G-Cloud 15 (RM1557.15) Covoxa.

Enterprise Resource Planning (ERP) Cloud Software Implementation and Support Services

Service Definition

January 2026

Table of contents

1 INTRODUCTION

1.1 Document structure

This Service Definition document provides information about the services offered by Covoxa under the G-Cloud 15 Framework. It is designed to help public sector buyers understand the functionality, security, pricing and management of our services and to provide clarity on how to engage with us through the framework.

Service description: Outlines our Enterprise Resource Planning (ERP) Cloud Software Implementation and Support Services, including key features, benefits, delivery methodology and assurance measures such as security and compliance.

Operational delivery and framework alignment: Explains how our services are delivered under the G-Cloud 15 framework, covering onboarding, service levels, data management, support and exit processes.

Supplier information: Summarises our company background, mission, relevant experience and how to procure our services through G-Cloud.

1.2 How to use this document

We have developed this document to support you throughout the G-Cloud procurement journey, summarised below:

Early-stage evaluation: Section 2 (Service description) outlines our service scope, delivery approach and core benefits to help determine alignment with organisational needs.
Due diligence and contract preparation: Section 3 (G-Cloud alignment information) provides details on onboarding, service levels, data management, support and exit procedures.
Data protection and compliance assurance: Section 4 (Security and data governance) explains our information-security framework, data-handling standards and business-continuity measures.
Supplier verification: Section 5 (Supplier information) includes background on Covoxa, relevant accreditations and procurement routes.

2 SERVICE DESCRIPTION

2.1 About our service

Covoxa provides Enterprise Resource Planning (ERP) Cloud Software Implementation and Support Services for public sector organisations, previous or current clients include Cabinet Office, Ministry of Justice, Foreign, Commonwealth and Development Office. . Our service helps buyers implement new ERP solutions or enhance existing deployments to maximise value and efficiency.

We work with leading platforms such as Oracle Fusion, Workday and SAP, combining industry best practices with proven methodologies. Our approach ensures alignment with organisational goals, compliance with government standards and measurable outcomes.

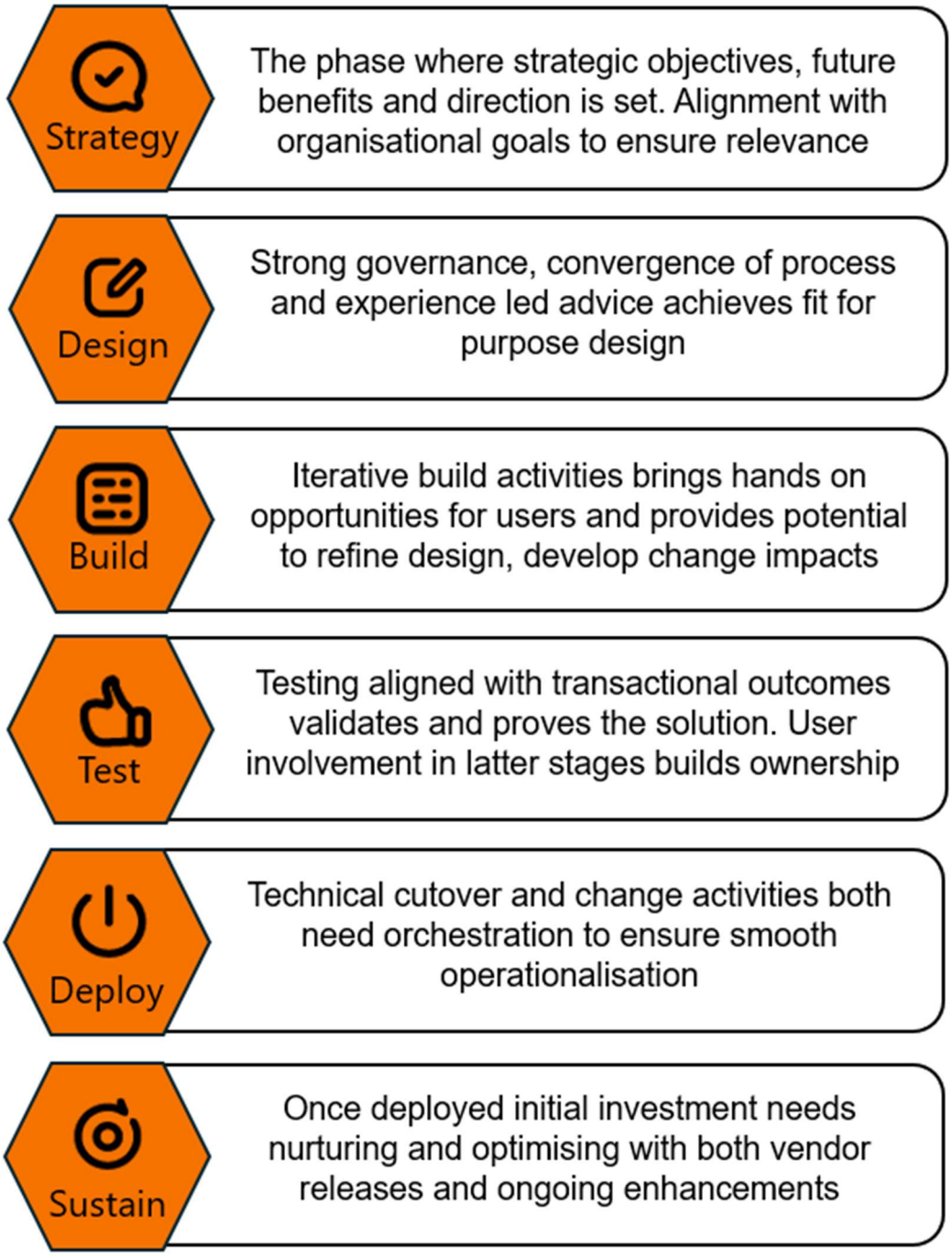
Under the G-Cloud 15 framework, we deliver structured implementation and support services that include:

