or DR-2	Cloud Ops Lead + DBA	CTO	Root-cause hypothesis documented; recovery path selected; CMT convened for DR-1.	§9.7.2
P-9.08	Customer DR Notification	DR incident classified as DR-1 or DR-2	Account Manager	Cloud Ops Lead	Customer notified within 30 min (DR-1) or 2 hr (DR-2); Incident Bridge convened for DR-1.	§9.7.2
P-9.09	Database Failover	DR-1 or DR-2 incident affecting database tier	DBA Lead	CTO	Database online on read-replica or restored from backup; referential-	§9.7.2

					integrity check passed.	
P-9.10	VM Restoration	DR-1 or DR-2 incident affecting compute tier	Cloud Ops	Cloud Ops Lead	VM restored from Azure Backup snapshot; application services responding; health-check passed.	§9.7.2
P-9.11	Application Verification	Database and/or VM restoration completed	QA / Cloud Ops	Cloud Ops Lead	Automated smoke tests and manual validation passed; no data corruption detected.	§9.7.2
P-9.12	Service Restoration Declaration	All recovery phases completed and verified	Cloud Ops Lead	CTO	Service declared restored; SLA clock resumes; heightened monitoring for 72 hours.	§9.7.2
P-9.13	Post-Incident Review	DR-1 or DR-2 incident resolved	Cloud Ops Lead	CTO	Post-Incident Report (PIR) with RCA, corrective actions, and BCDR plan updates; delivered to Customer within 5 Business Days.	§9.7.2
P-9.14	Secondary-Region Failover	Primary Azure region declared unrecoverable	Cloud Ops + DBA	CTO	Full platform operational in secondary region within 24 hours; Customer sign-off obtained.	§9.7.3
P-9.15	DR Drill Execution	Scheduled drill (monthly/quarterly/semi-annual/annual per §9.8.3)	Cloud Ops + DBA + QA	CTO	Drill completed; RPO/RTO measured against targets; Drill Report published.	§9.8.3

P-9.16	Data Export Fulfilment	Customer written request for on-demand or termination data export	Cloud Ops + DBA	Account Manager	Customer Data exported in agreed format within 2 Business Days; chain-of-custody documented.	§9.9.1
P-9.17	e-Discovery Hold	Customer written request citing litigation hold or regulatory investigation	DBA + Cloud Ops	CTO	Preservation hold applied; automated deletion suspended; affected data sets exported within 2 Business Days.	§9.9.3
P-9.18	BCDR Improvement Tracking	DR drill deviation, PIR finding, or BIA gap identified	Cloud Ops Lead	CTO	Corrective action implemented within 30 days; follow-up drill confirms remediation; tracked in Improvement Register.	§9.12
P-9.19	Warranty Defect Remediation	Customer reports confirmed material defect	Provider (Engineering)	CTO	Defect remediated at no cost within SLA targets; fix deployed via standard release process.	§9.13, §3
P-9.20	Escrow Deposit Update	Major version release or quarterly release cycle	Provider (Engineering)	CTO	Updated source code, build scripts, schemas, and documentation deposited with Escrow Agent.	§9.14.1
P-9.21	Escrow Verification	Annual verification cycle	Escrow Agent	CTO	Verification certificate confirming deposit completeness and buildability; copy to Customer on request.	§9.14.1

P-9.22	Escrow Release	Release condition triggered (insolvency, cessation, material breach, discontinuation)	Escrow Agent	Customer	Source code released to Customer under irrevocable licence; Customer may compile and operate Platform.	§9.14.2

9.17 Process Flow Schematic

The following nine-stage lifecycle illustrates the end-to-end flow of business-continuity and disaster-recovery management within the Provider's BCDR programme:

① BIA & Risk Assessment → ② BCP & DR Plan Development → ③ Backup & Replication Configuration

↓

④ Monitoring & Detection → ⑤ Incident Classification & Escalation → ⑥ Failover & Recovery Execution

↓

⑦ Service Restoration & Verification → ⑧ Post-Incident Review & PIR → ⑨ Continuous Improvement & Drill Programme

Stage ① BIA & Risk Assessment: Annual Business Impact Analysis identifies critical processes, maps Platform dependencies, and quantifies disruption impact. Recovery-priority rankings and RPO/RTO targets are calibrated based on BIA outputs (P-9.01).

Stage ② BCP & DR Plan Development: The Business Continuity Plan and DR procedures are developed or updated based on BIA findings, incorporating CMT composition, communication templates, resource inventories, and secondary-region activation procedures (P-9.02).

Stage ③ Backup & Replication Configuration: Backup schedules, retention policies, and replication architecture (LRS/ZRS/GRS/RA-GRS) are configured for each Customer environment. Enhanced DR read-replicas are provisioned where elected (P-9.03).

Stage ④ Monitoring & Detection: Azure Monitor, SIEM, and Resource Health continuously monitor all Platform components. Backup completion and integrity are verified automatically with alerting on failure (P-9.04, P-9.05, P-9.06).

Stage ⑤ Incident Classification & Escalation: Detected incidents are classified (DR-1 to DR-4) and escalated per the severity taxonomy. Customer notification timelines are triggered based on severity level (P-9.07, P-9.08).

Stage ⑥ Failover & Recovery Execution: Database failover, VM restoration, and application verification are executed in sequence per the failover procedure table. Secondary-region failover is invoked for DR-1 events where the primary region is unrecoverable (P-9.09 through P-9.11, P-9.14).

Stage ⑦ Service Restoration & Verification: Service is declared restored upon completion of all recovery phases. SLA clock resumes and heightened monitoring is maintained for 72 hours. DNS/network cutover is verified (P-9.12).

Stage ⑧ Post-Incident Review & PIR: Root Cause Analysis is conducted within 5 Business Days. The Post-Incident Report is delivered to the Customer with corrective actions, BCDR plan updates, and lessons learned (P-9.13).

Stage ⑨ Continuous Improvement & Drill Programme: DR drills (tabletop, component, full-stack, regional) are executed per the scheduled programme. Deviations from RPO/RTO targets trigger corrective actions tracked in the Improvement Register. The PDCA cycle loops back to Stage ① (P-9.15, P-9.18).

10 End-of-Life, Version Transition & Subscription Cessation

10.1 Overview & Purpose

This chapter establishes the comprehensive framework governing the end-of-life (EOL) lifecycle of the ProjectVIEW ERP Platform, including major-version transitions, migration services, re-training obligations, integration and customisation adoption, data-return rights, and subscription-cessation procedures. It supersedes and expands upon the summary provisions of Chapter 4, §4.7.4.

The Provider's EOL framework is modelled on the mature version-transition practices of leading enterprise SaaS and ERP vendors — including **SAP S/4HANA**, **Oracle Fusion Cloud**, **IFS Cloud**, and **Infor CloudSuite** — adapted to the Provider's dedicated private sovereign deployment model and the Customer's right to full data ownership (Chapter 9, §9.9).

The core design principle is **no Customer left behind**: every Customer shall receive adequate notice, comprehensive migration support, re-training, and data-return services regardless of whether they elect to transition to the successor version or to terminate the subscription.

10.2 Scope

This chapter covers:

(a) **Version lifecycle phases:** General Availability (GA), Mainstream Support, Extended Support, End of Engineering (EOE), and End of Life (EOL) for each major version of the Platform.

(b) **Migration services:** Provider-led data migration, schema transformation, environment provisioning, and cutover planning for Customers transitioning to a successor version.

(c) **Re-training & change management:** Mandatory training programmes, Champion re-certification, user-adoption workshops, and knowledge-base updates required for a successful version transition.

(d) **Integration & customisation adoption:** Assessment, re-engineering, and validation of Customer-specific integrations, customisations, and configurations on the successor version.

(e) **Data return for non-upgrading Customers:** Data-export obligations, format specifications, delivery timelines, and chain-of-custody documentation for Customers electing not to transition.

(f) **Subscription cessation:** Formal procedures for service wind-down, environment decommissioning, and contractual termination.

(g) **Roles & responsibilities:** RACI allocation for all EOL activities across Provider and Customer organisations.

This chapter does not cover incremental releases/updates within a major version (see Chapter 4, §4.7.1) or COTS platform upgrades performed during Mainstream Support (see Chapter 4, §4.7.3).

10.3 Version Lifecycle Phases

Each major version of the Platform (e.g., v11, v12) progresses through a defined lifecycle. The Provider's lifecycle model draws upon the version-support frameworks published by SAP (Maintenance Strategy), Oracle (Sustaining Support), IFS (Mainstream/Extended Maintenance), and Infor (Product Lifecycle Policy), adapted to the Provider's **SaaS-only** delivery model:

Phase	Duration	What the Customer Receives	Provider Obligations
General Availability (GA)	Ongoing until successor GA	Full access to all Platform features, modules, and APIs. Incremental releases (v11.01, v11.02…) delivered via Agile sprints (§4.7.1).	Active development, feature enhancements, bug fixes, security patches, COTS currency maintenance.
EOL Announcement	T− 12 months	Formal written notice that the current major version will reach End of Life. Notice specifies successor version, indicative migration timeline, and available transition services.	Publish EOL Announcement. Commence successor-version readiness assessment for each Customer.
Transition Window	T− 12 months to T− 30 days	Migration planning, data-migration execution, re-training, integration re-engineering, UAT on successor version, and parallel running (where elected).	Deliver Migration Services, Training, and Integration Adoption as defined in §10.5–§10.7.
End of Engineering (EOE)	T− 30 days	No new Change Requests accepted. Technical Support continues (Incident resolution + security patches only).	Continue security-patch delivery and P1/P2 Incident resolution for the legacy version.
End of Life (EOL)	T = 0 (12 months after Announcement)	All support for the legacy version ceases. The Customer must be operating on the successor version or have elected Subscription Cessation.	Decommission legacy environment. Execute data return if Customer has elected cessation (§10.9).
Extended Support (optional)	Up to 12 months post-EOL	Available upon written request and subject to additional fees. Provides P1/P2 Incident resolution and critical security patches only. No feature development.	Deliver Extended Support under a separate Extended Support Addendum to the Commercial Contract.

Key commitment: The Provider guarantees a minimum of **twelve (12) months** between the EOL Announcement and the EOL Date. No Customer shall be required to transition in less than 12 months from the date of formal written notice. This aligns with best practice as observed across SAP, Oracle, IFS, and Infor lifecycle policies.

10.4 EOL Announcement & Customer Communication

The Provider shall communicate the EOL lifecycle to each Customer through the following structured programme:

Communication	Timing	Channel	Content
EOL Announcement Letter	T− 12 months (minimum)	Written notice to Customer's designated contact + Account Manager email	Formal EOL date, successor version identification, summary of migration services, indicative timeline, and Customer action required.
Migration Readiness Assessment	T− 11 months	Joint workshop (remote or on-site)	Impact assessment of Customer-specific integrations, customisations, and data volumes. Preliminary migration plan and resource requirements.

Quarterly Transition Status Updates	T−−9, T−6, T−3 months	Service Review meeting + written report	Migration progress, outstanding actions, risk register, training schedule, and projected cutover date.
EOE Notice	T− 30 days	Written notice + in-application banner	Confirmation that new Change Requests will no longer be accepted for the legacy version. Support scope reduction notice.
Final Migration Confirmation	T− 14 days	Written notice	Confirmation of completed migration (or Customer election for cessation + data return). Final cutover logistics.
EOL Confirmation	T = 0	Written notice	Legacy version decommissioned. Successor version is the sole supported version. Extended Support availability confirmed (if applicable).

10.5 Migration Services

The Provider shall deliver a structured migration programme for each Customer transitioning to the successor version. Migration services are **included in the subscription at no additional cost** for the standard migration scope defined below. Enhanced migration services (e.g., legacy-system data ingestion, complex ETL transformations, parallel running beyond the standard period) are available as separately scoped engagements.

10.5.1 Standard Migration Scope

(a) **Environment provisioning:** The Provider shall provision a successor-version environment within the Customer's dedicated private sovereign Azure tenant, configured with the same security controls, networking, and compliance settings as the existing production environment.

(b) **Data migration:** Full migration of all Customer Data from the legacy-version database to the successor-version database, including master data, transactional data, configuration data, and audit trails. The Provider shall use automated schema-transformation scripts validated against the Customer's data profile.

(c) **Data cleansing advisory:** Consistent with Oracle Fusion and Infor CloudSuite best practice, the Provider shall advise the Customer on data-cleansing opportunities prior to migration. The recommended approach is to migrate no more than three (3) years of active transactional data, with historical data archived in a read-only format accessible for reporting and compliance.

(d) **Configuration migration:** All Customer-specific configurations (roles, workflows, approval chains, notification rules, report templates, dashboards) are migrated to the successor version using the Provider's configuration-export/import tooling.

(e) **Migration testing:** A minimum of two (2) full migration rehearsals shall be executed in the Staging Environment prior to production cutover. Each rehearsal includes data-integrity verification (referential, computational, temporal), application-layer smoke testing, and performance benchmarking.

(f) **Cutover execution:** Production cutover to the successor version during a pre-agreed maintenance window, including DNS/network transition, database switchover, post-cutover verification, and rollback readiness.

(g) **Hypercare period:** A minimum of thirty (30) calendar days of dedicated post-migration hypercare support, during which the Provider shall assign a Migration Lead and dedicated support resources for priority incident resolution and stabilisation.

10.5.2 Data Migration Integrity Assurance

The Provider shall apply the following data-integrity controls throughout the migration process, aligned with the AI-augmented testing framework defined in Chapter 5 (Software Quality & Testing):

(a) **Pre-migration baseline:** A cryptographic hash (SHA-256) of the complete database and row-count inventory is captured immediately prior to migration commencement, establishing the data-integrity baseline.

(b) **Post-migration reconciliation:** Row-count reconciliation, referential-integrity assertions, and computational-integrity checks are executed against the successor-version database. The post-migration hash is compared against the pre-migration baseline.

