G-CLOUD 15 (RM1557.15) EMPIRIC PROFESSIONAL SERVICES LTD

SAAS ENABLEMENT, TRANSFORMATION AND OPTIMISATION FOR ENTERPRISE APPLICATIONS

SERVICE DEFINITION

JANUARY 2025

Table of contents

1 Introduction

1.1 Document structure

This Service Definition document provides information about the Software as a Service (SaaS) Enablement, Transformation and Optimisation Service offered by Empiric Professional Services (EPS) 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 provide clarity on how to engage with us through the framework.

The document is divided into 3 core sections:

- **Service description:** Provides an overview of the SaaS Enablement, Transformation and Optimisation Service, including service scope, features, delivery approach, security and compliance controls and the outcomes delivered to public sector customers
- **Operational delivery and G-Cloud alignment:** Sets out how the service is delivered within customer SaaS environments, including onboarding, support, service levels, resilience, exit management, data handling and alignment to G-Cloud 15 requirements
- **Supplier information:** Information on EPS's experience, credentials and how to procure our services through G-Cloud 15

Each section is structured to allow buyers to quickly locate the information most relevant to their stage in the procurement process.

1.2 How to use this document

Placeholder text:

This document is designed to support buyers at each stage of the G-Cloud procurement and service lifecycle, from initial service evaluation through to contract award, mobilisation and ongoing service management. The sections should be used as follows:

- **Early-stage evaluation and service suitability:** Section 2 (Service description) provides an overview of the EPS SaaS Enablement, Transformation and Optimisation Service, including service scope, delivery approach, features and key benefits. This section supports buyers in assessing alignment with organisational needs and intended use
- **Due diligence and contract preparation:** Section 3 (G-Cloud alignment information) sets out onboarding arrangements, service levels, support models, data handling, exit management and commercial principles. This section supports buyer assurance, internal approvals and call-off contract preparation
- **Security, data protection and continuity assurance:** Section 4 (Security and data governance) describes EPS's information security framework, data protection arrangements, business continuity measures and alignment to relevant standards and statutory requirements
- **Supplier verification and procurement:** Section 5 (Supplier information) provides background information on Empiric Professional Services Limited, relevant accreditations and guidance on how the service can be procured through the G-Cloud 15 Framework

2 Service description

2.1 About our service

Our SaaS Enablement, Transformation and Optimisation Service provides a structured, managed service layer that operates within customer-owned SaaS environments.

Drawing on over 20years' experience delivering specialist technology services across regulated public sector and enterprise environments, we specialise in supporting organisations to adopt, stabilise, optimise and enhance live enterprise SaaS platforms. We support clients in maximising value from their existing SaaS investments by leading business transformation, configuration, process redesign, data migration, governance, user adoption and hypercare.

The service is designed for organisations operating complex, high-impact SaaS platforms such as ERP, finance, HR, property management and line-of-business systems. It supports customers at critical stages of SaaS adoption, including post-go-live stabilisation, transformation recovery, optimisation and operational transition.

EPS does not provide hosting, infrastructure or SaaS licences. Instead, the service operates as a vendor-independent enablement and optimisation layer, integrating directly into customer IT service management frameworks, governance models and security controls. This allows buyers to adopt, improve and extend their existing SaaS investments without introducing parallel systems or unmanaged technical risk.

The service is delivered as a repeatable, on-demand managed service. This enables public sector buyers to procure a defined, assured and auditable SaaS enablement capability through the G-Cloud 15 Framework.

2.2 What the service delivers

We provide structured, outcome-focused support across the full lifecycle of public sector SaaS environments, including helping organisations to:

- Overcome failed, delayed or high-risk SaaS implementations
- Stabilise large-scale SaaS transformations following go-live through extended hypercare and optimisation
- Migrate data from legacy systems into SaaS platforms safely and efficiently
- Redesign and automate inefficient or manual business processes
- Improve user adoption and business outcomes from SaaS investments
- Establish governance, reporting and operating models around SaaS platforms
- Reduce risk, disruption and operational instability during major system change
- Integrate with adjacent systems through Application Programming Interface (APIs), Extract, Transform, Load (ETL) or middleware

The service management functions provided through this service include:

- Demand and change management
- Incident, defect and hypercare management
- Risk, issue and dependency tracking
- Service transition and operational readiness planning
- Operational handover and governance alignment

EPS integrates directly into each customer's existing service management ecosystem, using client-owned tools, processes and governance frameworks wherever possible. This includes alignment with platforms such as ServiceNow, Jira, Azure DevOps and other customer-approved IT service management (ITSM) and delivery toolsets. This integrated delivery model allows buyers to adopt the service without introducing parallel tooling or unmanaged technical risk and supports consistent operational control across live SaaS environments.

2.2.1 What makes EPS different

The EPS SaaS Enablement, Transformation and Optimisation Service is differentiated by its delivery maturity and integration-first operating model. Key differentiators include:

- Proven delivery experience within regulated public sector and law enforcement environments, including central government and security-sensitive organisations
- Practical SaaS transformation and recovery delivery capability, not limited to advisory consultancy
- Integration-first delivery that operates within customer-owned platforms, tools and governance frameworks
- Strong governance and assurance controls, including structured reporting, risk and dependency management
- Security-by-design delivery model operated by security-cleared personnel under Cyber Essentials Plus controls
- Flexible commercial models supporting milestone-based, outcome-based and time-and-materials delivery
- Scalable delivery capability enabling rapid resourcing to meet programme demand

These characteristics support lower operational risk and higher adoption rates when compared to traditional consultancy-led delivery models.

2.3 Who the service is for

This service is designed for UK public sector organisations operating enterprise SaaS platforms, including:

- Central government departments and arm's-length bodies
- Local authorities and combined authorities
- Public sector property and estates organisations
- Police forces and law enforcement bodies
- Other public sector organisations operating regulated SaaS environments

The service is particularly suited to high-risk, high-impact SaaS programmes where continuity of operations, security, governance and adoption are critical to service delivery.

2.4 Delivery framework

Our service is delivered through a structured, repeatable lifecycle aligned to recognised public sector delivery and service management practices, including:

- Agile delivery methods
- Information Technology Infrastructure Library (ITIL) v4 service management principles
- PRINCE2-informed programme governance

Delivery follows a defined lifecycle comprising: Mobilisation and Discovery, Stabilisation and Risk Control, Optimisation and Transformation, Hypercare and Assurance, and Service Transition and Handover. Please refer to the below flow chart:

Mobilisation and Discovery

We start by understanding your objectives, operating environment and governance requirements for your SaaS platforms. To establish a controlled and auditable delivery baseline, we will confirm access, reporting, security controls and service arrangements.

Stablisation

We assess the live SaaS environment to identify risks, defects and dependencies that may impact service continuity. To reduce disruption and maintain operational stability, we implement immediate stabilisation actions and controlled change arrangements.

Optimisation and Transformation

We improve system performance, data quality and business processes through configuration, automation and integration enablement within the SaaS platform. These changes are delivered in line with agreed governance and reporting controls to support measurable improvement.

Hypercare and Assurance

To confirm system stability and user adoption, we provide enhanced support and monitoring following changes. To provide assurance and maintain service continuity, we will formally report on performance, incidents and risks.

Service Transition and Handover

We complete knowledge transfer, documentation handover and operational readiness activities to embed the service into business-as-usual operations. EPS access is removed and formal closure reporting is completed to support a clean and auditable exit.