- Design and configuration based on an adopt-not-adapt principle
- Enhancements to existing deployments based on vendor release as well as new functionality development based on changing business needs
- Data migration using iterative cycles to build confidence and accuracy
- Integration development for secure interoperability with existing systems
- Testing from unit to end-to-end and user acceptance stages
- Deployment and cutover activities for smooth transition to live operation
- Post-go-live support to optimise functionality and leverage vendor updates
- Change management and training embedded throughout delivery

Value and differentiators

2.2 Delivery framework

To provide structured and predictable delivery, we apply our proprietary Synergize methodology across every stage of the project lifecycle, outlined below. To achieve successful implementation, Synergize follows 6 phases: strategy, design, build, test, deploy and sustain. Each phase includes defined activities and checkpoints to maintain alignment with organisational goals and compliance requirements.



2.3 Service features / benefits

Requirement definition and user journey development

To ensure design reflects real operational needs, we conduct structured discovery, mapping end-to-end user journeys and capturing functional and non-functional requirements.

✓ **Benefit:** User-centric design – Ensures the ERP solution aligns with real user workflows, improving efficiency and adoption

Functional configuration based on adopt not adapt

Improving long-term maintainability and reducing customisation, we configure the ERP solution using standard functionality.

✓ **Benefit:** Future proof solutions – Minimises technical debt and accelerates uptake of vendor updates and innovations

Business process configuration

Ensuring best-practice workflow alignment, we converge and harmonise business processes across HR, finance and procurement.

✓ **Benefit:** Robust governance – Establishes consistent, compliant, scalable processes across the organisation

Integration specification and development

For seamless data flow, we design and build secure, scalable integrations between the ERP platform and external systems.

✓ **Benefit:** Proven scalability – Reliable integration patterns that have supported complex public-sector estates from 2,000 to 250,000+ users

Data migration (extraction, transformation and load)

We manage iterative data migration cycles to cleanse, transform and validate data from legacy systems into the new cloud ERP.

✓ **Benefit:** Maximised ROI – High-quality data reduces rework, improves reporting accuracy and accelerates realisation of benefits

Testing from Unit to End-to-End, User Acceptance (UAT) and Payroll (PCT)

We deliver a full testing lifecycle to validate configuration, integrations, payroll accuracy and end-to-end business processes.

✓ **Benefit:** Qualified expertise – Ensures compliance, defect reduction and confidence in go-live through chartered professionals (CIPP/CIPD)

Deployment, go-live and cutover activities

Ensuring a smooth transition for legacy systems, we manage deployment planning, cutover execution and support.

✓ **Benefit:** Value for money - Structured go-live minimises downtime, reduces delivery risk and avoids costly delays or failure points

Change and engagement activities

Supporting adoption of new ERP processes, we lead change impact assessments, communications, stakeholder engagement and readiness preparation.

✓ **Benefit:** Collaborative partnerships – Builds organisational buy-in and reduces resistance through shared outcomes and co-design

Training through train the trainer and end users

We deliver tailored training programmes, including super-user training, role-based learning and user enablement sessions.

✓ **Benefit:** Continuous knowledge transfer – Builds sustainable capability so internal teams can confidently support and evolve the system

Full portfolio of Workday and Oracle implementation, support and managed services

We provide end-to-end delivery and support capabilities across Workday and Oracle Fusion, from design through to ongoing optimisation.

✓ **Benefit:** Public sector focus – Deep experience across shared service clusters and central government ensures solutions meet policy, audit and compliance requirements

2.4 Service scope

Our service is designed to support public sector organisations with cloud Enterprise Resource Planning (ERP) adoption and optimisation. It operates as a standalone cloud support service but can also complement existing ERP implementations.

2.4.1 Add-ons and extensions

This service can function as an extension to existing ERP platforms such as Oracle Fusion, Workday and SAP. It enhances capability by providing advisory, migration and optimisation support without replacing core systems.

Integration is achieved through secure, standards-based methods including application programming interfaces (APIs) and vendor-native connectors. This approach ensures interoperability and compliance with government security standards.

2.4.2 Cloud deployment model

Covoxa does not host an ERP platform. We deliver Lot 3 cloud support services that help buyers plan, implement, and optimise ERP estates on buyer-controlled and vendor clouds, for example, Oracle Fusion, Workday and SAP. All work is performed within buyer environments under buyer access controls and governance.