(c) **AI-agent validation (optional):** Where the Customer has elected the AI-Augmented Testing service (Chapter 5), the Provider shall deploy AI agents against the successor-version environment to execute end-to-end simulation scenarios, validating data flows, business rules, and integration points.

(d) **Migration sign-off:** The Customer shall conduct UAT on the successor-version environment. Written Customer sign-off is required prior to production cutover, consistent with the UAT requirements defined in Chapter 5, §5.8.

10.6 Integration & Customisation Adoption

Major-version transitions may affect Customer-specific integrations, customisations, and third-party extensions. The Provider shall manage this transition through a structured adoption programme:

10.6.1 Integration Impact Assessment

Within thirty (30) calendar days of the EOL Announcement, the Provider shall deliver to the Customer an Integration Impact Assessment covering:

(a) **API compatibility analysis:** Mapping of all Customer-facing APIs used in the legacy version to their equivalents in the successor version, identifying breaking changes, deprecated endpoints, and new capabilities.

(b) **Third-party integration inventory:** Catalogue of all active integrations (middleware, B2G connectors, shipping APIs, banking interfaces, third-party reporting tools) with compatibility status for the successor version.

(c) **Customisation registry:** Complete inventory of Customer-specific customisations (compiled DLLs, custom SQL functions, bespoke reports, workflow extensions) with migration-path classification: (i) forward-compatible, (ii) requires re-engineering, (iii) deprecated / replacement available.

(d) **Effort estimate & timeline:** Indicative effort (person-days) and timeline for re-engineering non-compatible integrations and customisations, distinguishing between standard scope (included) and enhanced scope (separately quoted).

10.6.2 Re-Engineering & Validation

For integrations and customisations classified as “requires re-engineering”:

(a) **Provider-managed re-engineering:** Where the customisation was originally built by the Provider (recorded in the Git repository under the Customer’s Client Branch), the Provider

shall re-engineer and test the component at no additional cost as part of the standard migration scope.

(b) **Customer-managed or third-party integrations:** Where the integration was built by the Customer or a third party, the Provider shall (i) provide technical documentation for the successor-version API surface, (ii) make the Staging Environment available for testing, and (iii) offer optional professional-services assistance on a time-and-materials basis.

(c) **Integration regression testing:** All migrated integrations shall be subject to automated regression testing in the Staging Environment prior to production cutover, using the AI-agent framework (Chapter 5) or manual test scripts as agreed.

10.7 Re-Training & Change Management

A major-version transition constitutes a **Significant Platform Change** and triggers mandatory re-training obligations under Chapter 6 (Training & Knowledge Transfer). The Provider shall deliver a tailored transition-training programme encompassing:

10.7.1 Training Needs Re-Assessment

Within sixty (60) calendar days of the EOL Announcement, the Provider shall conduct a Training Needs Re-Assessment (TNRA) to identify:

(a) New or changed UI elements, workflows, and navigation patterns in the successor version.

(b) Deprecated features and their replacements.

(c) New capabilities enabled by the successor version (including AI-driven features where applicable).

(d) Role-specific training requirements based on the Customer's active module configuration and organisational structure.

The TNRA output is a Transition Training Plan, annexed to the Migration Plan, specifying sessions, durations, delivery methods, and target audiences.

10.7.2 Transition Training Programme

Training Component	Audience	Format	Timing	Duration
What's New Briefing	All Authorised Users	Webinar (recorded + AI-transcribed)	T−6 months	90 minutes
Hands-On Workshop: Core Changes	Super Users + Champions	Instructor-led (online or on-site)	T−5 to T−4 months	2–3 days per module group
Champion Re-Certification	DANAOS ProjectVIEW ERP Champions	Instructor-led + examination	T−4 to T−3 months	1 day per Champion
Integration & API Workshop	Customer IT / Integration team	Technical workshop (online)	T−4 months	1 day
UAT Guidance Session	UAT participants	Instructor-led briefing	T−2 months	Half day
Go-Live Readiness Check	Champions + Customer IT Lead	Checkpoint meeting	T−14 days	2 hours

Post-Migration Drop-In Clinics	All Authorised Users	Online Q&A (bi-weekly)	T + 0 to T + 90 days	1 hour per session

All transition training sessions shall be recorded and AI-transcribed in accordance with Chapter 6, §6.4.4. Recordings and transcripts shall be published to the Customer's **Per-Client Training Wiki** (https://docs.projectview.wiki/[client]) within five (5) Business Days of each session.

10.7.3 Knowledge-Base Updates

The Provider shall update the following knowledge resources prior to production cutover on the successor version:

(a) **Per-Client Training Wiki:** All module-specific pages, process guides, and FAQ articles updated to reflect successor-version UI, workflows, and terminology.

(b) **Platform Release Centre:** Release notes, deployment guides, and configuration references for the successor version published at .

(c) **In-application guidance:** Contextual tooltips, help links, and AI-assisted prompts updated to reference successor-version functionality.

10.8 Customer Decision: Transition or Cessation

No later than **six (6) months** before the EOL Date (i.e., T−6 months), the Customer shall formally notify the Provider of its election to either:

(a) **Option A — Transition:** Proceed with migration to the successor version. The Provider delivers Migration Services (§10.5), Integration Adoption (§10.6), and Re-Training (§10.7). The subscription continues uninterrupted on the successor version under the existing commercial terms (unless varied by mutual written agreement).

(b) **Option B — Subscription Cessation:** Elect not to transition. The Provider initiates the Subscription Cessation process (§10.9), including data return (§10.10), environment decommissioning (§10.11), and contractual termination (§10.12). The subscription terminates on the EOL Date (or the Extended Support expiry date, if elected).

If the Customer fails to provide written notification by the T−6 deadline, the Provider shall issue a reminder notice. If no response is received within a further thirty (30) calendar days, the Provider shall deem the Customer to have elected **Option A (Transition)**, and Migration Services shall proceed.

10.9 Subscription Cessation Process

Where the Customer elects Option B (Subscription Cessation), the following process shall apply:

Phase	Timing	Activity	Owner
1. Cessation Notice	T−6 months (Customer's election)	Customer provides written notice of intent not to transition. Provider acknowledges receipt within 2 Business Days.	Customer → Account Manager
2. Cessation Planning	T−6 to T−5 months	Provider and Customer agree a Cessation Plan covering: data-export format(s), timeline, contact handover, open-ticket resolution, and environment wind-down schedule.	Account Manager + Cloud Ops Lead

3. Data Export & Return	T−5 to T−2 months	Provider exports all Customer Data in agreed format(s) within 2 Business Days of each valid request (§10.10). Multiple export requests permitted.	DBA + Cloud Ops
4. Customer Validation	T−2 to T−1 month	Customer validates completeness and integrity of exported data. Raises data-completeness objections (if any) within 14 calendar days of receipt.	Customer IT Lead
5. Open-Ticket Resolution	T−3 to T−30 days	Provider resolves all open P1/P2 Incidents. Lower-priority tickets are closed with Customer agreement or documented as unresolved.	Cloud Ops + Account Manager
6. Environment Decommissioning	T = EOL Date	Legacy environment is decommissioned: VM shutdown, database deletion, storage-account purge, encryption-key destruction (§10.11).	Cloud Ops + DBA
7. Decommissioning Certificate	T + 14 days	Provider issues a Decommissioning Certificate confirming all Customer Data has been securely destroyed in accordance with NIST SP 800-88.	CTO → Customer
8. Contractual Termination	T + 30 days	Agreement formally terminates. Surviving clauses (confidentiality, IP, limitation of liability, data-protection residual obligations) continue per §10.12.	Legal / Account Manager

10.10 Data Return

The Customer retains **sole and exclusive ownership** of all Customer Data at all times (Chapter 9, §9.9). Upon Subscription Cessation, the Provider's data-return obligations are as follows:

10.10.1 Export Formats & Delivery

(a) **Standard export formats:** SQL Server backup file (.bak), CSV, JSON, and/or XML. The Customer may request any combination of formats.

(b) **Delivery timeline:** Within two (2) Business Days of receiving a valid written request from the Customer.

(c) **Delivery method:** Encrypted secure transfer via the Customer's designated SFTP endpoint, Azure Blob Storage SAS token, or physical encrypted media (courier-delivered with chain-of-custody documentation).

(d) **Scope of export:** All Customer Data including: master data, transactional data, configuration data, audit trails, change-tracking records, document attachments (blob storage), and application-generated reports.

(e) **Multiple exports:** The Customer may request multiple exports during the cessation period. Each request shall be fulfilled within 2 Business Days.

10.10.2 Data-Return Validation

Following each data export:

(a) **Integrity hash:** The Provider shall deliver a SHA-256 cryptographic hash of each exported data set, enabling the Customer to verify data integrity upon receipt.

(b) **Row-count certificate:** The Provider shall deliver a row-count certificate listing the record count for each table/entity in the export, cross-referenced against the production database at the point-in-time of export.

(c) **Validation window:** The Customer has fourteen (14) calendar days from receipt to raise a data-completeness or integrity objection. The Provider shall remediate and re-export within two (2) Business Days of any valid objection.

(d) **Deemed acceptance:** If the Customer does not raise an objection within the 14-day validation window, the export shall be deemed accepted.

10.10.3 Cost of Data Return

Data return within the standard scope (export in standard formats via secure digital transfer) is **included in the subscription at no additional cost**. The following services are available at additional cost on a time-and-materials basis:

(a) Transformation of exported data into non-standard formats (e.g., target-system-specific schema transformations for ingestion into a successor ERP).

(b) Physical media preparation and courier delivery.

(c) Extended data-export window beyond the standard cessation timeline.

(d) Technical advisory on data mapping, migration scripting, or ETL design for the Customer's successor system.

10.11 Environment Decommissioning

Upon completion of data return and expiry of the Customer's validation window, the Provider shall decommission the Customer's dedicated private sovereign environment:

(a) **Virtual machine shutdown:** All Customer VMs (production and staging) are stopped, disk images deleted, and compute resources deallocated.

(b) **Database destruction:** All SQL Server databases (production, staging, backups) are permanently deleted. Transaction logs and backup files in Azure Backup Vault are purged.

(c) **Storage-account purge:** All Azure Blob Storage containers, file shares, and table storage associated with the Customer are permanently deleted, including GRS-replicated copies in the secondary region.

(d) **Encryption-key destruction:** All Customer-specific encryption keys, secrets, and certificates in Azure Key Vault are purged (purge-protection override authorised by CTO).

(e) **Network cleanup:** Virtual networks, NSGs, public IP addresses, DNS records, and SSL/TLS certificates associated with the Customer are deprovisioned.

(f) **CMDB update:** All Customer-related configuration items are marked as decommissioned in the Provider's CMDB.

(g) **Secure data destruction:** All data destruction is performed in accordance with NIST SP 800-88 (Guidelines for Media Sanitisation). Azure's cryptographic erasure ensures that data on decommissioned storage is irrecoverable.

NIST SP 800-88 Rev. 1: Guidelines for Media Sanitization

Azure Data Destruction

10.12 Surviving Obligations

The following obligations survive the termination or expiry of the Framework and shall continue in full force and effect:

(a) **Confidentiality:** Mutual confidentiality obligations survive for five (5) years from the date of termination (Chapter 8, §8.11).

(b) **Intellectual Property:** All intellectual-property rights and licence restrictions survive indefinitely.

(c) **Data-protection residual obligations:** Privacy obligations under Chapter 7 survive with respect to any Personal Data retained by the Provider pursuant to a legal or regulatory obligation (Chapter 7, §7.13).

(d) **Limitation of liability:** Liability caps and exclusions continue to apply to claims arising from events during the Subscription Term.

(e) **Dispute resolution:** The governing law and dispute-resolution provisions continue to apply to any claim arising out of or in connection with the Framework.

(f) **Audit rights:** The Customer's right to audit data-destruction compliance survives for twelve (12) months following the date of the Decommissioning Certificate.

10.13 Extended Support Option

Consistent with the Extended Support models offered by SAP (Extended Maintenance), Oracle (Sustaining Support), IFS (Extended Maintenance), and Infor (Extended Maintenance), the Provider offers an optional **Extended Support** period for Customers who require additional time to complete their transition:

(a) **Availability:** Extended Support must be requested in writing no later than sixty (60) calendar days before the EOL Date.

(b) **Duration:** Up to twelve (12) months post-EOL Date, in quarterly increments.

(c) **Scope:** P1 and P2 Incident resolution and critical security patches only. No feature development, no new Change Requests, no new module activations.

(d) **Pricing:** Extended Support is charged at a premium of twenty percent (20%) above the then-current ARR, payable quarterly in advance.

(e) **Termination:** Extended Support terminates automatically at the end of the elected period. All Subscription Cessation provisions (§10.9–§10.12) apply upon Extended Support expiry.

10.14 Roles & Responsibilities (RACI Matrix)

The following RACI matrix allocates responsibilities for key EOL activities across Provider and Customer roles:

Activity	CTO	Cloud Ops Lead	Account Mgr	DBA Lead	Customer IT Lead	Customer Champions
EOL Announcement issuance	A	I	R	I	I	I
Migration Readiness Assessment	A	R	C	R	C	I
Integration Impact Assessment	I	R	C	C	R	I

Data-migration execution	I	R	I	R	C	I
Data-migration integrity verification	I	R	I	R	C	I
Transition Training Programme delivery	I	C	R	I	C	R
Champion Re-Certification	I	I	R	I	C	R
Knowledge-base updates	I	R	C	I	I	C
Integration re-engineering	I	R	I	C	R	I
UAT on successor version	I	C	C	C	R	R
Cutover planning & execution	A	R	C	R	C	I
Customer decision (Transition / Cessation)	I	I	C	I	R	I
Data-export fulfilment	I	R	C	R	R	I
Data-return validation	I	I	I	I	R	I
Environment decommissioning	A	R	I	R	I	I
Decommissioning Certificate issuance	R	C	I	C	I	I
Extended Support management	A	R	C	R	I	I

Legend: **R** = Responsible · **A** = Accountable · **C** = Consulted · **I** = Informed.