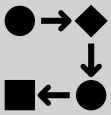
Each phase includes formal governance checkpoints, risk and dependency management, change control and structured reporting. This lifecycle supports controlled change, enabling buyers to adopt and improve SaaS platforms with reduced operational risk and a clear route into business-as-usual operations.

2.5 Service features / benefits

The SaaS Enablement, Transformation and Optimisation Service provides a structured set of features designed to stabilise, improve and protect live public sector SaaS environments. Below, we have highlighted what we deliver and the practical benefits our customers see as a result:

SaaS transformation programme delivery: Structured governance and delivery of SaaS transformation and recovery programmes

✓ **Maintains control over complex SaaS programmes and reduces delivery risk**



Post-go-live hypercare and stabilisation: Enhanced support following deployment

✓ **Accelerates stabilisation of live platforms and limits operational disruption**

Business process redesign and automation: Redesign and automation of processes within SaaS platforms

✓ **Streamlines processes and reduces manual effort**

Data migration and validation services: Safe migration and reconciliation of legacy data

✓ **Delivers reliable data migration with confidence in accuracy and completeness**

SaaS platform optimisation: Configuration, performance and usage optimisation

✓ **Improves system performance, usability and adoption**

Change and adoption enablement: User adoption and training coordination

✓ **Drives consistent usage through structured change and training**

Governance and reporting set-up: KPI frameworks and dashboards

✓ **Provides clear oversight and informed decision-making**

Interoperability and integration support: API and integration enablement

✓ **Enables secure, effective integration with existing systems**

Service transition and operational handover: Structured transition into business-as-usual

✓ **Supports a controlled transition into business-as-usual operations**

Risk, assurance and compliance management: Structured risk and compliance controls

✓ **Reduces exposure to delivery, audit and regulatory risk**

2.6 Service scope

2.6.1 Add-ons and extensions

Our service operates as an enablement and optimisation layer around customer-owned enterprise SaaS platforms. It extends and enhances existing SaaS platforms, including (but not limited to):

- Enterprise Resource Planning (ERP) SaaS platforms
- Finance, HR, property and line-of-business SaaS systems
- Customer-approved SaaS platforms such as ServiceNow and equivalent ITSM solutions

The service enhances configuration, governance, adoption, reporting, data migration and optimisation capabilities without replacing or reselling the underlying SaaS software.

All enablement and optimisation activities are delivered through SaaS-native APIs, approved integration layers and customer security and governance frameworks.

2.6.2 Cloud deployment model

The service is delivered within customer-owned public cloud and hybrid cloud SaaS environments.

Customer production data remains hosted within the buyer's SaaS platforms, which are typically hosted in UK-based public cloud environments aligned to public sector data residency requirements.

Where hybrid deployments are used, the service supports integration between public cloud SaaS platforms and on-premises or private cloud systems using customer-approved integration and security architectures.

EPS does not host customer production data or operate proprietary cloud platforms.

2.6.3 Service constraints

The service is delivered within the following standard constraints:

- Access to relevant customer systems, environments and stakeholders must be provided in line with agreed onboarding arrangements
- Delivery within regulated or secure environments is subject to appropriate access approvals and security clearances
- EPS does not provide hosting, infrastructure or SaaS software licences
- All changes impacting live environments are delivered in line with customer change and maintenance windows
- On-site activities are subject to site access, health and safety and local security requirements
- Deliverables and timescales may be affected by third-party vendor dependencies, infrastructure readiness and customer governance cycles
- Standard delivery hours are 09:00 to 17:30 UK time, Monday to Friday, excluding public holidays, unless otherwise agreed

2.6.4 System requirements

Keeping adoption straightforward, we deliver our service entirely within our customers' existing infrastructure and approved tools, with no need for dedicated hardware or proprietary installations. EPS does not provide a proprietary software application. System requirements are therefore governed by the customer's chosen SaaS platforms and internal IT standards.

To achieve optimal performance and a smooth experience, the following baseline requirements apply:

Requirement	Details
Supported browsers	Allowing teams to access the service without changing their usual workflow, we operate through standard web interfaces compatible with Microsoft Edge, Google Chrome, Mozilla Firefox and Safari (latest versions).
Operating systems	The service supports Windows 10/11, macOS, major Linux distributions, iOS and Android (latest 2 versions). This flexibility means your teams can work from the devices they already use.
Connectivity	A stable broadband connection is recommended for remote delivery and collaboration. Our service is designed to function efficiently even in varied network conditions, but a reliable connection helps optimise performance.
SaaS licences	Valid licences for customer-owned SaaS platforms will be required.
Integration options	All integrations use customer-approved frameworks, APIs and governance standards. For compliance and compatibility with customer environments, no proprietary connectors or middleware are required.

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

2.7 Reselling

EPS does not resell, license or distribute third-party cloud platforms, infrastructure or SaaS products. Our SaaS Enablement, Transformation and Optimisation Service operates as a managed enablement and optimisation layer within customer-owned SaaS environments. All underlying SaaS platforms, licences, hosting and infrastructure remain procured, owned and managed directly by the buyer.

2.8 User support

Ensuring your teams can tackle issues promptly without unnecessary delays, we provide expert support at every stage. Every query is handled by a qualified consultant with hands-on experience in SaaS optimisation. This approach gives our customers confidence that issues are resolved efficiently and correctly, while integrating smoothly with their existing service management processes.

Support is accessible through channels customers already use, including email, scheduled calls and collaboration tools such as Microsoft Teams or Slack. Avoiding the need for a separate system, where formal ticketing is required, we work directly within customers' platforms such as ServiceNow, Jira or Azure DevOps.

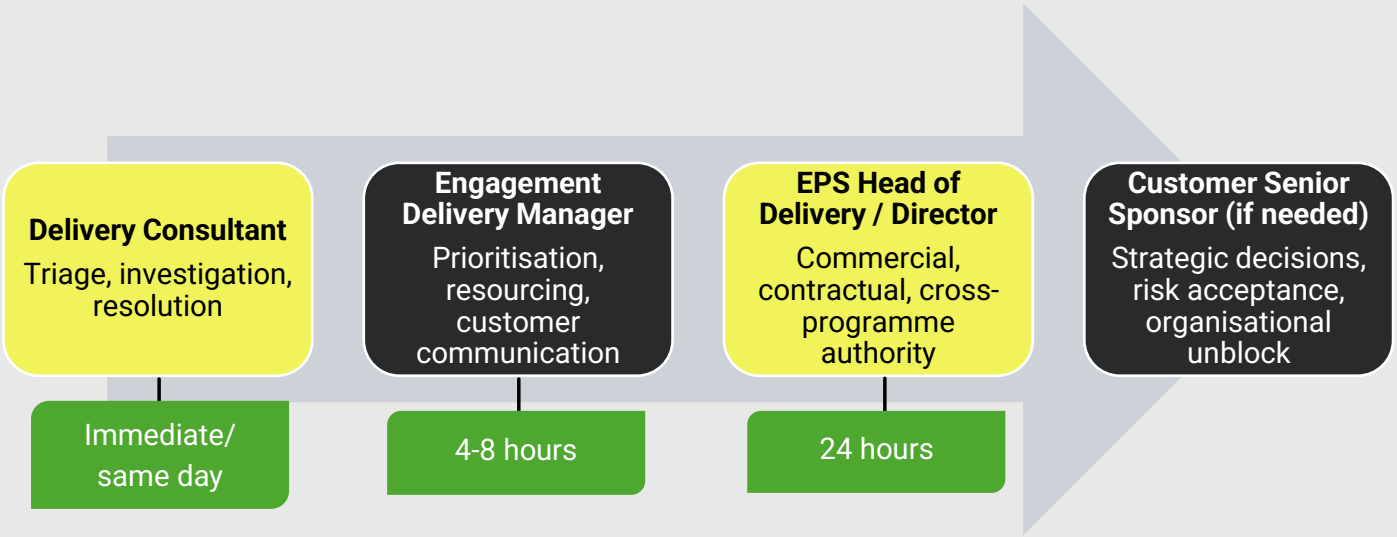
2.8.1 Support details

To keep projects on track, customers can rely on us to deliver support during core UK business hours (Monday to Friday, 09:00–17:30, excluding public holidays). Reducing the risk of disruption, we can also extend coverage for critical phases such as migrations, cutovers or hypercare.