2.4.3 Service constraints

We deliver services within the following standard constraints:

- Access to relevant buyer systems, environments and subject-matter experts must be provided as agreed in the Statement of Work (SOW)
- Planned maintenance is scheduled outside UK business hours and announced at least 48 hours in advance
- The service operates in a cloud-hosted environment and is accessible via modern browsers, including Chrome, Edge, Safari and Firefox
- Performance may vary when used outside UK regions due to data residency and latency differences
- Deliverables and timelines may be impacted by dependencies on third-party vendors or buyer-side decision cycles

2.4.4 System requirements

To ensure optimal performance, the service requires:

- **Supported browsers:** Latest versions of Chrome, Edge, Safari and Firefox.
- **Operating systems:** Windows 10+, macOS 12+, iOS and Android (latest two versions).
- **Connectivity:** Stable broadband connection (minimum 10 Mbps recommended).
- **User permissions:** Standard user account; administrative rights required only for optional local integrations.
- **Third-party prerequisites:**
    - Valid Microsoft 365 or Google Workspace licence for productivity integrations.

No specialist hardware is required. Any additional requirements specific to a buyer engagement will be confirmed in the Statement of Work.

2.5 Reselling

We do not resell any services outside those declared in our G-Cloud listing but we can work with your teams to assess, select and procure any required services. We only recommend third-party services where they demonstrably support the buyer's objectives and deliver measurable benefits.

2.6 User support

To ensure buyers receive timely assistance, we provide multiple support channels and clear escalation processes. Our support model, defined below, is designed for accessibility and responsiveness.

2.7.1 Support details

Category	Details
Support channels	• Email • Online ticketing portal Freshdesk • Telephone • Web Chat using Freshchat
Support hours	• Standard: Monday–Friday, 09:00–17:00 (UK time) • Extended or 24/7 support available by agreement
Response times	• High-priority: within 4 working hours • Standard enquiries: within 8 working hours
Support accessibility	• Online ticketing working to WCAG 2.2 AA standards compliance • Web chat meets EN 301 549 standards
Support for third parties	• Authorised third-party contractors can access support channels upon buyer request
Escalation process	• Built into the ticketing system • Critical issues assigned immediately to senior engineers

Account management	• Dedicated Technical Account Manager available for strategic engagements, onboarding and change requests

2.7.2 Accessibility and usability

Ensuring all users can access and use our service effectively, we design every interface to meet recognised accessibility standards. This guarantees adoption across the public sector without additional adjustments.

To comply with accessibility requirements, all interfaces and documentation meet Web Content Accessibility Guidelines (WCAG) 2.2 AA and EN 301 549 standards. These standards ensure compatibility with assistive technologies such as screen readers and keyboard navigation.

2.8 How users work with our service

2.8.1 Browsers

To ensure uninterrupted access to ERP functionality, the service works with all major browsers. We support the latest versions of Google Chrome, Microsoft Edge, Mozilla Firefox and Safari. Buyers receive advance notice of any changes to browser compatibility.

2.8.2 Desktop and application, service interface or API

Covoxa does not provide a desktop or mobile application, proprietary user interface, or private API. We work through approved vendor administration tools and APIs under buyer governance. Our service desk supports buyers via agreed channels and Service Level Agreements (SLAs).

2.8.3 Accessibility and usability

To improve usability for all users, including those with assistive technology needs, our service is designed in accordance with Web Content Accessibility Guidelines (WCAG) 2.2 AA standards. This ensures compliance with public sector accessibility requirements.

2.8.4 Customisation

To maximise flexibility and align ERP solutions with organisational goals, our service offers extensive configuration options without custom development. This ensures buyers can adapt the system to their processes while maintaining compliance.

Configurable elements include:

- Role-based access control to tailor HR, payroll, finance and procurement workflows

- Workflow and Business Process Automation rules and approval routes aligned with governance requirements
- Configuration of functionality, screens and fields to support user centric design
- User roles and permissions to support secure access and segregation of duties
- Reporting fields and analytics views for transparent performance tracking
- Configurable reporting
- Low Code integration development
- Branding options such as logos and terminology for organisational identity