10.15 Process Register

The following process register catalogues all formal processes defined in this chapter.

Process ID	Process Name	Trigger	Handler	Approver	Outcome	Section Ref.
P-10.01	EOL Announcement	Product roadmap decision to end-of-life a major version	Account Manager	CTO	Written EOL Announcement delivered to all affected Customers ≥ 12 months before EOL Date.	§10.4

P-10.02	Migration Readiness Assessment	EOL Announcement issued (T−11 months)	Cloud Ops + DBA	CTO	Customer-specific impact assessment and preliminary migration plan delivered.	§10.4
P-10.03	Integration Impact Assessment	EOL Announcement issued (within 30 days)	Cloud Ops Lead	CTO	API compatibility analysis, integration inventory, customisation registry, and effort estimate delivered.	§10.6.1
P-10.04	Training Needs Re-Assessment	EOL Announcement issued (within 60 days)	Account Manager	CTO	Transition Training Plan annexed to Migration Plan.	§10.7.1
P-10.05	Data Migration Execution	Migration Plan approved and Staging Environment provisioned	DBA + Cloud Ops	Cloud Ops Lead	Customer Data migrated; integrity verified; rehearsal(s) completed.	§10.5.1
P-10.06	Migration Integrity Verification	Data migration rehearsal or production cutover completed	DBA + Cloud Ops	Cloud Ops Lead	Pre/post hash comparison passed; row-count reconciliation complete; integrity report issued.	§10.5.2
P-10.07	Integration Re-Engineering	Integration classified as ‘requires re-engineering’ in Impact Assessment	Cloud Ops	Cloud Ops Lead	Integration updated, tested, and validated on successor version.	§10.6.2
P-10.08	Transition Training Delivery	Transition Training Plan approved	Account Manager + Trainers	Cloud Ops Lead	All scheduled training sessions delivered; recordings published to Wiki.	§10.7.2
P-10.09	Champion Re-Certification	Transition Training Programme scheduled	Account Manager	CTO	Champions pass successor-version examination; certificates issued.	§10.7.2
P-10.10	UAT on Successor Version	Migration rehearsal passed; training completed	Customer IT Lead + Champions	Customer	Written Customer sign-off on successor version obtained.	§10.5.2

P-10.11	Production Cutover	UAT sign-off received; cutover window agreed	Cloud Ops + DBA	CTO	Production environment running successor version; rollback available for 72 hours.	§10.5.1
P-10.12	Hypercare Support	Production cutover completed	Cloud Ops + DBA	Account Manager	30-day hypercare period delivered; stabilisation confirmed.	§10.5.1
P-10.13	Customer Cessation Election	Customer written notice of intent not to transition	Account Manager	CTO	Cessation Plan agreed; data-export schedule confirmed.	§10.8
P-10.14	Data Export & Return	Customer valid written request during cessation period	DBA + Cloud Ops	Account Manager	Customer Data exported in agreed format within 2 Business Days.	§10.10
P-10.15	Data-Return Validation	Data export delivered to Customer	Customer IT Lead	Customer	Customer confirms completeness within 14-day validation window (or deemed accepted).	§10.10.2
P-10.16	Environment Decommissioning	Data-return validation window expired; EOL Date reached	Cloud Ops + DBA	CTO	All Customer resources destroyed per NIST SP 800-88; CMDB updated.	§10.11
P-10.17	Decommissioning Certificate	Environment decommissioning completed	CTO	CTO	Decommissioning Certificate issued to Customer within 14 days.	§10.11
P-10.18	Extended Support Activation	Customer written request ≥60 days before EOL Date	Cloud Ops Lead	CTO	Extended Support Addendum executed; P1/P2 support continued for elected period.	§10.13

10.16 Process Flow Schematic

The following nine-stage lifecycle illustrates the end-to-end flow of version transition and subscription cessation:

① EOL Announcement & Communication → ② Readiness & Impact Assessment → ③ Customer Decision (Transition / Cessation)

↓

TRANSITION PATH: ④ Migration & Re-Engineering → ⑤ Re-Training & Change Management → ⑥ UAT & Production Cutover

↓

CESSATION PATH: ⑦ Data Export & Return → ⑧ Environment Decommissioning → ⑨ Contractual Termination

Stage ① EOL Announcement & Communication: The Provider issues the formal EOL Announcement ≥12 months before the EOL Date, initiating the structured communication programme (§10.4). All Customers receive written notice, and the Account Manager schedules the Migration Readiness Assessment (P-10.01).

Stage ② Readiness & Impact Assessment: The Provider delivers the Migration Readiness Assessment, Integration Impact Assessment, and Training Needs Re-Assessment within 60 days of the EOL Announcement (P-10.02, P-10.03, P-10.04).

Stage ③ Customer Decision: At T−6 months, the Customer formally elects to Transition (Option A) or Cessation (Option B). Default is Transition if no response within 30 days of reminder (P-10.13).

Stage ④ Migration & Re-Engineering (Transition Path): Data migration, configuration migration, and integration re-engineering are executed in the Staging Environment with ≥2 rehearsals (P-10.05, P-10.06, P-10.07).

Stage ⑤ Re-Training & Change Management (Transition Path): The Transition Training Programme is delivered: What's New briefings, hands-on workshops, Champion re-certification, and knowledge-base updates (P-10.08, P-10.09).

Stage ⑥ UAT & Production Cutover (Transition Path): Customer conducts UAT on successor version. Written sign-off triggers production cutover. 30-day Hypercare period follows (P-10.10, P-10.11, P-10.12).

Stage ⑦ Data Export & Return (Cessation Path): The Provider exports all Customer Data within 2 Business Days of each valid request. Multiple exports permitted. Integrity hash and row-count certificate delivered with each export (P-10.14, P-10.15).

Stage ⑧ Environment Decommissioning (Cessation Path): Upon validation-window expiry and EOL Date, the Provider destroys all Customer resources per NIST SP 800-88 and issues a Decommissioning Certificate (P-10.16, P-10.17).

Stage ⑨ Contractual Termination (Cessation Path): The Framework formally terminates 30 days post-decommissioning. Surviving obligations (confidentiality, IP, data protection, liability, audit rights) continue per §10.12 (P-10.18 if Extended Support was active).

11 Commercial Terms, Pricing & Payment

11.1 Overview & Purpose

This chapter establishes the commercial framework governing the DANAOS ProjectVIEW ERP SaaS subscription, including the Enterprise License Agreement (ELA), the flexible subscription model, pricing structure, Annual Recurring Revenue (ARR) calculation, invoicing cadence, payment obligations, taxes, price-escalation mechanisms, and financial remedies. All monetary amounts referenced in this Framework are exclusive of applicable taxes unless expressly stated otherwise.

The commercial model is based on an **Enterprise License Agreement (ELA)** which binds the Customer to ProjectVIEW ERP enrolment for a minimum subscription commitment (the "Bind-ing Period"). The ELA is designed to provide the Customer with predictable, transparent pricing tied directly to value delivered, while ensuring the Provider maintains sustainable investment in platform development, infrastructure, and support services.

All fees, charges, and financial obligations specified in this chapter are subject to the Commercial Contract (§1.3 — Order of Precedence). Where the Commercial Contract specifies terms that differ from this chapter, the Commercial Contract shall prevail.

11.2 Scope

This chapter covers:

(a) **Licensing model:** Universal/Concurrent User licensing, Intranet and Extranet user classification, module-based entitlements, standalone module provisions, and environment provisioning.

(b) **Flexible Subscription Model:** The usage-based model allowing the Customer to ADD or REMOVE User Licences within each Billing Period, subject to minimum commitments.

(c) **Pricing structure:** Annual subscription fees for modules, per-user pricing tiers by volume band, Addon/Portal/Connector pricing, and professional service fees.

(d) **Annual Recurring Revenue (ARR):** Calculation methodology, pro-rata adjustments for mid-term additions, and ARR recalculation triggers.

(e) **Invoicing & payment:** Billing cadence, milestone-based services payments, subscription licence payments, accepted payment methods, and overdue-payment consequences.

(f) **Price escalation:** Annual adjustment mechanisms based on the official inflation rate of the applicable jurisdiction and cap provisions.

(g) **Taxes & duties:** Responsibility for VAT, Withholding Tax (WHT), bank transfer costs, customs duties, and cross-border levies.

(h) **Financial remedies:** Penalties for Provider SLA non-compliance, late-payment interest, and disputed-invoice procedures.

(i) **Audit rights:** Licence-compliance auditing, usage verification, and true-up procedures.

This chapter does not cover implementation project fees in detail (addressed in the Commercial Contract, Statement of Work, and Cost of Services schedules) or Extended Support premium pricing (see Chapter 10, §10.13).

11.3 Licensing Model

11.3.1 Enterprise License Agreement (ELA)

ProjectVIEW ERP is licensed under an **Enterprise License Agreement (ELA)** which establishes the legal instrument governing the use of the Software. ProjectVIEW ERP is an enterprise-grade, centralised software suite of applications designed to function as One Integrated System/Platform. The ELA binds the Customer to ProjectVIEW ERP enrolment for a minimum subscription of the number of Billing Periods specified in the Commercial Contract (the "Bind-ing Period").

11.3.2 Universal/Concurrent User Licensing

The Platform is licensed on a **Universal/Concurrent User per Device** basis. This proprietary commercial licensing model is based on the metrics of Universal Users and Concurrent Users who share a finite amount of licences and may run the Software simultaneously from one device (floating licence).

A **Universal User** has direct access to one or more specific module(s)/device based on each User's login credentials as defined by the Customer's System Administrator, and indirect permission to features/data of another module that are required for the User to attain comprehensive operational knowledge as defined natively by the business logic of the System and the prerequisites of each module.

A **Concurrent User** is a named user who accesses the application at any given time simultaneously (per maximum concurrent users, ever). Concurrent Users are "floating users" counted per each device that is logged in: Workstation, Tablet, or Mobile device.

The minimum purchase commitment is **twenty (20) Universal/Concurrent User Licences** as specified in the Commercial Contract.

11.3.3 Intranet and Extranet User Classification

The System distinguishes between two classes of Users:

(j) **Intranet Users:** Company-authorised individuals (e.g., white-collar employees) who have access to the Customer's organisation's digital assets and are authorised to utilise ProjectVIEW ERP with enhanced features and access rights to perform task allocations, approvals, and access resources as defined by their role and the access permissions set by the Customer's IT System Administrator.

(k) **Extranet Users:** Company-authorised labour (blue-collar employees), certified subcontractors, suppliers, vendors, and external consultants who have limited access to the Customer's organisation's digital assets, predominantly via ProjectVIEW ERP dedicated Portals. Extranet Users are given login access with limited features and rights to perform specific tasks, upload personal data, quotations, certifications, and complete operational processes as defined by their role and the access permissions set by the Customer's IT System Administrator.

Extranet Users access the System through specialised gateways or interfaces (Portals) accessed through client-specific URL subdomains, providing access based on their company relationship and current status with the Customer. These Portals facilitate transactions for users—whether labour, external vendors, subcontractors, consultants, or other suppliers—allowing them to interact efficiently with the ProjectVIEW ERP modules.

11.3.4 Module-Based Entitlements

The Customer's subscription includes access to the specific ProjectVIEW ERP modules, Addons, Connectors, and Portals identified in the Commercial Contract. The System comprises Office Modules, Site Applications, Addons/Connectors, and Portals as follows:

11.3.4.1 Office Modules

Module Code	Module Name	Category
PV_00	Core Module (incl. DANAOS Business Analytics, Document Management)	Core
PV_01	Budget Estimation – Bidding (Estimation and Tendering)	Commercial
PV_02	Planning – Scheduling (Production and Fabrication Planning/Control)	Operations
PV_03	Progress Monitoring (Budgeting and Cost Control)	Commercial
PV_04	Document Management	Core
PV_05	Quantity Surveying – Cost Engineering (Subcontractors Management)	Commercial
PV_06	Construction Methods – Resources (Machinery & Maintenance Management)	Operations
PV_07	Contracts Administration (HRMS & Payroll – Labour Management)	Admin
PV_08	Procurement – Materials Management (Warehouse & Materials Management, Materials Cost DB)	Supply Chain
PV_09	Equipment – Fleet Management	Operations
PV_10	Customers Account Receivables (Accounting and Finance, Petty Cash, e-Invoicing)	Financial

11.3.4.2 Site Applications

In addition to Office Modules, the Platform includes Site/Yard Applications accessible by Intranet Users operating in the field. These include but are not limited to: Resources Planning/Levelling, Subcontractor Certifications Submittal, Site/Yard Item Request (SIR), Site/Yard Internal Order, Work Order Execution/Monitoring, Site/Yard Progress of Works, Site/Yard Certifications Approvals, Customer Contract Certification, Machinery Request/Monitoring, and Request for Inspection (RFI). Access to Site Applications is included within the Office Module licensing and is governed by the same Universal/Concurrent User metrics.

11.3.4.3 Addons, Connectors & Portals

Addons and Connectors are application tools (utilities) related to and integrated with one or more ProjectVIEW ERP Modules that supplement dedicated processes and operations. Portals act as specialised gateways providing Extranet Users with access based on their company relationship with the Customer. Addon/Connector/Portal licences are priced independently of the core module subscription as specified in the Commercial Contract:

Addon / Portal / Connector	Licensing Metric	User Scope
DANAOS Business Analytics	Named User (Minimum Intranet Users as per Commercial Contract)	Intranet
Document Management	Named User (included with core subscription)	Intranet
ExtraAXION 2D QTO	Named User	Intranet
BIM Connector	Per Connector	System-Level
Oracle P6 or MS Project Connector	Per Connector	System-Level

Subcontractor Certifications Submittal	Named Extranet User (Unlimited)	Extranet
Vendors Registration Marketplace	Named Extranet User (Unlimited)	Extranet
eRFQ for Suppliers/SubContractors & e-Auctioning	Named Extranet User (Unlimited)	Extranet
Employee Self-Service Portal	Named Intranet User (Unlimited)	Intranet
Job Recruiting Portal	Named Extranet User (Unlimited)	Extranet
Customer Portal (Approvals, Change Mgmt, RFIs/Certs)	Named User (Unlimited)	Both

Where an Addon or Portal specifies “Unlimited” user scope, the subscription fee is a flat annual fee regardless of the number of users accessing that Addon or Portal, as specified in the Commercial Contract.