We typically acknowledge standard enquiries within 1 business day. To support critical delivery needs, we can agree faster response times for high-priority programmes.

To address issues quickly and without ambiguity, every engagement includes a named Engagement Delivery Manager who acts as the single point of accountability. Creating a clear chain of responsibility,

they are supported by a Lead Consultant or Project Manager. This escalation model operates throughout the engagement and is time-bound and severity-based, providing rapid access to delivery, technical, commercial, and executive authority when required. The Engagement Delivery Manager retains end-to-end accountability for driving issues through to resolution and maintaining clear, proactive communication with the customer. If issues need escalation, the path for resolution is simple and transparent:



We don't rely on standalone web chat platforms or automated chatbots. Instead, we deliver our support through the collaboration tools your teams already use, with real, experienced consultants handling every enquiry. Where needed, authorised third-party contractors can also access these channels, always in line with specific governance policies.

2.8.2 Accessibility and usability

To make our service easy to use for everyone, we design accessibility into every interface, document and support channel from the start. This includes users who rely on assistive technologies so they can engage with the service confidently and independently. To meet public-sector expectations and regulatory requirements, our approach aligns with WCAG 2.2 (A, AA and AAA where applicable) and EN 301 549, with accessibility treated as a core design principle.

Allowing services to be adopted smoothly without rework or adjustment, we integrate accessibility considerations throughout discovery, design and implementation. Our consultants work within each customer's governance and assurance frameworks. This means organisational accessibility policies are met while avoiding unnecessary complexity or disruption.

To prevent accessibility issues from reaching end users, we carry out testing during major releases and service updates. Giving us both coverage and real-world insight, we use a balanced approach that combines automated tools such as Axe and WAVE with hands-on testing using assistive technologies, including JAWS and NVDA.

To continually improve the experience, we document testing outcomes and feed lessons learned directly into our improvement cycle. Ensuring our service continues to evolve in line with real user needs, we review accessibility feedback gathered during user-centred design workshops, applying it to future iterations.

To ensure accessible day-to-day communication and support, we work entirely within customer-owned ticketing and collaboration platforms such as ServiceNow, Jira and Microsoft Teams. These tools already support keyboard navigation and screen readers, which allows users to interact through familiar, compliant

environments. Reducing accessibility risk and keeping interactions consistent with established standards, we deliberately avoid introducing proprietary chat or chatbot tools.

To provide clear, usable information that supports understanding and adoption, we supply documentation in accessible formats including WCAG-compliant HTML and PDF. Where needed, we also offer alternatives such as large print, plain text or audio. Helping reduce cognitive load, we design training materials, process maps and quick-reference guides with clarity in mind. This makes it easier for users to find, understand and apply the information they need.

2.9 How users work with our service

2.9.1 Browsers

Our service is accessible through all modern, standards-compliant web browsers. We support the latest versions of:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox
- Apple Safari

For full functionality, we recommend enabling JavaScript and cookies. Supporting compatibility and uninterrupted access, buyers are notified in advance of any changes to browser support.

2.9.2 Desktop application

Our service does not require users to install any dedicated desktop application. We work within our customers' existing SaaS platforms and approved tools, using secure access methods already in place.

By working through familiar web interfaces and management consoles, we make sure our service:

- ✓ Fits smoothly into your current workflows
- ✓ Respects enterprise security policies
- ✓ Avoids disrupting day-to-day operations

2.9.3 Mobile

EPS does not provide a proprietary mobile application as part of this service. The service operates within customer-owned SaaS platforms and environments, which may provide native mobile applications or mobile-responsive web interfaces.

Where customer SaaS platforms support mobile access, EPS ensures that any configuration, optimisation, automation and adoption enablement activities delivered through this service are compatible with mobile-enabled workflows and user interfaces.

Mobile access, device compatibility, offline functionality and notification features are governed by the customer’s chosen SaaS platforms and mobile device management policies.

2.9.4 Service interface

To minimise disruption and reduce the learning curve, we do not introduce a proprietary interface and instead work entirely within customer-approved platforms and tooling. To make day-to-day interactions simple and efficient, these interfaces are typically role-based, mobile-responsive and designed for intuitive navigation.

Helping users get value quickly, we provide access to dashboards, reports and service management functions through familiar tools such as ServiceNow, Jira and cloud platform consoles. This means we can

maintain consistency with existing ways of working and allow teams to operate confidently without retraining.

To support fast task completion and consistent usability across devices, we design all documentation and service artefacts using clear user interface patterns and align them with WCAG 2.2 AA accessibility standards.

2.9.5 API

To reduce risk and avoid introducing unnecessary dependencies, we do not provide a proprietary API as part of our service. Ensuring integrations align with existing governance and security controls, we carry out all configuration and integration activities using customer-approved APIs within their existing platforms, such as cloud services and IT Service Management (ITSM) tools.

Where customer SaaS platforms provide APIs, EPS supports buyers to use these interfaces to:

- Configure workflows, modules and business rules
- Enable and manage integrations with adjacent systems
- Support data migration, reconciliation and validation activities
- Configure reporting, dashboards and automation routines
- Manage access controls and role-based permissions

Making integrations easy to understand and maintain, we rely on vendor-provided API documentation, typically available in OpenAPI (Swagger), HTML and PDF formats. To ensure changes are validated safely before go-live, we work within customer-owned sandbox or test environments to verify API connectivity and configuration before production deployment.

2.9.6 Accessibility and usability

By working entirely within customer-approved platforms, we give users an accessible experience they can trust from day 1. These platforms typically align with WCAG 2.2 AA and EN 301 549 and provide role-based, mobile-responsive interfaces that support keyboard navigation, screen readers, high-contrast mode and scalable text.

We keep the service intuitive and practical for everyday use by validating usability throughout delivery. Customer-led testing and EPS playback sessions help confirm that interfaces remain easy to navigate and accessible for all users, including those who rely on assistive technologies.

2.9.7 Customisation

This service provides extensive configuration and optimisation capability within customer-owned SaaS platforms, allowing buyers to tailor workflows, data structures and user experiences to local operational needs without custom software development. Customisable elements typically include:

- Business workflows, approval routes and automation rules
- User roles, permissions and segregation of duties
- Reports, dashboards and analytics views
- Data models, fields and validation rules
- Notifications and service alerts

Configuration can be performed by authorised buyer administrators within their SaaS platforms. Where required, EPS provides structured support to design, implement and document more complex configurations, subject to customer change control and governance arrangements. All configuration changes are delivered using SaaS-native tools and remain fully supported by the underlying SaaS providers.