3 G-CLOUD ALIGNMENT INFORMATION

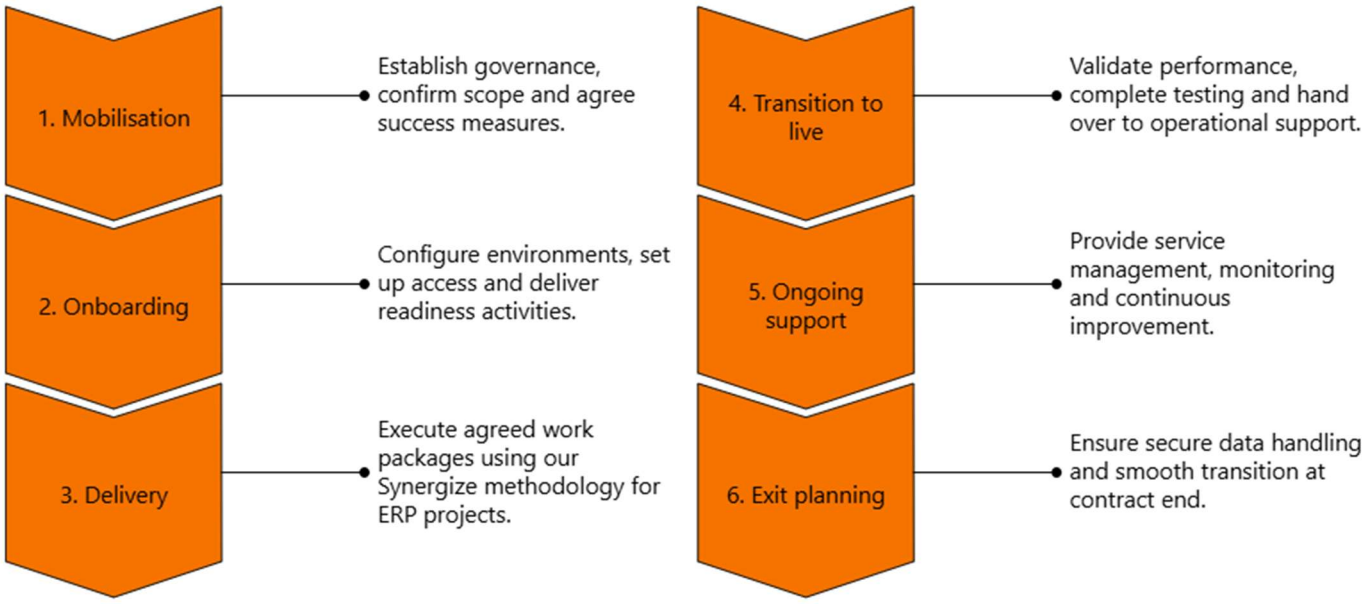
3.1 Section introduction

To ensure clarity and confidence for buyers, this section explains how our service is delivered and managed under the G-Cloud 15 framework. It covers the operational processes that support onboarding, configuration, live operation, service management and secure offboarding.

To deliver consistent quality and measurable outcomes, we apply a structured, yet flexible delivery model tailored to each buyer's objectives, governance requirements and scale. Our approach combines robust project controls with iterative methods to enable rapid progress without compromising compliance.

Every engagement follows a defined lifecycle supported by our ISO-aligned management system and ITIL-based service management framework. This ensures accountability, transparency and alignment with Crown Commercial Service standards.

Typical delivery lifecycle phases include:



3.2 Onboarding and offboarding processes

To establish clear expectations and reduce delivery risk, every engagement begins with a collaborative onboarding phase. This phase ensures governance, data access and communication structures are in place before delivery starts.

3.2.1 Onboarding

To establish clear expectations and reduce delivery risk, every engagement begins with a collaborative onboarding phase. This phase ensures governance, data access and communication structures are in place before delivery starts. Typical onboarding steps include:

1. **Kick-off and scoping:** We meet with buyer governance and project teams to confirm objectives, scope, timelines and success criteria.
2. **Statement of Work (SOW):** We finalise the SOW detailing deliverables, dependencies and commercial terms.
3. **Access and environment setup:** The buyer provides required system access and permissions. All work is conducted on buyer infrastructure to maintain data security.
4. **Resource allocation and scheduling:** We assign roles, confirm timelines and record milestones in the project plan.
5. **Discovery and requirements confirmation:** Workshops validate functional, technical and user requirements, forming the baseline for delivery.
6. Onboarding concludes when all stakeholders approve the SOW and project initiation documents.

3.2.2 Offboarding

To ensure a secure and transparent exit, every engagement concludes with a structured offboarding phase. This process confirms deliverables, transfers knowledge and ensures the buyer retains full ownership of systems and data. Typical offboarding steps include:

1. **Project closure review:** We confirm deliverables, capture lessons learned and assess performance against success criteria.
2. **Documentation and handover:** We provide complete delivery artefacts including configuration records, test outcomes, migration reports and training materials.
3. **Knowledge transfer:** Our specialists deliver targeted workshops or shadowing sessions to enable buyer teams to operate independently.
4. **Access revocation and data return:** All system access is revoked and any temporary project data is securely returned or deleted in line with governance policies.
5. **Post-engagement support:** Where required, we offer continued optimisation or advisory services under a new or extended SOW.

3.3 Data

3.3.1 Data importing and exporting

To ensure flexibility and prevent vendor lock-in, our service supports standards-based data import and export. Buyers can move data in and out of the system easily at any time.

Data import: To simplify onboarding, buyers can upload data using open formats such as CSV (Comma-Separated Values), JSON (JavaScript Object Notation) and ODF (Open Document Format). Bulk imports are supported through secure upload or API integration for efficiency.
Data export: To maintain portability, all data stored within the system can be exported in open formats, including CSV and ODF. Exports can be generated on demand or scheduled and accessed through the user interface or API depending on buyer preference.

3.3.2 Analytics

To support informed decision-making and governance, buyers can monitor operational activity through vendor ERP or BI tools. Covoxa does not provide a proprietary API. Enabling automation and advanced analysis, API access is available through vendor ERP platforms for programmatic retrieval of metrics.

3.3.3 Independence of resource

To ensure security and predictable performance, each buyer engagement is fully isolated within the buyer's chosen cloud environment or approved vendor platform. Covoxa does not operate shared multi-tenant compute for buyer workloads. Access to systems and data is granted strictly on a least-privilege basis and controlled through role-based permissions. All activities are logged for audit and reviewed in line with governance requirements. This approach guarantees that one organisation's processes cannot affect another and maintains compliance with public sector security standards.

3.3.4 Public sector networks

Covoxa uses buyers' existing accredited connections (PSN/HSCN/JANET) and does not provide its own connectivity. To support secure connectivity, the service can integrate with approved public sector networks where required. Any connection follows the relevant governance, accreditation and security standards to protect data in transit. If a buyer requires connectivity to a specific network, this is confirmed during onboarding and implemented in line with compliance requirements.