11.3.5 Standalone Module Provisions

Although ProjectVIEW ERP is intended for Universal Users as **One Integrated System**, the Customer may purchase licences for Standalone/Independent Modules subject to the following provisions:

(a) **Module prerequisites:** Certain modules may not be operated or purchased as standalone due to required features deriving from other modules (e.g., Budgeting and Cost Control requires Estimation and Tendering as a prerequisite). The Commercial Contract shall specify applicable module dependencies.

(b) **Universal user count alignment:** When purchasing standalone modules, the number of Concurrent Users required for the module with the highest user count shall apply to all other modules purchased or activated subsequently. The minimum for standalone module licensing is ten (10) Concurrent User Licences.

11.3.6 Flexible Subscription Model

The System operates under a **Flexible Subscription Model (Usage-Based Model)** whereby the Customer may ADD or REMOVE User Licences within each Billing Period based on operational requirements. This scalable model permits the Customer to adjust User Licence counts, always maintaining as a minimum the number of initial User Licences contracted in the Commercial Contract (the “Minimum Licence Commitment”).

User Licence additions take effect upon the Provider’s written acknowledgement and are invoiced pro-rata for the remaining duration of the current Billing Period. User Licence removals take effect at the commencement of the next Billing Period, subject to the Minimum Licence Commitment.

11.3.7 Environment Provisioning

The subscription includes the provisioning and maintenance of a **dedicated private sovereign environment** for each Customer on DANAOS Cloud (Microsoft Azure), operating in the closest available datacenter to the Customer’s location for minimum latency and higher response time, as described in Chapter 2, §2.3. During the implementation phase, two (2) environments are provisioned: Development/Sandbox and Production. Post Go-Live, the Development/Sandbox environment is re-designated as Staging (Chapter 4, §4.3).

The cost of setting up, fine-tuning, providing the required Commercial-Off-The-Shelf Software (COTS) licences, data integrity, backup, data and operational security, and generally maintaining the required infrastructure and COTS Software (Operating Systems, Databases, Antivirus, etc.) solely relies on the Provider as part of the SaaS subscription.

11.4 Pricing Structure

11.4.1 Annual Subscription Fee — Modules

The **Annual Subscription Fee** for ProjectVIEW ERP modules is calculated based on the Universal/Concurrent User licensing model. The subscription fee is determined by the volume band applicable to the Customer's total Concurrent User count, as specified in the Commercial Contract:

Volume Band	Concurrent Users	Pricing Characteristic
Band 1	Minimum – 20 Licences	Base per-user annual rate as specified in Commercial Contract
Band 2	21 – 30 Licences	Reduced per-user rate; volume discount applied
Band 3	31 – 50 Licences	Further reduced per-user rate
Band 4	51 – 100 Licences	Enterprise volume rate
Band 5	> 100 Licences	Maximum volume discount; bespoke pricing per Commercial Contract negotiation

The per-user annual rate for each volume band is specified in the Commercial Contract. Band placement is determined at the commencement of each Billing Period based on the total licensed Concurrent User count. If the Customer's user count crosses a band boundary mid-term due to additions, the new band rate applies from the next Billing Period unless the Commercial Contract specifies immediate band adjustment.

11.4.2 Addon, Connector & Portal Subscription Fees

Addons, Connectors, and Portals are priced separately from the core module subscription. Each Addon/Connector/Portal has its own licensing metric (Named User, Named Extranet User, Per Connector, or flat annual fee for unlimited users), as specified in the Commercial Contract.

Upon acceptance by the Customer, additional Addons, Connectors, or Portals required after the initial Contract shall be charged based on the Provider's published Addon/Portal Licensing Model Metric as specified in the Commercial Contract or applicable Module Activation Amendment.

11.4.3 Cost of Professional Services

Professional services required for setting up, customising, configuring the Software, and training the Customer's personnel are priced on a Man-Day basis by service type. The Cost of Services is specified in the Commercial Contract and includes:

Service Type	Metric	Scope
Project Management	Man Day	Coordination of daily tasks, consulting, monitoring deliverables, daily meetings, change requests, and Customer enquiries. The Provider requires a counterpart Project Manager from the Customer (at least 1 PM per 20 Users).
System Setup – Installation	Man Day	Assisting the Customer to set up the System on DANAOS Cloud; database and app server configuration, SSO, Active Directory, and installation on main workstations.
Data Migration/Import	Man Day	Providing Master Data Templates, main data cleansing, importing historical data into the System, testing data integrity and process consistency.
Configuration	Man Day	Setup of Company, Departments, Projects, Users, Roles, Workflows, Currencies, Templates, and other parameters.

Training/Consulting ProjectVIEW	Man Day	Remote and hands-on training for the number of Users, Wiki access, manuals, and support documentation.

The per-Man-Day rate for each service type is specified in the Commercial Contract. All services durations are managed and mutually agreed with the Customer's Project Manager.

11.4.4 Additional / Optional Services

The following services may be procured during the subscription period at rates specified in the Commercial Contract or upon quotation by the Provider:

Service Type	Metric	Provision
Custom Business Analytics Dashboards	Per Dashboard	ProjectVIEW ERP includes pre-initialised dashboards (one per module); custom dashboards available upon request.
Custom Reports	Per Report	ProjectVIEW ERP includes 150+ standard reports; custom reports developed upon request.
Extra Training and/or Consulting	Man Day	Additional training beyond the initial programme; new setup and installations.
Integration and/or Customisation Services	Man Day	Connectivity with third-party systems; custom feature development subject to business analysis.
Source Code Escrow — Escrow Agent fees	Annual	Pass-through at cost; borne by Customer (Chapter 9, §9.14.4).
Extended Support (post-EOL)	Annual	20% premium above current ARR (Chapter 10, §10.13).
On-Site Visits (accommodation)	Per Visit	Accommodation cost mutually agreed; level of accommodation is 4+ star hotels; paid by the Customer based on duration of stay.

Note: Based on the Provider's prerogative, the Provider may elect not to charge extra for customisation services where such customisations contribute to the enrichment of ProjectVIEW ERP's standard feature set.

11.4.5 Total Cost of Ownership

The Total Cost of Ownership (TCO) for the initial contract period comprises:

(a) **Recurring — Annual Subscription Licences:** The aggregate of module subscription fees plus Addon/Connector/Portal subscription fees, as specified in the Commercial Contract, payable annually.

(b) **One-Off — Cost of Services:** The aggregate of professional services fees for implementation, configuration, data migration, and training, as specified in the Commercial Contract, payable per the milestone-based payment schedule (§11.7).

Any discount applied to the TCO shall be specified in the Commercial Contract. All costs are denominated in the currency specified in the Commercial Contract and are exclusive of VAT, WHT, and bank transfer charges.

11.5 Annual Recurring Revenue (ARR)

11.5.1 ARR Definition & Calculation

The **Annual Recurring Revenue (ARR)** is the annualised value of the Customer's subscription, calculated as the sum of:

(a) **Module subscription fees** (the aggregate of per-user annual fees across all licensed modules within the applicable volume band);

(b) **Addon/Connector/Portal subscription fees** for all active Addons, Connectors, and Portals; and

(c) **Any recurring ancillary fees** expressly designated as ARR-contributing in the Commercial Contract.

ARR **excludes** one-off implementation/services fees, bespoke customisation charges, Extended Support premiums, Escrow Agent fees, accommodation costs, and any non-recurring professional-service fees.

11.5.2 Pro-Rata Adjustments

When User Licences, Addons, or modules are added mid-term, the additional fees are calculated **pro-rata** from the Activation Date to the end of the current Billing Period:

Pro-Rata Fee = (Annual Fee ÷ 365) × Remaining Days in Billing Period

The pro-rata fee is invoiced within fifteen (15) Business Days of the Activation Date and is payable in accordance with the standard payment terms (§11.7).

New User Licences and newly activated modules receive the **same SLA metrics, support entitlements, and performance commitments** as existing users and modules from the Activation Date (Chapter 3, §3.1). The ARR is recalculated to include the additional fees from the next Billing Period renewal.

11.5.3 ARR Recalculation Triggers

The ARR shall be recalculated upon the occurrence of any of the following:

(a) **User additions:** User Licences added via the Flexible Subscription Model (written request and Provider acknowledgement).

(b) **User reductions:** User Licences removed at Billing Period renewal (Minimum Licence Commitment applies per §11.5.4).

(c) **Module/Addon activation:** New modules or Addons/Portals activated via Module Activation Amendment.

(d) **Module/Addon deactivation:** Modules or Addons deactivated at Billing Period renewal (subject to minimum commitment per §11.5.4).

(e) **Volume band migration:** Customer's user count crosses a volume band boundary at Billing Period renewal.

(f) **Price escalation:** Annual price adjustment applied per §11.6.

11.5.4 Minimum Commitment

The Customer commits to a minimum ARR for the duration of the Binding Period as specified in the Commercial Contract (the "**Minimum Commitment**"). The Minimum Commitment is anchored to the initial number of User Licences contracted in the Commercial Contract. Reductions in User Licences or module/Addon deactivations at Billing Period renewal shall not reduce the ARR below the Minimum Commitment.

If the Customer's actual usage falls below the Minimum Commitment, the Customer remains liable for the Minimum Commitment amount. The Minimum Commitment is subject to annual price escalation per §11.6.

11.6 Price Escalation

11.6.1 Annual Adjustment

ProjectVIEW ERP Annual Subscription Licences and any Maintenance and Support Contracts are subject to a yearly adjustment according to the **official inflation rate** of the jurisdiction specified in the Commercial Contract (the "Index Jurisdiction"). Unless the Commercial Contract specifies a fixed-price term or an alternative escalation mechanism, the Provider may increase the subscription fees at each Billing Period renewal by the greater of:

(a) **Inflation Index:** The official inflation rate of the Index Jurisdiction over the twelve (12) months preceding the renewal date; or

(b) **Floor rate:** Three percent (3%) per annum.

11.6.2 Cap

The annual price increase shall not exceed **seven percent (7%)** of the prior-year subscription fees (the "Price Escalation Cap"), regardless of the inflation index movement.

11.6.3 Notice

The Provider shall provide the Customer with written notice of any price increase at least ninety (90) calendar days before the commencement of the next Billing Period. The notice shall specify the new fees, the applicable escalation factor, and the calculation methodology.

11.6.4 Fixed-Price Terms

Where the Commercial Contract specifies a fixed-price Binding Period, the subscription fees shall remain unchanged for the duration of the Binding Period. Price escalation shall apply from the first Renewal Term unless otherwise agreed in the Commercial Contract.

11.7 Invoicing & Payment

11.7.1 Services Payment Schedule

Unless the Commercial Contract specifies an alternative payment schedule, Professional Services fees (one-off Cost of Services) shall be invoiced on a milestone basis as follows:

Milestone	Percentage	Trigger
Milestone 1	As per Commercial Contract	Upon signing of the Contract
Milestone 2	As per Commercial Contract	Upon completion of Master Data import
Milestone 3	As per Commercial Contract	Upon finishing Training

The specific percentage allocation for each milestone is specified in the Commercial Contract. For accommodation and additional services such as integration and customisation, a separate invoice shall be issued upon the Customer's prior written approval, received via email, explicitly confirming that these services incur an extra cost.

11.7.2 Subscription Licence Payments

Annual Subscription Licence fees are payable **in full upon signing of the Contract** and upon commencement of each subsequent Billing Period, unless the Commercial Contract specifies an alternative billing cadence.

(a) **Annual billing (default):** A single invoice for the full Billing Period subscription fee, issued upon signing or thirty (30) calendar days before the commencement of each renewal Billing Period.

(b) **Pro-rata invoices:** Mid-term User Licence or Addon additions invoiced within fifteen (15) Business Days of the Activation Date.

(c) **Ancillary service invoices:** Issued upon completion of the applicable service or milestone as defined in the Commercial Contract or Statement of Work.

11.7.3 Invoice Requirements

Each invoice shall contain all information necessary, including but not limited to:

(l) Contract Reference Number

(m) The Provider's name and registered address

(n) The Subscription/Billing Period covered

(o) Bank details for electronic transfer

(p) A separate calculation of VAT or WHT (if required)

(q) An adequate description of the type of Services or Licences provided

11.7.4 Payment Terms

All invoices are payable within **thirty (30) calendar days** of the invoice date ("Payment Due Date") unless the Commercial Contract specifies alternative payment terms. Payment shall be made by electronic bank transfer to the Provider's designated bank account as specified on the invoice.

11.7.5 Overdue Payments

If the Customer fails to make any payment by the Payment Due Date:

(a) **Interest:** The Provider may charge interest on the overdue amount at the rate of two percent (2%) per annum above the base rate of the European Central Bank (ECB), calculated daily from the Payment Due Date until the date of actual payment.

(b) **Suspension notice:** If payment remains outstanding for more than sixty (60) calendar days after the Payment Due Date, the Provider may issue a written suspension notice giving the Customer thirty (30) calendar days to remedy the default.

(c) **Service suspension:** If the Customer fails to remedy the default within the thirty-day (30-day) cure period, the Provider may suspend the Customer's access to the Platform. Suspension does not relieve the Customer of its obligation to pay the outstanding fees. The Customer has total capacity and authority to ProjectVIEW ERP licences and Support/Maintenance Services only upon paying the Annual Subscription Cost of agreed/amended Software Licences.