2.9.8 Service levels and availability

The following Service Level Agreements (SLAs) define the responsiveness and performance standards for our consultancy service under G-Cloud 15. These SLAs focus on engagement responsiveness rather than platform uptime, as we do not operate hosted systems.

Metric	Target	Measurement / Reporting
Response to enquiries	Within 1 business day	Logged via email/customer ticketing
Issue acknowledgement	Within 1 business day	Service desk or agreed communication
Progress reporting	Weekly or as agreed	Governance reports/dashboards
Escalation resolution	Agreed within 1	Documented in governance logs

Performance monitoring: To give customers clear visibility and confidence in service performance, we track all SLAs through customer-approved ITSM tools, such as ServiceNow and Jira. To confirm compliance and identify opportunities for improvement, we review performance regularly through governance meetings and provide structured reporting that highlights trends.

Escalation and corrective actions: To resolve issues quickly and minimise impact, any SLA breach triggers immediate escalation to the Engagement Delivery Manager and, where necessary, EPS senior leadership. We carry out root-cause analysis and implement corrective actions using our ITIL-aligned service management framework. Service credits apply only where they are explicitly defined in the contract.

Resilience and continuity: To maintain consistent service delivery under changing conditions, we operate with remote delivery capability, backup communication channels and clear resource substitution plans. As EPS does not host customer systems, technical resilience remains governed by the customer's own infrastructure controls. This ensures continuity aligns with existing operational and security arrangements.

3 G-Cloud alignment information

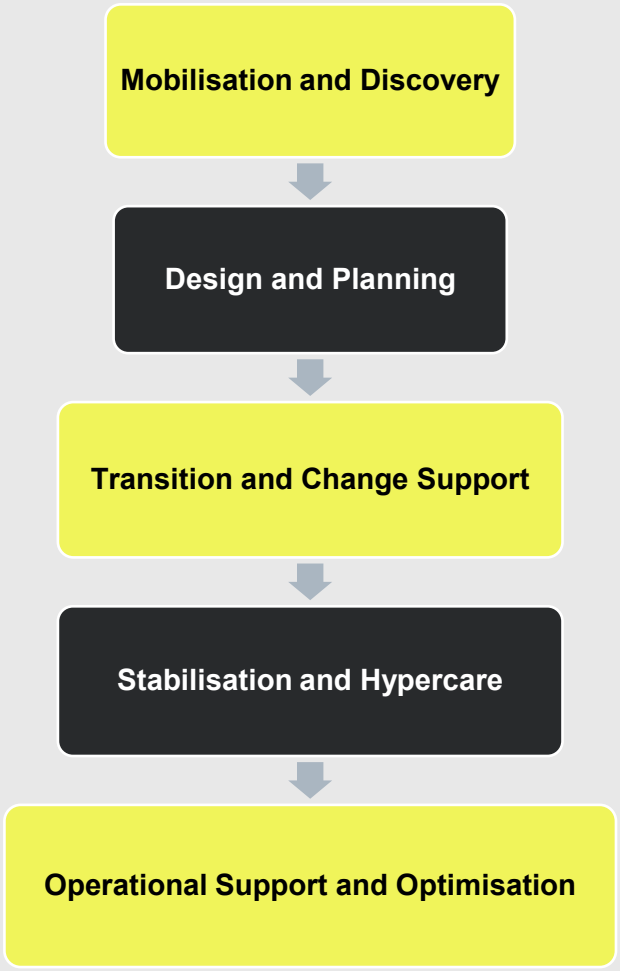
3.1 Section introduction

To give buyers a clear understanding of what happens after purchase, this section explains how we deliver and manage our SaaS Enablement, Transformation and Optimisation Service through the G-Cloud framework. It focuses on onboarding, governance, service management and ongoing support throughout the contract term.

To support complex public-sector SaaS environments without slowing delivery, we use a structured yet flexible delivery model. Allowing us to mobilise quickly while maintaining control and transparency, our approach combines ITIL-aligned service management, Agile practices and strong governance.

Delivery lifecycle overview

The diagram below provides a high-level view of the lifecycle, showing how we phase each engagement from initial assessment to ongoing optimisation.



Phase descriptions

To ensure accountability and continuous improvement from start to finish, this lifecycle provides clear ownership, decision points and feedback loops, fully aligning with G-Cloud 15 requirements.

1. **Mobilisation and Discovery:** This phase establishes a clear understanding of the buyer's objectives, governance structures and live SaaS environment. EPS works with stakeholders to confirm access arrangements, security controls, service management frameworks, risks and dependencies. Outputs include agreed scope, onboarding plan, baseline risk and dependency log and governance alignment

2. **Design and Planning:** EPS supports the design of target-state SaaS configuration, reporting and governance approaches. A phased optimisation and improvement plan is developed, aligned to buyer approval processes, service management frameworks and delivery priorities
3. **Transition and Change Support:** EPS coordinates and assures controlled changes within live SaaS platforms, including optimisation releases, data migration activities and integration enablement. Formal change governance, assurance checkpoints and escalation routes are applied to reduce disruption and maintain continuity
4. **Stabilisation and Hypercare:** EPS provides enhanced hypercare following changes to confirm stability, monitor incidents and performance, and support rapid issue resolution. Knowledge capture and operational readiness activities are completed to prepare services for steady-state support
5. **Operational Support and Optimisation:** EPS provides ongoing support, governance and optimisation activities aligned to ITIL principles and customer service management frameworks. Continual improvement, performance and adoption reviews, and structured reporting support long-term service control and value realisation

3.2 Onboarding and offboarding processes

3.2.1 Onboarding

To establish governance, security, access and delivery readiness for live SaaS environments, we operate a structured onboarding and mobilisation process:

1. **Organisational context and service objectives:** EPS works with the buyer to understand organisational objectives, operating environment, governance frameworks and service constraints for the SaaS platforms in scope. This establishes service priorities, success measures, risks and dependencies and confirms how the service will operate within existing service management structures
2. **Service overview and delivery objectives:** Providing a shared understanding of how the service will operate, a formal mobilisation meeting is held to confirm:
    - Service scope and objectives
    - Roles, responsibilities and escalation routes
    - Governance, reporting and assurance arrangements
    - Delivery priorities, dependencies and risks
3. **Onboarding documentation and service pack:** Buyers receive structured onboarding documentation, including:
    - Service operating model
    - Points of contact and escalation routes
    - Support and reporting arrangements
    - Security, data protection and acceptable use guidance
    - Change and assurance controls
4. **System and access provisioning:** All access is provisioned in line with buyer security policies and least-privilege principles. EPS supports the provisioning of required system access within customer SaaS environments, including:
    - User account creation and role-based permissions
    - Identity and access management alignment
    - Integration and platform access
    - Tooling and reporting access

5. **Security and compliance readiness:** Where required, EPS supports identity verification, security clearance validation and compliance with information security and physical security requirements prior to service commencement
6. **Service mobilisation and commencement:** A formal mobilisation session confirms service readiness, governance controls, escalation routes and immediate delivery priorities. This marks the transition into active service delivery
7. **Stakeholder integration:** EPS facilitates structured integration with customer delivery, technical and operational stakeholders to establish clear ownership, communication routes and escalation structures
8. **Transition to steady-state delivery:** Once onboarding is complete and the buyer confirms readiness, the service transitions into steady-state delivery with agreed service levels, reporting and governance processes activated

3.2.2 Offboarding

To support a clean exit and continuity of service, our structured offboarding process will be jointly planned and agreed upon between the buyer and EPS. On notification of exit, an agreed offboarding plan is initiated covering the following steps:

1. **Knowledge transfer and delivery artefacts:** EPS supports structured handover of all relevant delivery materials, which may include:
    - Service documentation and delivery artefacts
    - SaaS configuration records and optimisation documentation
    - Data migration, validation and assurance reports
    - Operational procedures, governance controls and reporting frameworks

Targeted handover sessions can be provided to support continuity for customer teams or successor suppliers.