3.3.5 Data-in-transit protection

To ensure confidentiality and integrity, all data transmitted to and from the service is encrypted using Transport Layer Security (TLS) 1.2 or higher. This protects information between the buyer's network and our systems. To maintain security within our environment, internal system and microservice communication is encrypted. Secure API gateways enforce strong authentication and role-based access controls. For buyers with enhanced security requirements, we support Virtual Private Network (VPN) and IPsec connections for additional protection. Legacy, non-secure protocols are not supported.

3.3.6 Asset protection

To safeguard data at rest, all information is stored within secure UK-based data centres that comply with ISO 27001 and Cloud Security Alliance (CSA) Cloud Controls Matrix standards. Data is encrypted using Advanced Encryption Standard (AES) 256-bit encryption. To maintain logical separation, tenant data is isolated through role-based access controls and environment segregation. Data sanitisation follows industry best practice, using cryptographic erasure or secure deletion techniques to ensure information cannot be recovered. Any end-of-life hardware is disposed of in accordance with recognised standards, ensuring complete destruction of stored data and compliance with UK government security requirements.

3.4 Availability and resilience

3.4.1 Guaranteed availability

To ensure service continuity during unexpected events, Covoxa applies proven resilience measures across infrastructure, processes and recovery planning. Our service leverages leading cloud platforms such as Microsoft Azure, Amazon Web Services (AWS), Oracle Fusion and Workday. These platforms provide built-in redundancy and compliance with the National Cyber Security Centre (NCSC) 14 Cloud Security Principles.

Availability targets apply to Covoxa's support tooling (ticketing portal) where provided. ERP platform availability is provided by buyer's chosen vendor.

If an outage occurs, we provide timely updates through a public status page and email notifications. This ensures buyers remain informed and can plan accordingly. Daily backups and tested disaster recovery processes enable rapid service restoration. These measures minimise disruption and help buyers return to business as usual quickly.

Isolation between customer environments ensures independence of resources. This prevents cross-impact and safeguards data integrity across all hosted services. Our incident management process

includes root cause analysis and corrective actions. This reduces recurrence and strengthens overall service resilience.

3.5 Governance

To ensure professional delivery and compliance, Covoxa operates under a structured governance framework aligned with recognised standards. Our services follow the National Cyber Security Centre (NCSC) 14 Cloud Security Principles and hold **Cyber Essentials certification**. This ensures robust security and risk management throughout delivery. We align service management processes with ITIL v4 principles to support continual improvement and consistent quality. This approach helps maintain predictable outcomes and reduces operational risk. Performance data, customer feedback and audit findings are reviewed monthly. These reviews identify improvement opportunities and track corrective actions to maintain service excellence. Our Compliance Manager oversees governance of all management systems. This role reports to the board-level Quality and Security Committee to ensure accountability and transparency.

3.6 Security

To protect sensitive data and maintain compliance, Covoxa embeds security into every stage of service delivery. To ensure confidentiality, integrity and availability, we apply a comprehensive set of policies aligned to ISO 27001 and the UK government's cloud security principles. These controls reduce risk and safeguard buyer information.

To strengthen resilience against cyber threats, we hold Cyber Essentials certification and follow the National Cyber Security Centre (NCSC) 14 Cloud Security Principles. This ensures compliance with recognised government standards for cloud adoption.

To maintain secure data handling, we enforce strict access controls, encryption and secure disposal processes. To provide accountability, a board-level Security Lead oversees governance, risk management and compliance activities. This role ensures security remains a strategic priority.
To drive continuous improvement, security responsibilities, KPIs and audit outcomes are reviewed regularly. These reviews identify risks early and enable proactive mitigation.

To comply with UK General Data Protection Regulation (GDPR), buyer data is normally held on buyer-provided infrastructure. This approach minimises exposure and ensures compliance with data protection laws. Covoxa staff screening processes can conform to BS7858:2019 and achieve government security clearances up to Developed Vetting (DV) if required.

3.6.1 Operational security

To maintain service stability and protect buyer data, Covoxa applies structured operational security controls across all environments. To ensure secure and predictable changes, all configuration updates follow a formal assessment and approval process. This reduces risk and prevents unauthorised modifications. To minimise exposure to threats, we conduct regular vulnerability assessments and apply patches promptly. This proactive approach helps prevent exploitation and maintain compliance. To detect issues early, we use continuous monitoring supported by threat intelligence feeds, automated scanning and Security Information and Event Management (SIEM) tools. These measures enable rapid identification of suspicious activity. To respond effectively to incidents, we follow a documented response plan. This includes rapid triage, containment, resolution and reporting to affected buyers, ensuring transparency and trust. To strengthen resilience against emerging threats, we review operational security KPIs and audit outcomes regularly. This drives continuous improvement and proactive risk management.

3.6.2 Staff security

To protect buyer data and maintain compliance, Covoxa enforces strict staff security measures for all personnel with system or data access. Ensuring trust and integrity, all staff undergo background screening that meets Baseline Personnel Security Standard (BPSS) or BS7858:2019 requirements. This reduces insider risk and ensures suitability for sensitive roles.

To minimise exposure, access is granted on a strict least-privilege basis and protected through multi-factor authentication (MFA) and activity logging. These controls prevent unauthorised access and enable full traceability.

To support government projects, Covoxa can sponsor additional security clearances, including Security Check (SC) and Developed Vetting (DV), for designated roles. This ensures compliance with public sector security requirements. To maintain accountability, staff security responsibilities and clearance levels are reviewed regularly.