(d) **Termination:** If payment remains outstanding for more than one hundred and twenty (120) calendar days after the Payment Due Date, the Provider may terminate the Framework upon

thirty (30) calendar days' written notice, subject to the data-return obligations of Chapter 10, §10.9–10.11.

Note: The Provider shall not suspend access to the Platform while a bona fide dispute is being resolved in accordance with §11.9.

11.7.6 Currency

All fees and charges shall be denominated in the currency specified in the Commercial Contract. Where the Commercial Contract does not specify a currency, all amounts shall be denominated in United States Dollars (USD). The Customer shall bear the cost of bank transfer charges, exchange-rate fluctuations for cross-border payments, and any charges levied by intermediary banks, unless otherwise agreed in the Commercial Contract.

11.8 Taxes & Duties

11.8.1 General Principle

All fees specified in this Framework and the Commercial Contract are exclusive of applicable taxes, duties, levies, and government-imposed charges ("Taxes") unless expressly stated as tax-inclusive. When applicable, the Customer pays the cost of VAT, WHT, and/or bank transfer charges.

11.8.2 Value Added Tax (VAT) / Goods & Services Tax (GST)

Where the supply of the Services is subject to VAT, GST, or equivalent consumption tax in the applicable jurisdiction, the Provider shall add the applicable tax to each invoice. The Customer shall pay the tax amount in addition to the quoted fees. The Provider shall issue VAT-compliant invoices in accordance with the tax regulations of the invoicing jurisdiction.

11.8.3 Withholding Tax (WHT)

If the Customer is required by law to deduct or withhold any tax from payments to the Provider, the Customer shall:

(a) **Gross-up:** Increase the payment amount such that the net amount received by the Provider after withholding equals the full invoiced amount; or

(b) **Certificate:** Provide the Provider with official tax-withholding certificates within thirty (30) calendar days of the relevant payment to enable the Provider to claim credit or relief.

The Parties shall co-operate in good faith to minimise withholding-tax exposure, including by applying for relief under applicable double-taxation treaties.

11.8.4 Customs & Digital Services Taxes

As the Platform is delivered as a SaaS service, no physical goods are imported. In the event that any jurisdiction imposes customs duties, digital-services taxes, or equivalent charges on SaaS services, such charges shall be borne by the Customer unless the Commercial Contract expressly provides otherwise.

11.9 Disputed Invoices

If the Customer disputes any invoice or portion thereof, the Customer shall:

(a) **Notify:** Provide written notice of the dispute to the Provider within fifteen (15) Business Days of the invoice date, specifying the disputed amount, the reason for the dispute, and any supporting documentation.

(b) **Pay undisputed portion:** Pay the undisputed portion of the invoice by the Payment Due Date.

(c) **Resolution:** The Parties shall negotiate in good faith to resolve the dispute within thirty (30) calendar days of the dispute notice. If the dispute is not resolved within this period, either Party may escalate the matter through the governance framework (§11.14) or the dispute resolution provisions of the Framework.

During the dispute-resolution period, the Provider shall not suspend access to the Platform, charge late-payment interest on the disputed amount, or initiate termination proceedings in respect of the disputed amount.

11.10 Financial Remedies & Penalties

11.10.1 SLA Non-Compliance Penalties

Where the Provider fails to meet the Service Level Objectives specified in Chapter 3, the Customer is entitled to **Penalties** (not "Service Credits") calculated as a percentage of the total ARR. The penalty regime is defined in Chapter 3, §3.8 and is summarised below for cross-reference:

SLA Breach Category	Penalty (% of ARR)	Measurement Period	Cap
Availability < 99.9%	Per schedule in §3.8	Monthly	25% of monthly ARR
RPO breach (> 15 min data loss)	Per schedule in §3.8	Per incident	Cumulative cap per §3.8
RTO breach (> 4 hrs recovery)	Per schedule in §3.8	Per incident	Cumulative cap per §3.8
P1 response-time breach	Per schedule in §3.8	Per incident	Cumulative cap per §3.8

Penalties are applied as **credits against future invoices** unless the Customer requests a cash refund. The aggregate penalties payable by the Provider in any Billing Period shall not exceed the annual-cap specified in Chapter 3, §3.8. Penalties constitute the Customer's sole and exclusive financial remedy for SLA non-compliance and do not limit claims for general breach of contract.

11.10.2 Penalty Claim Process

The Customer shall submit penalty claims within thirty (30) Business Days of the end of the measurement period in which the breach occurred. Claims must be submitted through the Embedded Ticketing System and must reference the applicable SLA metric, the measured performance, and the calculated penalty amount. The Provider shall validate and respond to each claim within fifteen (15) Business Days.

11.11 Licence-Compliance Auditing

11.11.1 Audit Right

The Provider reserves the right to audit the Customer's use of the Platform to verify compliance with the Universal/Concurrent User licensing terms of this Framework. Audits may be conducted **no more than once per Billing Period**, upon a minimum of thirty (30) calendar days' written notice.

11.11.2 Audit Procedure

Audits shall be conducted as follows:

(a) **Self-certification:** The Provider issues a Licence Usage Declaration form. The Customer completes and returns it within fifteen (15) Business Days, certifying the number of active Universal/Concurrent Users and licensed modules/Addons.

(b) **System validation:** The Provider may verify the self-certification against the Platform's authentication logs and Active Directory integration records. All validation is performed within the Provider's systems; no access to the Customer's internal systems is required.

(c) **Discrepancy resolution:** If the audit reveals that the Customer's actual usage exceeds the licensed entitlements, the Provider shall issue a True-Up Notice specifying the excess usage and the applicable fees.

11.11.3 True-Up

Upon receipt of a True-Up Notice, the Customer shall:

(a) **Regularise:** Execute a User Licence Amendment or Module Activation Amendment to bring usage into compliance within thirty (30) calendar days.

(b) **Back-pay:** Pay the pro-rata fees for the excess usage from the date the excess commenced (or the start of the current Billing Period if the commencement date cannot be determined) to the date of regularisation.

If the audit reveals that the Customer's actual usage is within the licensed entitlements, the Provider shall bear the cost of the audit. If the audit reveals excess usage of more than ten percent (10%), the Customer shall reimburse the Provider's reasonable audit costs.

11.12 Subscription Term & Renewal

11.12.1 Binding Period & Initial Term

The **Binding Period** commences on the Commencement Date (the date of the Framework) and continues for the number of Billing Periods specified in the Commercial Contract. Each Billing Period has a duration of twelve (12) months starting on the date of the Framework signing.

The subscription includes Second Level Support (maintenance and support) and free Software Updates and Upgrades provided by the Provider throughout the Billing Period.

11.12.2 Evergreen Contract & Auto-Renewal

Upon and beyond the completion of the Binding Period, the Framework operates as an **Evergreen Contract** whereby Second Level Support (maintenance and support) and free Software Updates and Upgrades are provided by the Provider in perpetuity and are automatically renewed (rolled over) after each end of a Billing Period based on the Commercial Contract's Terms and Conditions, until cancelled by the Customer.

Unless either Party provides written notice of non-renewal at least **ninety (90) calendar days** before the expiry of the then-current Billing Period, the subscription shall automatically renew for successive periods of twelve (12) months (each a "Renewal Term") at the then-current fees (subject to price escalation per §11.6).

11.12.3 Termination for Convenience

Neither Party may terminate the Framework for convenience during the Binding Period. During any Renewal Term, either Party may terminate by providing ninety (90) calendar days' written notice prior

to the end of the then-current Billing Period. Early termination during a Renewal Term does not entitle the Customer to a refund of pre-paid fees for the remainder of that Billing Period.

11.12.4 Termination for Cause — Provider's Default

The Customer may terminate the Framework with immediate effect upon written notice if the Provider:

(a) **Performance failure:** Fails to execute the Contract or to perform its obligations in accordance with the terms of this Framework.

(b) **Maintenance failure:** Refuses to remedy software defects or fails to provide the required maintenance and support services under the Contract, being directed in writing to do so by the Customer.

(c) **Insolvency:** Commits an act of bankruptcy, enters into a deed of arrangement with its creditors, or being a company, goes into liquidation (other than a voluntary liquidation for the purposes of reconstruction).

Upon termination for Provider's default, the Provider shall refund a pro-rata portion of any pre-paid subscription fees for the period from the effective date of termination to the end of the then-current Billing Period. The first party may claim compensation against the second party or its representative as a collective liability under this Contract.

11.12.5 Termination for Cause — General

Either Party may terminate the Framework with immediate effect upon written notice if the other Party:

(a) **Material breach:** Commits a material breach of the Framework and fails to remedy such breach within sixty (60) calendar days of receiving written notice specifying the breach.

(b) **Regulatory action:** Is subject to a regulatory action or order that renders continued performance of the Framework unlawful or commercially impracticable.

Termination for cause does not prejudice either Party's accrued rights or remedies.

11.13 Refund Policy

Pre-paid subscription fees are non-refundable except in the following circumstances:

(a) **Termination for Provider breach/default:** Pro-rata refund from the effective date of termination per §11.12.4.

(b) **Persistent SLA failure:** If the aggregate SLA penalties in any six (6) consecutive months exceed twenty percent (20%) of the monthly ARR, the Customer may elect to terminate and receive a pro-rata refund of pre-paid fees.

(c) **Regulatory impossibility:** If a change in law renders the provision of the Services unlawful, the Provider shall refund pre-paid fees for the unexpired portion of the term.

Refunds shall be processed within thirty (30) calendar days of the effective date of termination and shall be paid to the Customer's designated bank account by electronic transfer.

11.14 Data Ownership & Return

Client Data (digital information stored by the Customer in the ProjectVIEW ERP database through the use of the Software) **belongs to the Customer**. The Customer may request the data from the Provider at any time. The Provider shall transmit the data to the Customer within three (3) Business Days of notification.

Detailed data export/return obligations, formats, and procedures are set forth in Chapter 10, §10.9–10.11.

11.15 Warranties & Obligations

11.15.1 Provider's Warranties

Without prejudice to any other warranties expressed elsewhere in this Framework or implied by law, the Provider warrants, represents, and undertakes to the Customer that it:

(a) **Authority:** Has the power and authority to grant the subscription for the Services granted to the Customer hereunder.

(b) **Qualifications:** Has the required qualifications, professional skills, experience, personnel, technical resources, and capability to provide the required Software and perform the necessary Services.

(c) **Maintenance:** Shall maintain the Software (Upgrades) and provide all patches and fixes (Updates) to the Software at no additional cost as part of the Annual Subscription.

(d) **Project management:** Shall maintain a Project Manager and requires a counterpart Project Manager from the Customer to facilitate the smooth execution of works and ensure the completion of deliverables.

(e) **Lifetime Software Warranty:** Co-extensive with the Subscription Term (Chapter 9, §9.13).

11.15.2 Provider's Obligations

The Provider shall:

(a) Supply the Software and perform the Services in accordance with the terms and conditions of this Contract.

(b) Provide such written or oral advice or information regarding the Software and/or the Services as the Customer may reasonably require.

(c) Comply with all lawful and reasonable directions of the Customer relating to the supply of the Software and performance of the Services, including the Customer's Project Management, Security, and Safety requirements.

(d) Only use personnel who are suitably qualified and experienced to perform their role, hold up-to-date professional certifications relevant to the Services they are providing.

(e) Complete the execution of each Service on or before the applicable date specified in the Project Plan finalised at the Kickoff Meeting.

(f) Provide all electronic portals with links to documents/videos as a Training Knowledge Base to the Customer.

11.15.3 Customer's Obligations

The Customer shall:

(a) Pay the fees and services due under this Contract upon the terms and dates provided for under this Contract.

(b) Allow the Provider access to sites, data, and the hosting environment, including third-party applications and COTS.

(c) Use its best efforts to ensure that Authorised Users use the Software in accordance with the terms and conditions of this Framework.

(d) Appoint ProjectVIEW ERP Champions (Power Users / Super Users) as first-level support respondents and system ambassadors (Chapter 4, §4.5).

(e) Acknowledge that the Software will be operated based on the Pricing Metrics of each Module (per User) as specified in the Commercial Contract.

11.16 Commercial Governance

11.16.1 Account Management

The Provider shall appoint a dedicated Contract/Account Manager who shall serve as the primary commercial contact for the Customer. The Account Manager's contact details shall be specified in the Commercial Contract and updated in writing upon any change.

11.16.2 Review Cadence

Commercial matters shall be governed through the **Steering Committee** framework, which includes the following cadence:

Review	Frequency	Participants	Agenda
Operational Review	Monthly	Account Manager, Customer Project Lead, Champions	Ticket volumes, SLA performance, upcoming releases, pending Change Requests, Monthly Status Report
Commercial Review	Quarterly	Account Manager, Customer Commercial Lead, Provider CTO	ARR reconciliation, usage trends, pipeline of add-ons/expansions, pricing review, budget planning
Executive Review	Bi-annually	Provider CEO/CTO, Customer C-Suite / Steering Committee	Strategic alignment, roadmap preview, contract health, escalated issues, renewal planning, Digital Transformation Roadmap

Minutes of each review shall be recorded and circulated within five (5) Business Days. Action items shall be tracked in the Embedded Ticketing System with assigned owners and due dates.

11.17 Roles & Responsibilities (RACI Matrix)

The following RACI matrix defines role allocations for all commercial processes:

Activity	Account Mgr	CTO	Finance	Customer PM	Customer Finance
Commercial Contract / ELA negotiation & execution	R	C	C	R	C
Invoice issuance	C	I	R	I	I
Payment processing	I	I	I	I	R

ARR recalculation	R	I	C	I	I
Price-escalation notice	R	A	C	I	I
Disputed-invoice resolution	R	C	C	R	C
Penalty claim validation	R	C	C	R	I
Licence-compliance audit	R	A	I	R	I
True-up execution	R	I	R	R	R
Renewal / non-renewal notice	R	A	C	R	C
Mid-term User Licence additions/removals	R	I	C	R	I
Module/Addon activation	R	C	C	R	I
Services milestone approval	C	I	R	R	I
Accommodation/travel approval	C	I	I	R	R
Commercial Review chairing	R	C	I	R	I
Executive Review chairing	C	R	I	C	I

Legend: **R** = Responsible · **A** = Accountable · **C** = Consulted · **I** = Informed.