2. **Data handling and portability:** Where applicable, EPS supports buyer-led data extraction activities from SaaS platforms, including validation, reconciliation and secure transfer. EPS does not retain customer production data beyond the engagement period
3. **Identity and access closure:** All EPS physical and logical access to customer environments is:
    - Formally revoked
    - Confirmed as deactivated
    - Logged and auditable

    This includes user accounts, administrative permissions, integration credentials and API access.
4. **System and service access revocation:** All system, integration and service management access is formally removed in line with buyer security policies and governance requirements
5. **Closure review and service confirmation**: A formal closure review is completed to confirm that all contractual obligations have been met, service artefacts have been handed over and the buyer has accepted closure
6. **Service termination:** Formal written confirmation of service termination is provided where required. Additional optimisation or advisory support can be provided under a new Statement of Work.

This offboarding model supports secure exit, knowledge continuity and full service portability across public sector SaaS environments.

3.3 Data

3.3.1 Data importing and exporting

To give buyers full control over their data, we do not host or store customer information. All data remains in the customer's environment throughout the engagement, avoiding vendor lock-in and keeping responsibility with the organisation.

To make data import simple and reliable, we use customer-approved tools and platforms. Ensuring compatibility with existing systems and avoiding proprietary constraints, we handle structured imports in open formats such as CSV, Excel (XLS/XLSX), XML or JSON.

To allow unrestricted access to data, we enable export at any time using the client's platform capabilities, including SQL exports, reporting tools, or native cloud platform functions. We provide guidance and scripts if required, without limiting or controlling extraction.

To manage end-of-contract handover efficiently, we provide all deliverables, configuration documentation and transformation details in open, non-proprietary formats (CSV, PDF, XML, JSON). We also securely delete any incidental working files within 30 days of project closure.

3.3.2 Analytics

To give buyers clear, real-time insight into service performance, we provide dashboards, monthly service reports and structured governance updates. These tools track key metrics such as:

- Environmental health and performance
- Configuration and change activity
- Incident and problem resolution trends
- Migration progress and milestone tracking

To make data actionable and easy to use, we deliver reports in HTML and PDF formats, with CSV or Excel exports for integration with external BI tools. Allowing advanced analytics and automated reporting, where customer platforms support APIs, we enable programmatic access to service data.

To support effective decision-making and proactive risk management, we ensure all reporting is timely, accurate and aligned with governance requirements.

3.3.3 Independence of resource

To give buyers full control and isolation, we deliver all work within customer-owned SaaS environments. This means each buyer's production data, configuration and system performance are isolated within their own SaaS platform and hosting arrangements. This ensures complete separation of systems and data:

- **No multi-tenant risk:** Each engagement runs entirely within the client's infrastructure, so other customers cannot affect performance or availability
- **Resource control:** Compute, storage and network resources remain under the client's governance, with us working inside those boundaries
- **Performance assurance:** We apply structured planning and scheduling to avoid contention and maintain consistent delivery quality

3.3.4 Public sector networks

We do not operate our own network or hosting platform. All work is performed within customer-owned SaaS platforms and approved network environments. If a customer requires integration with specific public sector networks (such as PSN, HSCN, JANET, PNN, SWAN), this is managed entirely within their environment and governance framework.

We support these requirements by:

- Working with customer security and network teams to validate compliance with relevant standards
- Following all accreditation and assurance processes for secure connectivity
- Ensuring that all configuration, optimisation and integration activities maintain network integrity, confidentiality and availability

Any network-specific requirements are confirmed during onboarding and delivered in line with public-sector security and governance policies.

3.3.5 Data-in-transit protection

To ensure all data remains secure, we protect data in transit through the security controls of customer-owned SaaS platforms and approved network environments. This protects sensitive information while keeping control firmly with the customer.

Where EPS accesses customer systems, we will use:

- TLS 1.2+ encryption: Secures web-based access and API calls, preventing interception
- VPN or IPsec tunnels: Used where required by client security policies to safeguard network traffic
- Multi-factor authentication (MFA) and secure access controls ensuring only authorised EPS consultants can access systems

Aligning with G-Cloud 15 requirements for secure, auditable consultancy activity, we do not use legacy or non-secure protocols. All work is carried out under the client's governance framework.

3.3.6 Asset protection

To ensure buyers retain full control over their data, we do not host or store customer production information**.** All data remains within the customer's environments, either on-premises or in their chosen cloud region. All customer data is stored and processed within customer-owned SaaS platforms and approved hosting environments. These are typically hosted within UK-based data centres aligned to recognised security and resilience standards such as ISO/IEC 27001. Other asset protection measures we implement include:

Data at rest protection: We operate strictly within the customer's platform and security controls, including encryption at rest, key management and role-based access. We do not move or replicate data outside the customer's environment.

Datacentre and security standards: When customers SaaS platforms are hosted within third-party data centres or cloud providers, compliance with standards such as ISO 27001 is the responsibility of the buyer or provider. We align with client governance and provide configuration and support activities without introducing additional hosting.

Data sanitisation: We minimise temporary data and securely delete all working materials, including documentation drafts, anonymised extracts and screenshots stored in collaboration tools. We complete deletion within 30 days of project closure, or sooner if requested and provide written confirmation to the client.

Hardware disposal: We do not operate customer infrastructure or store production data on EPS devices. Disposal of hardware and storage media is managed entirely by the customer under their own standards and EPS retains no custody of any equipment or media.

3.4 Availability and resilience

3.4.1 Guaranteed availability

EPS delivers this service within customer-owned SaaS platforms and hosting environments. Availability and platform-level resilience are therefore provided by the buyer's SaaS vendors and cloud providers, which typically operate multi-availability-zone, geographically resilient datacentre architectures aligned to recognised security and resilience standards.

EPS guarantees 99.99% service availability during core service hours (09:00–17:30, Monday to Friday) for its enablement, optimisation and support service activities. Availability is monitored through customer ITSM platforms and EPS service reporting.

Continuity is supported through:

- Formal change and release governance to prevent unplanned disruption
- Risk, dependency and issue management
- Structured escalation routes and hypercare support
- Alignment to customer disaster recovery and business continuity frameworks

Where service-impacting incidents occur, EPS coordinates outage reporting and recovery activities through customer ITSM systems, SaaS vendor dashboards and formal escalation routes. Root cause analysis and corrective action planning are completed following any material incidents.

3.5 Governance

Our services are delivered under a fully integrated management system aligned to recognised public sector and international standards, including:

- ISO 9001 – Quality management
- ISO 27001 – Information security management
- Cyber Essentials Plus – Cyber security assurance
- ITIL v4 – Service management and continual improvement principles

To identify improvement opportunities and track corrective actions, performance data, customer feedback and audit findings are reviewed monthly.