3.6.3 Secure development

- Minimising security risks and ensuring compliance, Covoxa applies secure development practices throughout the software lifecycle
- To prevent vulnerabilities early, we follow a secure software development lifecycle that includes threat modelling, code review and adherence to secure coding standards. This approach reduces defects and strengthens resilience
- To validate security controls, we use automated security testing during development. This ensures issues are identified and resolved before deployment

- To provide independent assurance, we commission regular penetration tests and secure development audits. These assessments confirm compliance with recognised standards and maintain buyer confidence
- To align with industry best practice, our development processes follow frameworks such as ISO 27034 and Cloud Security Alliance Cloud Controls Matrix (CSA CCM)
- To support continuous improvement, findings from audits and tests are reviewed and tracked. This enables proactive remediation and strengthens future releases

3.6.4 Identity and authentication

To ensure only authorised users access the system, Covoxa applies strong identity and authentication controls. To protect user accounts, access is managed through multi-factor authentication (MFA), single sign-on (SSO) and identity federation. These measures reduce the risk of credential compromise and simplify secure access. To enforce best practice, password policies meet recognised security standards and include complexity, expiry and lockout rules. Session management prevents unauthorised access by terminating inactive sessions promptly. To safeguard administrative functions, elevated permissions require MFA and strict approval. All privileged activity is logged for audit and review, ensuring accountability and transparency. To minimise risk, management interfaces are restricted to authorised personnel and protected by network-level controls.

3.7 Auditing

To provide transparency and support compliance, Covoxa maintains comprehensive audit capabilities across all user and system activities. To ensure accountability, audit logs capture all significant actions, including authentication events, data changes and administrative activity. This helps buyers track usage and investigate issues quickly. To give buyers full visibility, audit logs can be accessed in real time or delivered through scheduled reports. Logs can also be exported in open formats for compliance and investigation purposes. Maintaining transparency, supplier activity is logged and made available on request. This ensures buyers have complete oversight of all operational actions. To support regulatory requirements, logs are retained in line with buyer-defined retention periods.

3.7.1 Performance monitoring and metrics

To provide transparency and confidence, Covoxa monitors service performance continuously and shares meaningful metrics with buyers. Ensuring proactive management, we track key indicators such as system availability, response times and resource usage. This helps identify issues early and maintain service stability. To support informed decision-making, buyers receive regular performance reports and can request real-time data. Reports include usage trends, uptime statistics and any incidents logged. Driving continuous improvement, we analyse performance data alongside customer feedback and audit findings. This enables us to implement corrective actions and optimise service delivery.

3.7.2 Compliance and quality management

To ensure consistent quality and compliance, Covoxa operates under an integrated management system aligned with recognised industry standards. To assure professional delivery, our services follow ISO 9001 for quality management, ISO 20000-1 for IT service management and ISO 27001 for information security. These standards reduce risk and maintain predictable outcomes.

To strengthen security posture, we hold Cyber Essentials certification and embed the National Cyber Security Centre (NCSC) 14 Cloud Security Principles into our processes. This ensures compliance with UK government requirements. To drive continual improvement, we align service delivery with ITIL v4 principles. This structured approach supports efficiency, reliability and proactive service enhancement.

To maintain accountability, performance data, customer feedback and audit findings are reviewed monthly by Thursten Clements, Managing Director. These reviews identify improvement opportunities and track corrective actions. To ensure governance, our Compliance Manager oversees all management systems and reports to the board-level Quality and Security Committee. This provides transparency and strategic oversight.

3.8 Backup, restore & disaster recovery

To safeguard buyer data and maintain service continuity, Covoxa ensures ERP vendors apply robust backup and disaster recovery measures aligned with recognised standards.

Overview and governance

To minimise disruption, our Business Continuity Management (BCM) framework identifies potential threats, assesses impact and defines structured recovery procedures. A designated Incident Manager activates recovery protocols, coordinates communications and oversees restoration. We conduct risk reviews bi-annually and verify readiness through annual disaster recovery exercises.

3.9 Training

To ensure successful adoption and long-term value from cloud ERP solutions, Covoxa provides tailored training and knowledge transfer as part of every engagement. To maximise user confidence and reduce operational risk, training programmes are customised to buyer systems, workflows and user groups. This approach ensures relevance and accelerates adoption. Our training services typically include:

- End-user training: Instructor-led sessions or e-learning covering day-to-day functionality and process integration

- Train-the-trainer programmes: Developing in-house super-users to deliver ongoing local training and support
- Adoption workshops: Focusing on workflow changes, communication strategies and confidence-building for operational teams
- Reference materials: Bespoke user guides, process maps and quick-reference sheets provided in accessible digital formats

To align with organisational learning frameworks, we co-design training with buyer stakeholders. This collaborative approach ensures consistency with internal standards and maximises engagement. Supporting continuous improvement, we measure training effectiveness through participant feedback, completion records and post-training assessments. Findings are used to refine future sessions and enhance user experience.

3.10 Service pricing

To provide transparency and value for money, Covoxa offers clear and competitive pricing under the G-Cloud 15 framework. Our pricing model is based on standard G-Cloud terms and is published in the separate Pricing Document available on the Digital Marketplace. This document includes full details of day rates, role definitions and any optional services.

To give buyers flexibility, we offer multiple pricing options:

- Time and Materials (T&M): Charged per day for consultancy and support services
- Fixed-price engagements: Available for defined deliverables or project phases
- Outcome-based pricing: Negotiated for specific results where appropriate

Discounts may be available for longer-term engagements or volume commitments.