11.18 Process Register

The following process register catalogues all formal processes defined in this chapter.

Process ID	Process Name	Trigger	Handler	Approver	Outcome	Section Ref.
P-11.01	ELA / Commercial Contract Execution	New Customer or material amendment	Account Manager	CTO	Signed ELA/Commercial Contract; ARR established; Binding Period commenced; provisioning initiated.	§11.3, §11.4
P-11.02	Mid-Term User Licence Addition	Customer written request to add Universal/Concurrent Users	Account Manager	Finance	User Licence acknowledged; pro-rata invoice issued; SLA coverage	§11.3.6, §11.5.2

					confirmed from Activation Date.	
P-11.03	Mid-Term User Licence Removal	Customer written notice for next Billing Period	Account Manager	Finance	Licence removal scheduled; Minimum Licence Commitment verified; ARR recalculated.	§11.3.6, §11.5.4
P-11.04	Mid-Term Module/Addon Activation	Customer written request to activate module or Addon	Account Manager	CTO	Module Activation Amendment executed; pro-rata invoice issued; training scheduled.	§11.3.4, §11.5.2
P-11.05	Annual Price Escalation Notice	90 days before Billing Period renewal	Finance	CTO	Written notice of fee increase delivered to Customer with inflation index and calculation methodology.	§11.6.3
P-11.06	Subscription Renewal (Evergreen)	60 days before Billing Period expiry; no non-renewal notice received	Account Manager	CTO	Auto-renewal confirmed; updated Commercial Contract issued; invoice raised for next Billing Period.	§11.12.2
P-11.07	Non-Renewal Notice	Customer or Provider written notice ≥90 days before Billing Period expiry	Account Manager	CTO	Cessation planning initiated per Chapter 10.	§11.12.2
P-11.08	Services Invoice Issuance	Milestone completion trigger per services payment schedule	Finance	Account Manager	Invoice issued to Customer per milestone percentage with applicable taxes.	§11.7.1
P-11.09	Subscription Invoice Issuance	Billing Period commencement or contract signing	Finance	Account Manager	Annual subscription invoice issued with applicable taxes.	§11.7.2
P-11.10	Invoice Dispute	Customer written dispute notice within 15 Business Days	Account Manager	CTO	Dispute logged; investigation commenced; 30-day resolution window initiated.	§11.9

P-11.11	Overdue Payment Escalation	Payment overdue > 60 calendar days	Finance	CTO	Suspension notice issued; 30-day cure period commenced.	§11.7.5
P-11.12	Service Suspension	Cure period expired without payment	Account Manager	CTO	Platform access suspended; Customer notified; data preserved.	§11.7.5
P-11.13	Penalty Claim Submission	SLA breach identified within measurement period	Customer	Account Manager	Claim logged in Ticketing System; validated within 15 Business Days.	§11.10.2
P-11.14	Penalty Credit Application	Penalty claim validated and approved	Finance	CTO	Credit applied to next invoice or cash refund processed within 30 days.	§11.10.1
P-11.15	Licence Compliance Audit	Annual audit trigger; 30-day notice issued	Account Manager	CTO	Self-certification received; system validation completed; discrepancy report issued (if applicable).	§11.11
P-11.16	True-Up Execution	Audit reveals excess usage	Finance	Account Manager	User Licence Amendment executed; back-pay invoice issued; compliance confirmed.	§11.11.3
P-11.17	Termination for Provider Default	Provider default event per §11.12.4	Customer	Customer C-Suite	Termination notice issued; data-return per Chapter 10; pro-rata refund processed.	§11.12.4
P-11.18	Refund Processing	Termination for Provider breach or persistent SLA failure	Finance	CTO	Pro-rata refund calculated and paid within 30 calendar days.	§11.13
P-11.19	Data Return Request	Customer request at any time during or after subscription	Account Manager	CTO	Client Data transmitted to Customer within 3 Business Days.	§11.14

11.19 Process Flow Schematic

The following nine-stage lifecycle illustrates the end-to-end commercial lifecycle from ELA execution through Evergreen renewal or termination:

① ELA Negotiation & Commercial Contract Execution → ② Subscription Activation & Cloud Provisioning → ③ Invoicing & Milestone Payments

↓

④ Ongoing Usage & Compliance Monitoring → ⑤ Flexible Subscription Amendments → ⑥ SLA Performance & Penalty Management

↓

⑦ Annual Review & Price Escalation → ⑧ Licence Audit & True-Up → ⑨ Evergreen Renewal / Non-Renewal / Termination

Stage ① ELA Negotiation & Commercial Contract Execution: The commercial relationship commences with the negotiation and execution of the Enterprise License Agreement and Commercial Contract, which specifies the Binding Period, volume band, module/Addon entitlements, Universal/Concurrent User count, Minimum Licence Commitment, billing cadence, services payment milestones, and currency (P-11.01).

Stage ② Subscription Activation & Cloud Provisioning: Upon Commercial Contract execution, the Provider provisions the Customer's dedicated private sovereign environment on DANAOS Cloud (Microsoft Azure) and installs the Vanilla Version of ProjectVIEW ERP. User accounts are created, roles assigned, and the Kickoff Meeting is scheduled (Chapter 2, Chapter 6). Subscription licences are activated immediately upon Contract signing.

Stage ③ Invoicing & Milestone Payments: Subscription licence invoices are issued upon Contract signing. Services invoices follow the milestone-based payment schedule. The Customer pays within thirty (30) calendar days. Disputed invoices follow the resolution process of §11.9 (P-11.08, P-11.09, P-11.10).

Stage ④ Ongoing Usage & Compliance Monitoring: The Provider continuously monitors Universal/Concurrent User counts and module usage against licensed entitlements. Monthly Operational Reviews track ticket volumes, SLA performance, and Monthly Status Reports (P-11.15).

Stage ⑤ Flexible Subscription Amendments: Additional User Licences or modules/Addons are activated via the Flexible Subscription Model. Licence removals are scheduled for the next Billing Period, subject to the Minimum Licence Commitment. Pro-rata fees are invoiced immediately for additions. ARR is recalculated for the next Billing Period (P-11.02, P-11.03, P-11.04).

Stage ⑥ SLA Performance & Penalty Management: SLA breaches trigger penalty claims per Chapter 3. Claims are submitted through the Embedded Ticketing System and validated within fifteen (15) Business Days. Credits are applied to the next invoice (P-11.13, P-11.14).

Stage ⑦ Annual Review & Price Escalation: Ninety (90) days before each Billing Period renewal, the Provider issues the price-escalation notice based on the official inflation rate of the Index Jurisdiction. The Quarterly Commercial Review assesses usage trends, ARR reconciliation, and upcoming amendments (P-11.05).

Stage ⑧ Licence Audit & True-Up: The Provider conducts an annual licence-compliance audit. Discrepancies are resolved through self-certification and system validation. Excess usage triggers a True-Up with back-pay (P-11.15, P-11.16).

Stage ⑨ Evergreen Renewal / Non-Renewal / Termination: The subscription operates as an Evergreen Contract, auto-renewing unless either Party provides ninety-day (90-day) non-renewal notice. Termination for Provider default follows §11.12.4. Non-renewal triggers the Subscription Cessation procedures of Chapter 10 (P-11.06, P-11.07, P-11.17).

12 Governance, Compliance & Dispute Resolution

This chapter establishes the governance framework, regulatory compliance obligations, audit rights, dispute-resolution mechanisms, limitation of liability, indemnification provisions, and general contractual terms that underpin the relationship between the Provider and the Customer throughout the Subscription Term.

12.1 Contract Governance Framework

The Parties shall establish a structured governance framework to ensure effective management of the contractual relationship, alignment of commercial objectives, and timely resolution of operational matters.

12.1.1 Governance Tiers

The governance framework operates across three tiers:

Tier	Forum	Cadence	Provider Attendees	Customer Attendees	Purpose
Tier 1 — Strategic	Executive Steering Committee	Semi-Annual	CEO / Managing Director, Account Director	C-Suite Sponsor, IT Director / CIO	Strategic alignment, roadmap review, partnership health, escalation resolution
Tier 2 — Tactical	Quarterly Service Review (QSR)	Quarterly	Account Manager, Delivery Lead, Technical Lead	Project Manager, IT Manager, Department Heads	SLA performance, CSI actions, change-request pipeline, licence utilisation, training effectiveness
Tier 3 — Operational	Monthly Operations Meeting	Monthly	Account Manager, Support Lead	IT Manager, DANAOS Champions	Incident trends, open tickets, upcoming releases, operational issues

12.1.2 Steering Committee

The Executive Steering Committee shall comprise no fewer than two (2) senior representatives from each Party. The Committee shall:

(a) Review strategic alignment between the Platform roadmap and the Customer's business objectives;

(b) Approve material changes to scope, commercial terms, or service-level targets;

(c) Resolve escalated disputes that have not been settled at the tactical or operational tiers;

(d) Review and endorse the annual Customer Satisfaction Survey results and improvement plan;

(e) Approve any amendments to the Enterprise License Agreement or Commercial Contract.

12.1.3 Quarterly Service Review (QSR)

Each QSR shall include, at a minimum:

- SLA compliance report (uptime, MTTR, GOS by priority) for the preceding quarter;

- Penalty/credit summary (if applicable) per Chapter 11;
- CSI (Continual Service Improvement) progress tracker;
- Licence utilisation report — Concurrent User peak/average, Volume Band compliance;
- Change-request and release pipeline status;
- Security posture update (vulnerability scan summary, incident count);
- Training effectiveness metrics and upcoming TNA/TNRA activities;
- Risk register review.

QSR minutes shall be circulated within five (5) Business Days and become a governed record.

12.1.4 Governance Records

All governance meetings shall be minuted, and actions shall be logged in a shared Governance Action Register maintained by the Provider. Actions not closed within two (2) consecutive review cycles shall be automatically escalated to the next governance tier.

12.2 Escalation Matrix

Disputes, service failures, and unresolved operational issues shall be escalated through the following tiers. Each tier has a defined resolution window before automatic escalation to the next level.

Escalation Level	Provider Contact	Customer Contact	Resolution Target	Trigger
Level 1 — Operational	Account Manager	IT Manager / Champion	5 Business Days	Initial issue or dispute raised
Level 2 — Management	Delivery Director	Project Director / IT Director	10 Business Days	Level 1 unresolved or SLA breach
Level 3 — Executive	CEO / Managing Director	C-Suite Sponsor	15 Business Days	Level 2 unresolved or material breach
Level 4 — Formal Dispute	External Legal Counsel	External Legal Counsel	Per §12.10	Level 3 unresolved after 15 Business Days

Escalation does not relieve the Provider of its obligation to continue providing the Services in accordance with the agreed Service Levels during the pendency of any dispute.

12.3 Regulatory Compliance

12.3.1 Provider's Compliance Obligations

The Provider shall comply with all applicable laws, regulations, and industry standards in the jurisdictions in which the Services are delivered, including but not limited to:

(a) The General Data Protection Regulation (EU) 2016/679 (GDPR) — as detailed in Chapter 7;

(b) The UAE Federal Decree-Law No. 45 of 2021 on Personal Data Protection (PDPL) — as detailed in Chapter 7;

(c) ISO/IEC 27001:2022 (Information Security Management Systems) — as referenced in Chapter 8;

(d) ISO/IEC 27701:2019 (Privacy Information Management) — as referenced in Chapter 7;

(e) ISO 22301:2019 (Business Continuity Management) — as referenced in Chapter 9;

(f) The EU Artificial Intelligence Act (Regulation (EU) 2024/1689) — to the extent AI capabilities are deployed within the Platform;

(g) NIST AI Risk Management Framework (AI RMF 1.0) — as referenced in Chapter 4;

(h) OWASP Application Security Verification Standard (ASVS) — as referenced in Chapter 8;

(i) Microsoft Azure compliance certifications applicable to the Customer's sovereign environment.

12.3.2 Customer's Compliance Obligations

The Customer shall:

(a) Ensure that its use of the Platform complies with all applicable laws in its jurisdiction;

(b) Obtain and maintain all necessary consents and lawful bases for the processing of Personal Data uploaded to the Platform;

(c) Promptly notify the Provider of any regulatory inquiry, investigation, or enforcement action that may affect the Provider's obligations under this Framework;

(d) Cooperate with the Provider in responding to Data Subject requests in accordance with Section 7.8;

(e) Comply with the Acceptable Use Policy set out in §12.4.

12.3.3 Regulatory Change Management

Where a change in applicable law or regulation requires modification to the Services, the Platform, or the data-processing arrangements:

(a) The Provider shall notify the Customer within thirty (30) calendar days of becoming aware of the regulatory change;

(b) The Parties shall cooperate in good faith to agree on the necessary modifications and any associated cost implications;

(c) Where the regulatory change materially increases the Provider's cost of delivering the Services, the Parties shall negotiate an equitable adjustment to the fees;

(d) Where the regulatory change renders continued performance commercially impracticable, either Party may invoke the termination provisions of §12.9.4.

12.4 Acceptable Use Policy

The Customer shall not, and shall ensure that its Authorised Users do not:

(a) Use the Platform for any unlawful purpose or in violation of any applicable law or regulation;

(b) Upload, store, or transmit any content that infringes the Intellectual Property Rights of any third party;

(c) Attempt to reverse-engineer, decompile, disassemble, or otherwise derive the source code of the Platform;

(d) Use the Platform to transmit malware, viruses, or any other malicious code;

(e) Exceed the licensed Universal/Concurrent User count or circumvent the licensing model;

(f) Share access credentials or permit unauthorised individuals to access the Platform;

(g) Use automated tools (bots, scrapers, crawlers) to access the Platform without the Provider's prior written consent;

(h) Interfere with or disrupt the integrity or performance of the Platform or its infrastructure.