Governance of all management systems is overseen by Mailyn Sheik, Compliance Manager, who reports to the board-level Quality and Security Committee.

3.6 Security

To protect the confidentiality and integrity of our Enablement, Transformation and Optimisation Service, we embed security into the design and delivery of the service.

For effective leadership oversight, the service and delivery team will hold accountability for information security governance, risk management and compliance. To reduce the risk of breaches and operational disruption, we formally approve, review and enforce security policies all service delivery activities. Our approach includes:

- Information security and data protection policies aligned to UK GDPR and the Data Protection Act 2018

- Access control, identity management and least-privilege principles
- Secure endpoint management and encrypted communications
- Incident and breach response procedures aligned to ISO 27035
- Change and configuration management controls
- Third-party and supplier security governance

We review security performance, audit outcomes and risk registers through formal governance processes, with corrective actions tracked to completion. All staff receive mandatory security awareness training and are subject to formal screening prior to system access being granted.

3.6.1 Operational security

To maintain service stability and provide continuous assurance across live SaaS environments, we operate formal operational security controls, including:

- **Controlled change:** All configuration, optimisation and delivery changes are subject to formal change control aligned to ITIL v4 and ISO 27001. To prevent unplanned disruption, changes are risk-assessed, approved through governance routes and implemented within agreed change windows. Emergency changes follow defined expedited approval and post-implementation review processes
- **Rapid vulnerability management:** EPS actively monitors vendor security advisories, NCSC guidance and threat intelligence feeds. Vulnerabilities are assessed immediately on identification, prioritised based on risk and remediated in line with defined patching timeframes. High and critical vulnerabilities are escalated and addressed as a priority, with customer notification where required
- **Continuous monitoring:** Protective monitoring includes log collection, access monitoring and anomaly detection across EPS-managed delivery environments and endpoints. This supports early detection of suspicious activity, operational issues and security events
- **Professional incident management:** EPS operates documented incident and breach response procedures aligned to ISO 27035. Incidents are triaged rapidly, escalated through formal governance routes, and managed through containment, remediation and root-cause analysis, with timely customer communication and corrective action planning

3.6.2 Staff security

To ensure only trusted individuals ever access customer systems or data, we apply rigorous personnel security and access controls across every engagement. To meet public-sector security expectations without slowing delivery, this includes:

- Formal screening
- Government clearance capability
- Tightly controlled technical access

All consultants complete Baseline Personnel Security Standard checks before being assigned to client work. Where roles involve sensitive or restricted environments, we can also provide staff vetted to BS7858 standards. For government environments, we maintain a pool of consultants who already hold Security Check clearance, with the ability to transfer clearance where required. Where a role demands it, we can sponsor additional Security Check or higher-level clearance, including Developed Vetting, subject to customer approval and government processes.

Access to systems follows a strict least-privilege model aligned with customer governance. Consultants receive only the permissions needed to perform their role and all remote access uses customer-approved secure Virtual Private Network (VPN) or Virtual Desktop Infrastructure (VDI) solutions with multi-factor authentication. Providing full traceability, every action is logged within the customer's own platforms.

3.6.3 Secure development

EPS does not develop or operate proprietary SaaS applications as part of this service. The service operates within customer-owned SaaS platforms and approved integration layers.

Where configuration, automation, integration or extension development activities are delivered, EPS applies secure development and assurance practices aligned to recognised standards, including:

- Secure design and threat modelling prior to implementation
- Use of secure coding standards and vendor-supported development frameworks
- Peer review and controlled change governance
- Validation of changes within vendor-provided test or sandbox environments

Independent security assurance is supported through customer or vendor-provided penetration testing, platform security certifications and independent audits aligned to standards such as ISO/IEC 27034 and recognised cloud security frameworks.

3.6.4 Identity and authentication

EPS does not operate proprietary user authentication platforms. All user and administrative access is managed through customer-owned identity and access management frameworks and SaaS platform security controls.

To reduce the risk of credential compromise, access to customer SaaS environments is controlled using strong authentication mechanisms including:

- Multi-factor authentication (MFA)
- Single sign-on (SSO)
- Identity federation where supported by the underlying SaaS platforms

Privileged and administrative access is restricted to authorised EPS personnel on a least-privilege basis and is protected by MFA. All privileged access and configuration activities are logged, monitored and auditable in line with customer governance and information security policies.

EPS aligns delivery activities to customer identity management standards and does not introduce independent authentication systems or unmanaged access pathways into buyer environments.

3.7 Auditing

To provide buyers with clear visibility and control over activity within their SaaS environments, EPS supports comprehensive auditing and activity logging using customer-approved platforms and tools.

Audit logging is provided through customer-owned SaaS platforms and associated monitoring and SIEM tools. These logs capture user activity, EPS consultant activity and system-level events in line with customer governance and information security policies.

What do we log?

To support investigation, assurance and compliance, we record all significant actions. For full accountability of all delivery-related actions, this includes EPS consultant activity alongside user activity:

- **Authentication activity:** Logins, MFA challenges, failed attempts and session starts
- **Change and data activity:** Configuration updates, data changes and deployment actions
- **Privileged operations:** Administrative access, elevated commands and management actions

To avoid delays during reviews or incidents, buyers can access audit data directly within their existing platforms. Logs are available in real time through customer-approved tools such as ServiceNow, Azure Monitor or SIEM solutions.

To support governance and reporting needs, we also provide scheduled audit outputs in open formats including CSV, JSON and PDF for compliance reviews, investigations or assurance reporting.

Retention and compliance

To align with regulatory and organisational requirements, we retain audit logs in line with buyer-defined policies and UK GDPR obligations. Retention periods are configurable to match customer standards, including extended retention for regulated environments.

To support external audits or investigations, we enable secure export and transfer of audit logs using customer-approved mechanisms.

3.7.1 Performance monitoring and metrics

EPS provides continuous visibility of service delivery through structured monitoring and governance processes aligned to customer IT service management and programme governance frameworks.

Performance monitoring is delivered through customer-owned SaaS platform monitoring tools, ITSM systems and EPS service management reporting. These provide early visibility of service performance, risks and trends, enabling proactive management of live SaaS environments.

Accountable delivery roles

Typical accountable roles supporting performance monitoring include:

- **Service Delivery Lead (Accountable)**: Owns overall service performance, reporting cadence, governance forums and escalation routes
- **Technical / Solution Lead (Responsible)**: Oversees technical quality, configuration and change assurance and supports incident and problem investigation
- **Information Security and Compliance Lead (Assurance)**: Oversees security controls, access reviews, audit actions and security incident handling
- **Operations / Transition Lead (where applicable)**: Oversees onboarding, service transition, operational readiness and handover controls
- **Reporting and Governance Coordinator (where applicable)**: Maintains RAID logs, action tracking, reporting packs and governance cadence

Monitored metrics

To enable informed decision-making and maintain governance compliance, we provide actionable, public-sector-aligned performance metrics. Performance monitoring typically includes:

Service stability	Availability, incident volumes and trends, service response performance
Delivery progress	Optimisation and change milestones, adherence to agreed delivery plans
Cost performance	FinOps and GreenOps savings; forecast accuracy

Security posture	Patch compliance; vulnerability remediation status
Capability transfer	Training completion; adoption of delivered processes and controls

Governance and reporting cadence

Governance channels typically include:

- **Operational service reviews (weekly/fortnightly)**: Performance, incidents, changes, risks and actions
- **Monthly service governance reviews**: Trend analysis, root cause review and improvement planning
- **Ad hoc escalation:** Immediate escalation routes for high-impact or service-critical events

3.7.2 Compliance and quality management

To meet all expectations for quality, security and continual improvement, we deliver our services under a governed, integrated management system, aligned to recognised best-practice standards:

Evidencing our strong technical and procedural security measures, we hold **Cyber Essentials Plus certification.** Ensuring structured service delivery and continual improvement, we also apply ITIL v4 principles across all service processes.