Free trials are not applicable for consultancy services, but we provide initial scoping sessions at no additional cost to help buyers define requirements.

All pricing is transparent, with no hidden charges. Any additional costs, such as training or bespoke deliverables, are clearly itemised in the Pricing Document.

3.11 Invoicing process

To provide clarity and predictability, Covoxa follows standard government invoicing and payment practices. Invoices are issued monthly in arrears unless otherwise agreed in the Call-Off Contract. This approach ensures buyers only pay for services delivered. Payment terms comply with the UK government's standard 30-day payment policy, supporting prompt settlement and financial transparency. Accepted payment methods include BACS transfer, purchase order (PO) and other standard government-approved channels. This ensures compatibility with public sector finance

systems. There is no minimum contract term for our services unless specified in the buyer's Statement of Requirements. Billing periods are flexible and aligned to the engagement scope. All invoicing is supported by clear itemisation of services, day rates and any agreed additional charges. Buyers can also access self-billing options where required.

3.12 Termination terms

To provide clarity and compliance, termination is governed by the Crown Commercial Service (CCS) G-Cloud 15 Call-Off Terms and Conditions. To give buyers flexibility, contracts can be terminated in accordance with these terms by providing written notice. This ensures buyers retain full control over service engagement.

Covoxa may terminate only in cases of material breach or non-payment, protecting both parties from undue risk. To maintain data security, all buyer information is handled in line with our offboarding and data-deletion process. This includes secure removal of data and confirmation of deletion. There are no early termination penalties unless specified in the buyer's Statement of Requirements. Any agreed notice periods will be documented in the Call-Off Contract.

4 SECURITY AND DATA GOVERNANCE

4.1 Data protection and encryption

Covoxa normally processes data within buyer environments. Where transfer or temporary processing is required, we apply TLS 1.2+ in transit and AES-256 at rest, with key management and access controls aligned to buyer policies. Secure API gateways provided by vendor platforms enforce strong authentication and role-based access controls. Covoxa configures and uses these gateways under buyer governance.

To protect sensitive information and maintain compliance, Covoxa applies robust encryption and network security measures across all environments. To ensure confidentiality during transmission, all data in transit is encrypted using TLS 1.2 or higher. This prevents interception and safeguards integrity between the buyer's network and our systems. To protect data within our network, internal traffic between system components is encrypted and routed through secure API gateways. Network segmentation and firewalls isolate critical services and reduce attack surfaces.

To strengthen security between networks, buyers may connect via VPN or IPsec tunnels for additional protection. These options provide secure, private channels for sensitive data exchange. To maintain data integrity at rest, all stored data is encrypted using AES-256 or equivalent standards. Encryption keys are managed through secure key-management systems with strict rotation and access controls.

4.2 Data at rest, storage locations and physical security

For this service, all buyer data we process is stored within the data centres operated by the relevant ERP platform vendors, such as Oracle, SAP and Workday. As such, data storage, physical security and environmental controls inherit the protections and certifications provided by those vendors.

Where requested, we can support buyers and ERP vendors to specify data residency requirements, including UK-only or EEA-based storage as subject to the capabilities of the selected platform. All data location support is agreed as part of the call-off process and documented within the Statement of Work.

4.3 Data sanitisation and disposal

To prevent data leakage and maintain compliance, Covoxa applies secure data sanitisation and equipment disposal practices aligned with NCSC guidance and ISO 27001 standards. To guarantee irrecoverable deletion, we use cryptographic erasure or secure overwrite methods before storage reuse or system decommissioning. These methods ensure deleted data cannot be recovered. To provide assurance, certificates of deletion or destruction are available on request. All sanitisation steps, authorisations and verification outcomes are logged and retained for audit purposes.

Sanitisation methods

- Cryptographic erase: Encryption keys are destroyed, rendering data unreadable.
- Secure overwrite: Data is overwritten using approved patterns and verified.
- Physical destruction: Media is shredded or crushed where sanitisation is not feasible.
- Degaussing: Magnetic media is degaussed where appropriate.

Equipment disposal

- Managed through accredited third-party destruction services or in-house processes compliant with ISO 27001, CAS(S) and CSA CCM.
- Certificates of destruction provided on request.
- Disposal follows environmental regulations and WEEE compliance.

Buyer options

- Request preferred sanitisation method based on data classification.
- Witness destruction activities on-site.
- Specify retention of certificates and supporting audit evidence.

To strengthen assurance, we review sanitisation outcomes after each exercise or disposal event and integrate lessons learned into updated procedures.

4.4 Security testing and assurance

To maintain system integrity and protect buyer data, Covoxa conducts regular security testing and assurance activities aligned with recognised standards. To identify vulnerabilities early, we perform scheduled penetration testing at least annually, or more frequently for major system changes. Tests are carried out by certified testers to ensure independent and accredited assurance.

Providing continuous protection, we use automated vulnerability scanning tools across all environments. Scans run on a defined schedule and after significant updates. Identified vulnerabilities are prioritised and remediated within agreed timelines based on severity. To strengthen resilience, we review test results and integrate findings into our security improvement plan. This ensures lessons learned are applied to future releases and operational processes. Maintaining transparency, buyers can request summaries of penetration test outcomes and remediation actions.