A material breach of the Acceptable Use Policy shall entitle the Provider to suspend the affected User's access immediately upon written notice, and may constitute grounds for termination under §12.9.3.

12.5 Audit Rights

12.5.1 Provider Audit of Customer

The Provider may conduct a licence-compliance audit no more than once per Billing Period, upon thirty (30) calendar days' written notice, to verify that the Customer's usage does not exceed the licensed Universal/Concurrent User count, Volume Band, or module entitlements. The audit process is governed by Chapter 11, §11.11.

12.5.2 Customer Audit of Provider

The Customer (or its appointed independent auditor) may, upon forty-five (45) calendar days' written notice, conduct an audit of the Provider's:

(f) Information security controls and ISMS documentation (Chapter 8);

(g) Data protection and privacy practices (Chapter 7);

(h) Business continuity and disaster recovery preparedness (Chapter 9);

(i) SLA compliance records and supporting evidence (Chapter 3);

(j) Sub-Processor compliance (Chapter 7, §7.12).

Audits shall be conducted during normal business hours, shall not unreasonably interfere with the Provider's operations, and shall be limited to one (1) audit per Billing Period unless a material breach has been identified. The Provider shall cooperate fully and provide all reasonably requested documentation within ten (10) Business Days of the request.

12.5.3 Audit Costs

Each Party shall bear its own costs in connection with any audit. However, if a Provider audit reveals a material licence overuse (exceeding five percent (5%) of the licensed count), the Customer shall reimburse the Provider's reasonable audit costs in addition to the True-Up fees. If a Customer audit reveals a material Provider non-compliance, the Provider shall reimburse the Customer's reasonable audit costs.

12.5.4 Third-Party Certifications

In lieu of or in addition to direct audits, the Provider shall maintain and make available to the Customer upon request:

- ISO/IEC 27001:2022 certification (or equivalent) — renewed annually;
- ISO 22301:2019 certification (or equivalent) — renewed annually;
- Annual penetration-test executive summary (Chapter 8, §8.10);
- Azure compliance attestations applicable to the Customer's sovereign environment.

12.6 Representations & Warranties

12.6.1 Mutual Representations

Each Party represents and warrants that:

(a) It has the legal capacity and authority to enter into and perform its obligations under this Framework;

(b) The execution and performance of this Framework does not violate any other agreement to which it is a party;

(c) It shall comply with all applicable laws and regulations in the performance of its obligations.

12.6.2 Provider's Warranties

The Provider warrants that:

(a) The Platform shall perform materially in accordance with the specifications set out in this Framework and the applicable documentation throughout the Subscription Term (Lifetime Software Warranty — Section 9.13);

(b) The Services shall be performed with reasonable skill and care by appropriately qualified personnel;

(c) The Platform does not, to the Provider's knowledge, infringe any third-party Intellectual Property Rights in the jurisdictions in which the Customer is authorised to use it;

(d) The Provider maintains all necessary licences, certifications, and authorisations to deliver the Services;

(e) The Provider shall maintain insurance coverage adequate to cover its obligations, including professional indemnity, public liability, and cyber-liability policies.

12.6.3 Disclaimer

Except as expressly set out in this Framework, the Provider makes no warranties, express or implied, including any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. The Platform is provided on an "as available" basis subject to the Service Levels and warranties expressly stated herein.

12.7 Limitation of Liability

12.7.1 Aggregate Cap

Subject to §12.7.3, the total aggregate liability of either Party under or in connection with this Framework, whether in contract, tort (including negligence), breach of statutory duty, or otherwise, shall not exceed the total fees paid or payable by the Customer during the twelve (12) month period immediately preceding the event giving rise to the claim.

12.7.2 Exclusion of Consequential Loss

Subject to §12.7.3, neither Party shall be liable to the other for any indirect, incidental, special, consequential, or punitive damages, or for any loss of profits, revenue, data, goodwill, or business opportunity, arising out of or in connection with this Framework, even if advised of the possibility of such damages.

12.7.3 Uncapped Liabilities

The limitations in §12.7.1 and §12.7.2 shall not apply to:

(a) Liability for death or personal injury caused by negligence;

(b) Liability for fraud or fraudulent misrepresentation;

(c) The Provider's indemnification obligations under §12.8.1 (IP infringement);

(d) Either Party's breach of its confidentiality obligations (Chapter 8, §8.12);

(e) Either Party's breach of Data Protection Laws (Chapter 7);

(f) The Customer's obligation to pay fees under Chapter 11.

12.7.4 Duty to Mitigate

Each Party shall take all reasonable steps to mitigate any loss or damage for which it is entitled to bring a claim under this Framework.

12.8 Indemnification

12.8.1 Provider's Indemnification

The Provider shall defend, indemnify, and hold harmless the Customer and its officers, directors, employees, and agents from and against any third-party claim, action, suit, or proceeding alleging that the Customer's use of the Platform in accordance with this Framework infringes any third-party patent, copyright, trademark, or trade secret.

If the Platform becomes, or in the Provider's reasonable opinion is likely to become, the subject of an infringement claim, the Provider shall, at its sole expense and option:

(a) Procure for the Customer the right to continue using the Platform;

(b) Modify the Platform to make it non-infringing without materially reducing functionality; or

(c) Replace the infringing component with a functionally equivalent non-infringing alternative.

If none of the foregoing is commercially practicable, the Provider may terminate the affected portion of the Framework and refund to the Customer a pro-rata portion of pre-paid fees for the unexpired Billing Period.

12.8.2 Customer's Indemnification

The Customer shall defend, indemnify, and hold harmless the Provider from and against any third-party claim arising from:

(a) The Customer's breach of the Acceptable Use Policy (§12.4);

(b) Customer Data that infringes any third-party Intellectual Property Rights;

(c) The Customer's use of the Platform in violation of applicable law.

12.8.3 Indemnification Procedure

The indemnified Party shall:

(a) Promptly notify the indemnifying Party in writing of any claim (failure to provide timely notice shall not relieve the indemnifying Party of its obligations except to the extent materially prejudiced);

(b) Grant the indemnifying Party sole control of the defence and settlement of the claim;

(c) Cooperate fully at the indemnifying Party's expense in the defence of the claim.

The indemnifying Party shall not settle any claim that imposes obligations on the indemnified Party or admits liability on its behalf without the indemnified Party's prior written consent (not to be unreasonably withheld).

12.9 Term & Termination

12.9.1 Term

This Framework shall commence on the Subscription Start Date and continue for the Initial Term (Binding Period) as specified in the Commercial Contract and Enterprise License Agreement. Following the expiry of the Binding Period, the Framework shall renew automatically for successive Billing Periods under the Evergreen Contract mechanism unless terminated in accordance with this Section.

12.9.2 Termination for Convenience

Following the expiry of the Binding Period, either Party may terminate this Framework by providing written non-renewal notice at least ninety (90) calendar days before the expiry of the then-current Billing Period. Termination for convenience during the Binding Period is not permitted unless mutually agreed in writing.

12.9.3 Termination for Cause — Customer Default

The Provider may terminate this Framework immediately upon written notice if the Customer:

(a) Fails to pay any undisputed amount within sixty (60) calendar days of the due date;

(b) Commits a material breach of the Acceptable Use Policy (§12.4) that is not remedied within thirty (30) calendar days of written notice;

(c) Becomes insolvent, enters into administration, liquidation, or any equivalent proceedings.

12.9.4 Termination for Cause — Provider Default

The Customer may terminate this Framework immediately upon written notice if the Provider:

(a) Fails to meet the applicable Service Level (SLO) for three (3) or more consecutive calendar months;

(b) Commits a material breach of its data protection or information security obligations under Chapters 7 or 8 that is not remedied within thirty (30) calendar days of written notice;

(c) Becomes insolvent, enters into administration, liquidation, or any equivalent proceedings;

(d) Fails to deliver a critical software update or security patch within the timeframes specified in Chapter 4 for three (3) or more consecutive instances.

Cross-reference: Provider's Default provisions in Chapter 11, §11.12.4 apply in addition to this Section.

12.9.5 Consequences of Termination

Upon termination or expiry of this Framework:

(a) The Provider shall perform the data return obligations set out in Chapter 11, §11.14, delivering all Customer Data within three (3) Business Days of the Customer's written request;

(b) The end-of-life and decommissioning procedures set out in Chapter 10 shall apply;

(c) All licences granted to the Customer shall terminate immediately;

(d) Each Party shall return or destroy the other Party's Confidential Information in accordance with Chapter 8, §8.12;

(e) Any accrued rights and obligations (including payment obligations for Services rendered) shall survive termination;

(f) The Source Code Escrow provisions (Section 9.14) shall survive termination to the extent specified therein.

12.9.6 Survival

The following provisions shall survive termination or expiry of this Framework: §12.5 (Audit Rights — for twelve (12) months post-termination), §12.6 (Representations & Warranties), §12.7 (Limitation of Liability), §12.8 (Indemnification), §12.9.5 (Consequences of Termination), §12.10 (Dispute Resolution), §12.11 (Governing Law), §12.12 (Confidentiality — per Chapter 8), and §12.13 (General Provisions).

12.10 Dispute Resolution

Any dispute arising out of or in connection with this Framework ("Dispute") shall be resolved in accordance with the following sequential procedure:

12.10.1 Good-Faith Negotiation

The Parties shall first attempt to resolve the Dispute through good-faith negotiation at the Management level (Escalation Level 2) for a period of thirty (30) calendar days following written notice of the Dispute.

12.10.2 Mediation

If the Dispute is not resolved through negotiation within the thirty (30) day period, either Party may refer the Dispute to mediation administered by the Dubai International Arbitration Centre (DIAC) or another mutually agreed mediation body. The mediator shall be appointed by mutual agreement; failing agreement within fifteen (15) calendar days, the mediation body shall appoint the mediator. Mediation shall be conducted in English. The costs of mediation shall be borne equally by the Parties.

12.10.3 Arbitration

If the Dispute is not resolved through mediation within sixty (60) calendar days of the referral to mediation, either Party may refer the Dispute to final and binding arbitration administered by DIAC under its applicable Arbitration Rules in effect at the time of filing:

(a) The arbitral tribunal shall consist of one (1) arbitrator for Disputes with a value below USD 500,000 and three (3) arbitrators for Disputes at or above that threshold;

(b) The seat of arbitration shall be Dubai, United Arab Emirates;

(c) The language of the arbitration shall be English;

(d) The arbitral award shall be final and binding and may be enforced in any court of competent jurisdiction.

12.10.4 Injunctive Relief

Nothing in this Section shall prevent either Party from seeking injunctive or other equitable relief from a court of competent jurisdiction to prevent irreparable harm, including but not limited to the protection of Confidential Information, Intellectual Property Rights, or data security.

12.10.5 Continuation of Services

During the pendency of any dispute, mediation, or arbitration, the Parties shall continue to perform their respective obligations under this Framework in good faith.

12.11 Governing Law & Jurisdiction

This Framework shall be governed by and construed in accordance with the laws of the Emirate of Dubai and the applicable federal laws of the United Arab Emirates, without regard to conflict-of-law principles.

Subject to the dispute-resolution provisions of §12.10, the courts of the Dubai International Financial Centre (DIFC) shall have non-exclusive jurisdiction in respect of any proceedings arising out of or in connection with this Framework.

Data Protection jurisdiction: Where the Customer's operations are subject to the GDPR, the data-protection provisions of Chapter 7 shall be interpreted in accordance with EU law, and the CJEU shall have jurisdiction in respect of GDPR-specific disputes to the extent required by law.

12.12 Force Majeure

Neither Party shall be liable for any failure or delay in performing its obligations under this Framework to the extent that such failure or delay is caused by a Force Majeure Event.

12.12.1 Notification

The affected Party shall:

(k) Notify the other Party in writing within forty-eight (48) hours of becoming aware of the Force Majeure Event;

(l) Provide reasonable details of the event, its expected duration, and the obligations affected;

(m) Use all commercially reasonable efforts to mitigate the effects and resume performance as soon as practicable.

12.12.2 Prolonged Force Majeure

If a Force Majeure Event continues for a period exceeding ninety (90) consecutive calendar days, either Party may terminate this Framework by providing thirty (30) calendar days' written notice. In such event, the Provider shall refund to the Customer a pro-rata portion of any pre-paid fees for the unexpired portion of the then-current Billing Period.

12.12.3 Exclusions

Force Majeure shall not include: the Provider's failure to maintain adequate BCDR arrangements (Chapter 9); market changes, financial difficulties, or inability to meet cost obligations; or planned maintenance or scheduled downtime.

12.13 General Provisions

12.13.1 Entire Agreement

This Framework, including all Chapters, Appendices, the Commercial Contract, and the Enterprise License Agreement, constitutes the entire agreement between the Parties with respect to its subject matter and supersedes all prior and contemporaneous agreements, representations, warranties, and understandings, whether written or oral.

12.13.2 Amendments

No amendment or modification to this Framework shall be effective unless made in writing and signed by duly authorised representatives of both Parties. Amendments to the Commercial Contract (including User Licence Amendments and Module Activation Amendments) shall follow the processes set out in Chapter 11.

12.13.3 Severability

If any provision of this Framework is held to be invalid, illegal, or unenforceable, the remaining provisions shall continue in full force and effect. The Parties shall negotiate in good faith to replace the invalid provision with a valid provision that achieves, to the extent possible, the original commercial intent.

12.13.4 Waiver

No failure or delay by either Party in exercising any right, power, or remedy under this Framework shall operate as a waiver thereof, nor shall any single or partial exercise preclude any further exercise of the same or any other right.

12.13.5 Assignment

Neither Party may assign or transfer its rights or obligations under this Framework without the prior written consent of the other Party, except that:

(a) The Provider may assign this Framework to an affiliate or successor entity in connection with a merger, acquisition, or sale of substantially all of its assets, provided the assignee assumes all obligations; and

(b) The Customer may assign this Framework to an affiliate, provided the affiliate meets the same creditworthiness and compliance standards.