Governance and assurance

To maintain accountability and transparency, Mailyn Sheikh, Compliance Director, will lead the following governance activities:

- Review formal policies and operating procedures annually or more often in line with changes to legislation or best practice. These are them formally approved by senior management
- Monthly performance reviews using service metrics and KPIs
- Analysis of customer feedback to identify opportunities for improvement
- Internal audits and corrective action tracking to maintain compliance and quality

To ensure lessons are applied, findings from audits and reviews feed directly into EPS's improvement roadmap. This drives refinements to processes, tools and delivery practices.

3.8 Backup, restore & disaster recovery

EPS does not host or control customer production data or SaaS platforms. All customer production data remains within buyer-owned SaaS environments and approved hosting arrangements. Backup, restore and

disaster-recovery operations for live systems are therefore provided and managed by the buyer and/or their SaaS platform providers.

Customer production data is typically stored within UK-based data centres or UK cloud regions, in line with public sector data residency requirements.

Backup and data protection

Backup frequency, retention policies and storage locations for live customer data are governed by the buyer's SaaS platform and hosting providers. EPS does not perform or control backups of customer production data.

EPS supports customers by:

- Aligning delivery activities to customer backup and data-protection policies
- Providing assurance input into data migration, reconciliation and validation activities
- Ensuring operational handover documentation reflects customer continuity and backup arrangements

Any incidental working files held on EPS-managed devices during delivery are encrypted and securely deleted following service closure.

Recovery objectives and resilience planning

Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) for live SaaS platforms and data are defined and managed by the buyer and/or their SaaS providers. EPS does not control recovery operations for live environments. EPS supports customers by:

- Defining and aligning RPO and RTO targets during SaaS transformation and optimisation programmes
- Integrating continuity and resilience planning into service transition and operational handover models
- Supporting resilience and recovery planning where required

EPS business continuity measures

EPS maintains its own internal business continuity and disaster recovery arrangements to protect service delivery continuity. These include:

- Remote-first delivery capability across geographically distributed delivery teams
- Backup access to secure collaboration and delivery platforms
- Crisis escalation routes and continuity planning for active engagements
- Resource flexibility across programmes to maintain delivery during incidents
- Alignment with customer crisis response and incident management frameworks for critical public sector environments

Where EPS is embedded within critical government programmes, continuity procedures are aligned directly to the buyer's incident and crisis management frameworks.

Continuous improvement and assurance

Service-impacting incidents and continuity exercises are reviewed through formal governance forums. To continually strengthen service resilience and continuity controls, lessons learned are captured, corrective actions are defined and tracked to completion.

3.9 Training

To ensure technology changes are adopted effectively, we embed training and knowledge transfer into every engagement. Grouped into 3 core streams as follows, our programmes are tailored entirely to customer systems, workflows and user groups:

End-User Training	Technical and Administrator Training	Business Readiness and Adoption Workshops
		
What is it? Instructor-led sessions (on-site or remote), live online walkthroughs and role-based instruction focused on business processes and daily tasks **What are the benefits and impacts?** ✓ Accelerates adoption ✓ Reduces errors ✓ Minimises support demand ✓ Users gain confidence and competence in day-to-day system use	**What is it?** On-site or remote instructor-led sessions for admins and super-users, plus train-the-trainer programmes to build in-house capability **What are the benefits and impacts?** ✓ Strengthens internal expertise ✓ Reduces dependency on external support ✓ Strengthens governance ✓ Technical teams and administrators can manage and configure systems independently	**What is it?** Workshops addressing process changes, communication strategies and confidence-building for operational staff **What are the benefits and impacts?** ✓ Minimises transition risk ✓ Increases user engagement ✓ Operational teams can implement new workflows and processes smoothly

Supporting learning artefacts

To reinforce knowledge and ensure ongoing reference, we provide a suite of customer-specific artefacts:

- Quick-reference handbooks which include step-by-step guidance
- Process maps and workflow documentation for a visual representation of procedures
- Video walkthroughs and recorded demos
- Knowledge-base articles and FAQs for reference

Learning journey

Discovery → Role assessment → Tailored training → Artefact handover → Adoption monitoring → Continuous improvement

Discovery and role assessment: Identify knowledge gaps and target training to the right user groups
Tailored training delivery: Delivery role-specific sessions and workshops
Artefact handover: Provide reference materials for ongoing use
Adoption monitoring: Track participation, completion and competency
Continuous improvement: Capture lessons learned and feedback to refine future engagements

Measurement

To deliver tangible results, we co-develop training plans with customer stakeholders and measure effectiveness through:

- Participant feedback surveys
- Completion records for instructor-led sessions and e-learning modules
- Post-training assessments to validate knowledge retention

Keeping training aligned with operational needs and project objectives, EPS uses these insights to continuously refine programmes.

3.10 Service pricing

Our SaaS Enablement, Transformation and Optimisation Service can be procured through the G-Cloud 15 Framework using transparent and flexible pricing models aligned to public sector procurement practices.

Pricing models

EPS offers the following pricing models:

- **Outcome-based milestone pricing**: Linked to clearly defined deliverables, milestones and acceptance criteria
- **Time and Materials (T&M)**: Based on SFIA-aligned day rates for named delivery roles
- **Fixed price**: Considered on a case-by-case basis where scope, dependencies and outcomes are sufficiently defined

EPS does not provide subscription or licence-based pricing, as the service does not include a proprietary SaaS product.

Rates and charging structure

Day rates are aligned to the published SFIA rate card and vary depending on role seniority, specialist skills and clearance requirements. We do not charge monthly licence fees.

EPS does not sell pre-packaged service tiers. Engagements are structured around defined delivery phases and milestones, which can typically be grouped as:

- **Discovery and assessment:** Current-state analysis, gap assessment and roadmap development
- **Design and configuration support:** Process design, data modelling and configuration support
- **Implementation and change support:** Business analysis, UAT coordination, change management and training
- **Hypercare and optimisation:** Post-go-live support, performance monitoring and optimisation

Each phase is priced based on agreed scope, outcomes and resource requirements.

Additional services and charges

Additional services may be charged where they fall outside the agreed Statement of Work, including:

- Bespoke or extended training programmes
- Large-scale organisational change rollouts
- Additional data migration or reconciliation support
- Out-of-hours or enhanced support coverage
- Specialist assurance or audit activities

All additional charges are governed by the published rate card or milestone agreements and managed through formal change control.

3.11 Invoicing process

We use a transparent invoicing process aligned with UK government procurement standards:

- **Billing cycle:** Invoices are issued monthly in arrears or on completion of agreed milestones, depending on the pricing model selected (T&M or Outcome-Based)
- **Payment terms:** Standard 30-day payment terms apply, in line with government requirements
- **Accepted payment methods:** EPS accepts BACS transfers and purchase orders (PO) raised through the customer's finance system
- **Minimum contract or billing period:** There is no minimum contract term; engagements can scale up or down based on customer needs
- **Self-billing portals:** EPS does not operate self-billing portals, but can work with customer systems where required

3.12 Termination terms

Termination is governed by the Crown Commercial Service G-Cloud 15 Call-Off Terms and Conditions. Buyers may terminate the contract in accordance with these terms by providing written notice.