4.5 Configuration and change management

To maintain service stability and security, Covoxa applies a controlled, auditable change management process aligned with ITIL best practices. Reducing risk and ensuring predictability, all changes follow a formal process that includes impact assessment, approval, controlled deployment and post-implementation review. This prevents unauthorised or disruptive updates.

To maintain traceability, configuration items are tracked throughout their lifecycle in a Configuration Management Database (CMDB). This provides full visibility of components, version history and dependencies. To enable rapid recovery, version control and rollback procedures are in place for all critical updates. This ensures services can be restored quickly if issues occur. To strengthen governance, major changes are reviewed by a Change Advisory Board (CAB). This oversight ensures alignment with security, compliance and operational requirements. To protect against vulnerabilities, all changes undergo a security impact assessment before release. Findings are documented and addressed before deployment.

4.6 Information security management and certifications

To provide assurance and maintain compliance, Covoxa operates a robust information security management framework that has been independently certified. To protect buyer data and reduce risk, our services align with ISO 27001 for information security, ISO 20000-1 for IT service management and ISO 9001 for quality management.

We hold Cyber Essentials certification, embedding UK government security principles into our processes. To ensure ongoing compliance, we undergo annual audits and surveillance reviews by accredited certification bodies. Findings are tracked and integrated into our continuous

improvement programme. To maintain accountability, governance is overseen by a named Information Security Manager, supported by a board-level Quality and Security Committee. Thursten Clements, Data Protection Officer (DPO) supports our information security management.

4.7 Secure development and cryptography

To minimise vulnerabilities and strengthen resilience, Covoxa applies secure development practices and robust cryptographic controls. To prevent security flaws, we follow a Secure Software Development Lifecycle (SDLC) that includes code reviews, dependency scanning and automated security testing. All development adheres to OWASP Top 10 guidelines. To protect sensitive data, cryptographic controls include TLS 1.2+ for data in transit and AES-256 for data at rest. Encryption keys are managed through secure key-management systems with strict rotation policies.

4.8 Identity and access management

To ensure only authorised users access systems, Covoxa enforces strong identity and access controls. Reducing risk of unauthorised access, all administrative accounts require multi-factor authentication (MFA) and strict approval processes. Privileged activity is logged for audit and review. To simplify secure access, we support Single Sign-On (SSO) and identity federation using SAML and OAuth2 standards. This enables seamless integration with buyer identity systems.
To maintain least-privilege principles, access is role-based (RBAC) and reviewed regularly. Session management and automated lockouts prevent credential misuse.

5 SUPPLIER INFORMATION

5.1 About us

Covoxa is a UK-based consultancy founded in 2010, specialising in Enterprise Resource Planning (ERP) cloud solutions for public sector organisations. We combine deep industry knowledge with proven methodologies to deliver successful ERP transformations that align with organisational goals and government digital strategies including the Shared Services Strategy for Government.

Our mission is to empower organisations through cutting-edge ERP solutions that streamline back-office operations, improve efficiency and unlock long-term value. Collaboration is at the heart of our approach, ensuring shared goals and measurable outcomes. Our core expertise includes:

- Strategy and advisory services for Tier 1 ERP platforms such as Oracle Fusion, Workday and SAP
- Implementation and support services covering design, configuration, data migration, integration and testing
- Client-side advisory services for larger implementations

- Change management and user adoption strategies to maximise benefits and reduce risk

Why buyers choose Covoxa

✓ **Proven experience** delivering ERP programmes for central government departments and shared service clusters.
✓ **Independence** from ERP vendors and system implementers, ensuring impartial advice.
✓ **Certified professionals** with vendor-specific accreditations and extensive public sector experience.
✓ **Security and compliance** embedded in every engagement, supported by **Cyber Essentials certification** and alignment with **NCSC cloud security principles**.

Our values:

- Collaboration and partnership
- Innovation and excellence
- Integrity and accountability
- User-centric design
- Sustainability and long-term value

Covoxa is proud to be a UK-based SME committed to delivering social value proportionate to our size, supporting local communities and contributing to government sustainability goals.

5.2 Relevant experience and testimonials

To give buyers confidence in our capability, Covoxa brings extensive experience delivering complex ERP programmes for public sector organisations.

Client Side Advisory Services for a New ERP System Implementation: Working with a large Government Department at the heart of UK Government on a tier 1 ERP replacement programme Covoxa is providing client side advisory services for the design, configuration, data migration, testing and deployment of a full platform solution.

Enhancements and Improvements to an Existing ERP Installation: Contracted to this large central Government Department Covoxa are helping maximise an existing ERP investment by implementing solutions for emerging business priorities and exploiting new functionality from vendor periodic releases.

5.3 How to buy

Covoxa's services can be procured directly through the Crown Commercial Service (CCS) G-Cloud 15 Digital Marketplace.

Buyers can search for Covoxa on the Digital Marketplace and select the required service listing. Once selected, the buyer and Covoxa will:

- Agree a Statement of Work (SOW) detailing scope, deliverables, timescales and pricing
- Raise a Call-Off Contract under the G-Cloud framework terms
- Issue a Purchase Order (PO) to confirm commencement

Ensuring transparency and compliance with public-sector procurement regulations, all engagements are delivered in line with G-Cloud framework conditions.

Enquiries or pre-contract discussions can be arranged through our central contact point:

- Thursten Clements
- thursten@covoxa.co.uk
- 07979 576547