Any purported assignment in violation of this Section shall be void.

12.13.6 Notices

All notices required or permitted under this Framework shall be in writing and shall be deemed delivered:

(a) Upon delivery, if delivered by hand;

(b) Upon confirmed receipt, if sent by registered mail or internationally recognised courier (e.g., DHL, FedEx);

(c) Upon confirmed receipt, if sent by email to the designated notice address specified in the Commercial Contract, provided a delivery confirmation is obtained.

Each Party shall designate a primary and secondary notice contact in the Commercial Contract and shall notify the other Party of any changes within ten (10) Business Days.

12.13.7 No Partnership or Agency

Nothing in this Framework shall create, or be deemed to create, a partnership, joint venture, agency, or employment relationship between the Parties. Neither Party has authority to bind the other in any way.

12.13.8 Third-Party Rights

Except as expressly provided (including in respect of indemnified persons under §12.8), no person who is not a Party to this Framework shall have any right to enforce any of its terms.

12.13.9 Counterparts

This Framework may be executed in any number of counterparts, each of which shall be deemed an original and all of which together shall constitute one agreement. Electronic signatures shall be deemed equivalent to original signatures for all purposes.

12.13.10 Order of Precedence

In the event of any conflict or inconsistency between the documents forming this Framework, the following order of precedence shall apply (highest first):

(a) The Commercial Contract (and any amendments thereto);

(b) The Enterprise License Agreement;

(c) The main body of this Framework (Chapters 1–12);

(d) The Appendices.

12.14 Insurance

The Provider shall maintain throughout the Subscription Term, at its own expense, the following minimum insurance coverage:

Insurance Type	Minimum Coverage	Scope
Professional Indemnity (Errors & Omissions)	As specified in the Commercial Contract	Claims arising from professional negligence, errors, or omissions in the delivery of Services
Public Liability	As specified in the Commercial Contract	Third-party bodily injury or property damage arising from the Provider's operations
Cyber Liability / Data Breach	As specified in the Commercial Contract	Data breaches, cyber incidents, regulatory fines and penalties, notification costs, forensic investigation
Employer's Liability	As required by applicable law	Employee injury or illness arising in the course of employment

The Provider shall provide certificates of insurance to the Customer upon request and shall notify the Customer of any material change to or cancellation of coverage within ten (10) Business Days.

12.15 Anti-Corruption & Ethical Conduct

Each Party represents, warrants, and undertakes that:

(a) It shall comply with all applicable anti-bribery and anti-corruption laws, including the UK Bribery Act 2010, the US Foreign Corrupt Practices Act (FCPA), and UAE Federal Decree-Law No. 11 of 2023 on Anti-Money Laundering;

(b) It shall not, directly or indirectly, offer, promise, give, or authorise the giving of any improper payment, gift, or benefit to any person in connection with this Framework;

(c) It shall maintain and enforce adequate procedures to prevent bribery, corruption, and unethical conduct by its employees, officers, and sub-contractors;

(d) It shall promptly notify the other Party if it becomes aware of any breach or suspected breach of this Section.

A breach of this Section shall constitute a material breach entitling the non-breaching Party to terminate this Framework immediately upon written notice.

12.16 Confidentiality

The comprehensive confidentiality provisions governing this Framework are set out in Chapter 8, §8.12. This Section provides a summary of the key principles:

(a) Each Party shall treat the other Party's Confidential Information with at least the same degree of care as it treats its own confidential information, and in no event less than reasonable care;

(b) Confidential Information shall not be disclosed to any third party without the prior written consent of the disclosing Party, except as required by law or regulation;

(c) Confidential Information may be disclosed to employees, officers, advisors, and sub-contractors on a need-to-know basis, provided they are bound by obligations of confidentiality no less protective than those in this Framework;

(d) Obligations of confidentiality shall survive termination of this Framework for a period of five (5) years, except that trade secrets shall remain protected indefinitely.

12.17 Governance, Compliance & Dispute Resolution

R = Responsible | A = Accountable | C = Consulted | I = Informed

Activity	Provider CEO	Provider Account Mgr	Provider Legal	Customer C-Suite	Customer IT Dir	Customer Legal
Establish governance framework	A	R	C	A	R	I
Conduct QSR	I	R	I	I	R	I
Conduct Steering Committee meeting	R	C	I	R	C	I
Manage Governance Action Register	I	R	I	I	C	I
Escalation management	A	R	C	A	R	C
Regulatory change assessment	I	R	R	I	C	A
Licence-compliance audit (Provider-led)	I	R	C	I	R	I
Security/privacy audit (Customer-led)	I	C	C	A	R	C
Maintain third-party certifications	A	I	I	I	I	I
Negotiate dispute resolution (Level 1–2)	I	R	C	I	R	C

Activity	Provider CEO	Provider Account Mgr	Provider Legal	Customer C-Suite	Customer IT Dir	Customer Legal
Manage mediation / arbitration	A	C	R	A	C	R
Insurance certificate maintenance	A	R	I	I	I	I
Anti-corruption compliance monitoring	A	R	R	A	I	R
Force Majeure notification	A	R	C	A	R	C
Agreement amendment execution	A	C	R	A	C	R
Termination notice and exit management	A	R	R	A	R	R

12.18 Process Register — Governance, Compliance & Dispute Resolution

ID	Process	Trigger	Handler	Approver	Outcome	Cross-Ref
P-12.01	QSR Preparation & Delivery	Quarterly calendar trigger	Account Manager	Customer IT Dir	QSR report delivered, actions logged	§12.1.3
P-12.02	Steering Committee Meeting	Semi-annual calendar trigger	Account Director	CEO + C-Suite Sponsor	Strategic decisions recorded, actions logged	§12.1.2
P-12.03	Operational Escalation (L1→L2)	L1 unresolved within 5 BD	Delivery Director	Account Director	Issue escalated with action plan	§12.2
P-12.04	Executive Escalation (L2→L3)	L2 unresolved within 10 BD	CEO / MD	C-Suite Sponsor	Executive intervention, resolution or formal dispute	§12.2
P-12.05	Regulatory Change Notification	New law/regulation identified	Legal Counsel	CEO / C-Suite	Impact assessment delivered, modifications agreed	§12.3.3
P-12.06	Licence-Compliance Audit	Annual or per-Billing-Period	Account Manager	Delivery Director	Audit report, True-Up Notice if required	§12.5.1, §11.11

ID	Process	Trigger	Handler	Approver	Outcome	Cross-Ref
P-12.07	Customer Security/Privacy Audit	Customer 45-day notice	CISO / DPO	Account Director	Audit completed, findings shared	§12.5.2
P-12.08	Third-Party Certification Renewal	Annual renewal cycle	CISO	CEO	Certificates renewed and shared	§12.5.4
P-12.09	Good-Faith Negotiation	Formal dispute notice	Account Manager	Delivery Director	Resolution or escalation to mediation	§12.10.1
P-12.10	Mediation Referral	Negotiation unresolved (30 days)	Legal Counsel	CEO	Mediator appointed, mediation conducted	§12.10.2
P-12.11	Arbitration Filing	Mediation unresolved (60 days)	External Legal	CEO + Board	Arbitral award	§12.10.3
P-12.12	Force Majeure Notification	FM Event occurs	Account Manager	CEO	48h notification, mitigation plan	§12.12.1
P-12.13	Prolonged FM Termination	FM >90 consecutive days	Legal Counsel	CEO	Agreement terminated, pro-rata refund	§12.12.2
P-12.14	Insurance Certificate Request	Customer request or annual	Account Manager	CEO	Certificate provided within 10 BD	§12.14
P-12.15	Anti-Corruption Incident	Suspected breach reported	Legal Counsel	CEO	Investigation, remediation, potential termination	§12.15
P-12.16	Agreement Amendment Execution	Amendment request by either Party	Account Manager	Legal Counsel + CEO	Signed amendment, updated Commercial Contract	§12.13.2
P-12.17	Termination Notice Issuance	Non-renewal or cause trigger	Legal Counsel	CEO	Formal notice, exit process initiated	§12.9
P-12.18	Post-Termination Audit	Termination effective date + 30 days	Account Manager	CISO / DPO	Data return verified, decommissioning confirmed	§12.9.5, §10.10

12.19 Process Flow Schematic — Governance & Dispute Resolution Lifecycle

The following nine-stage lifecycle depicts the governance, compliance, and dispute-resolution flow from contract inception through post-termination:

① Contract Inception

Agreement executed → governance framework established → governance contacts designated → meeting cadences set → Governance Action Register created.

② Operational Governance

Monthly Operations Meetings → incident/ticket trend review → release pipeline status → Champion engagement → action items logged and tracked.

③ Tactical Governance (QSR)

Quarterly Service Review → SLA/GOS reporting → CSI progress → licence utilisation → security posture → training metrics → risk register → minutes circulated within 5 BD.

④ Strategic Governance (Steering)

Semi-annual Steering Committee → roadmap alignment → commercial review → ELA/Commercial Contract amendments → customer satisfaction → escalated dispute resolution.

⑤ Compliance & Audit

Regulatory change monitoring → Provider/Customer compliance obligations → licence audits → security/privacy audits → certification renewals → anti-corruption checks.

⑥ Issue Escalation

L1 Operational (5 BD) → L2 Management (10 BD) → L3 Executive (15 BD) → L4 Formal Dispute → services continue during dispute.

⑦ Dispute Resolution

Good-faith negotiation (30 days) → Mediation via DIAC (60 days) → Binding arbitration (DIAC Rules) → Injunctive relief preserved → award enforcement.

⑧ Termination & Exit

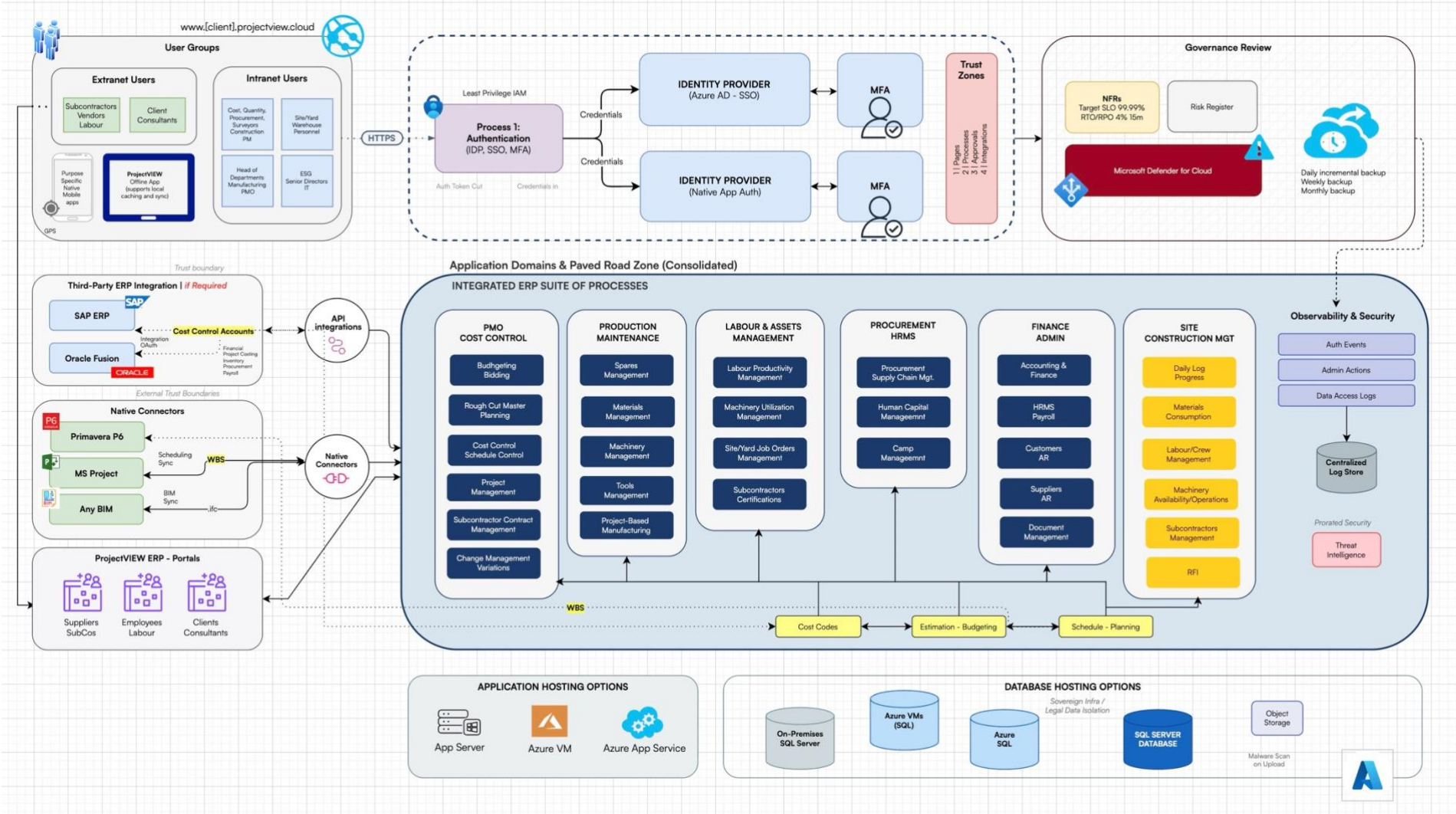
Non-renewal notice (90 days) or cause trigger → data return (3 BD) → EOL/decommissioning (Chapter 10) → licence revocation → Confidential Information return/destruction.

⑨ Post-Termination

Survival clauses active → audit rights (12 months) → liability/indemnification obligations → escrow rights preserved → confidentiality (5 years / indefinite for trade secrets).

13 Appendices

13.1 ProjectVIEW ERP Architecture and Deployment Options



13.2 ProjectVIEW ERP Master Flows