EPS Termination Policy

- **Minimum contract term:** None, engagements are flexible and can scale up or down based on buyer needs
- **Notice period:** Standard notice is 30 days (4 weeks) unless otherwise agreed in the Call-Off Contract
- **Early termination:**
    - No penalties or termination fees apply
    - Charges apply only for work completed or in progress up to the termination date
    - Any planned future work or milestones not yet started will be cancelled without charge
    - Where resources have already been engaged on a milestone or work package, costs will be calculated pro-rata based on the applicable SFIA rate card and proportion of work delivered

Data handling on termination

Ensuring all customer data remains within customer-controlled environments, upon termination, EPS follows the offboarding and data-deletion process described in *Section 3.2.2 Offboarding*. This confirms secure deletion of any temporary working materials.

4 Security and data governance

4.1 Data protection and encryption

EPS does not operate proprietary hosting or network infrastructure. All customer production data remains within buyer-owned SaaS platforms and approved hosting environments.

All communications between EPS delivery resources and customer SaaS environments are protected using TLS 1.2 or higher encryption to ensure confidentiality and integrity. API-based integrations, configuration activities and reporting access are delivered through secure, encrypted channels governed by customer identity and access management frameworks.

Where additional network-layer protection is required, EPS supports the use of VPN or IPsec connections in line with customer network security policies.

Data at rest is protected by the underlying SaaS platform providers using industry-standard encryption controls, typically AES-256 or equivalent, alongside role-based access controls and logical data separation.

Key management, firewalling, network segmentation, intrusion detection and monitoring are provided by the customer's SaaS platforms and hosting providers. EPS aligns delivery activities to these controls and does not introduce independent encryption or key management services into buyer environments.

To maintain future-ready security assurance, EPS aligns with evolving post-quantum cryptography guidance.

Additional controls

- We do not keep customer information on local EPS devices or removable media
- Activity logs and audit trails are maintained entirely within client systems
- We operate under Cyber Essentials and ISO 27001-aligned practices for every engagement

4.2 Data at rest, storage locations, and physical security

To give buyers full control and ownership of their data, EPS does not host or store customer production data or operate proprietary datacentres. All customer production data remains within buyer-owned SaaS platforms and approved hosting environments. Buyers determine where data is stored and processed, such as UK-only or UK/EU regions and maintain their own retention and backup policies.

To reduce the risk of data exposure, we operate strictly within the buyer's platform security controls. Encryption at rest is managed by the client's platform and we do not move or replicate data outside the environment.

To maintain compliance and transparency, data is stored in the locations selected by the buyer. We do not operate data centres or sub-processors for hosting. The customer's hosting provider manages compliance with standards such as ISO 27001, CSA CCM or SOC 2.

To ensure data is physically protected, customers rely on their chosen cloud provider or on-premises facilities. Physical controls typically include 24/7 manned security, biometric access, CCTV and perimeter protection. We do not manage these facilities, but ensure all our activities align with client governance and security requirements.

To prevent residual data risk, we securely clean down all temporary working materials. We delete documentation drafts, anonymised extracts and other materials held in collaboration tools within 30 days of project closure, with written confirmation provided on request.

Where EPS consultants work remotely, we maintain physical and endpoint data protection through a layered security model covering secure access, endpoint controls and working practices:

- Access to customer SaaS platforms is only permitted through customer-approved secure connectivity, such as VPN, zero-trust gateways or bastion/jump services
- Customer environments are not exposed to unmanaged or personal devices
- Access is role-based, time-bound and fully logged within customer audit frameworks
- Where required, customers mandate the use of controlled virtual desktops or secure jump environments, ensuring that customer data remains within the customer estate at all times.

4.3 Data sanitisation and disposal

EPS does not host customer production data or operate proprietary storage platforms. All customer production data remains within buyer-owned SaaS platforms and approved hosting environments.

Any incidental customer data held on EPS-managed devices during service delivery is protected and securely disposed of in line with recognised public sector and NCSC-aligned data sanitisation practices.

Secure disposal controls include:

- Use of operating-system and platform-native secure deletion and cryptographic erasure methods designed to prevent data recovery
- Secure wiping of endpoint devices and removable media before reuse or disposal
- Verification of deletion before device redeployment or disposal
- Written confirmation of deletion provided on request to support audit and compliance requirements

EPS does not manage or dispose of customer-owned hardware or storage media. Where EPS-owned devices reach end of life, they are disposed of through reputable IT asset recycling and disposal providers that demonstrate appropriate security and environmental handling practices. Evidence of destruction or recycling is retained where available and can be provided on request.

4.4 Security testing and assurance

To ensure clients maintain control and visibility over system security, we do not conduct independent penetration testing on customer systems. Penetration testing remains the responsibility of the buyer or their appointed third-party provider. We support these activities by supplying configuration details, enabling authorised access and assisting with remediation when required. Where EPS systems, such as collaboration tools, fall within scope, we conduct testing in accordance with our policies using CHECK- or CREST-certified testers.

To minimise risk and maintain system integrity, we do not introduce proprietary software. Vulnerability scanning and patching remain fully under the buyer’s control. We ensure that all configuration or migration activities comply with the client’s vulnerability management processes and remediation timelines.

To provide ongoing assurance and governance, we operate under Cyber Essentials and ISO 27001-aligned practices. Security responsibilities and audit outcomes are regularly reviewed as part of engagement governance and evidence of compliance can be provided on request.

4.5 Incident and protective monitoring management

To ensure security incidents are detected quickly and handled consistently, we work directly within the buyer's existing monitoring and response capability. All environments are covered by customer-owned 24/7 SIEM or SOC monitoring. This gives continuous visibility of security events without introducing parallel tooling or new risk.

To enable fast, controlled response when issues occur, we integrate into the buyer's incident-response process from day 1. Incidents are:

- Classified by severity and business impact
- Escalated through agreed channels
- Managed within defined notification and resolution timelines

Ensuring full auditability, we use customer-approved ITSM tools to log, track and report incidents.

To support structured, repeatable incident handling, we align our approach with ISO 27035 incident-response principles. To reduce the likelihood of recurrence, we contribute technical analysis, support investigation/remediation and participate in post-incident reviews. All incident records and monitoring data remain within the buyer's environment at all times.

4.6 Configuration and change management

To support controlled, auditable updates within live SaaS environments, EPS operates formal configuration and change management controls aligned to ITIL v4 and ISO 27001. Ensuring changes are predictable, traceable and reversible, we work entirely within the buyer's environments and follow their established approval and assurance processes.

To assess and approve changes properly, our consultants follow an ITIL-aligned change-management process. Every change includes:

1. **Change initiation:** Managed through an ITIL-aligned change-management process
2. **Impact assessment:** Includes an assessment of technical, operational and security impacts
3. **Approval:** Routed through customer approval workflows prior to implementation
4. **Deployment:** Approved changes are deployed within agreed release windows
5. **Post-implementation review:** Reviews are conducted to confirm outcomes and capture lessons learned

To maintain full visibility and traceability, we manage all changes using customer-approved tools such as ServiceNow, Jira or Azure DevOps. Providing a clear record from deployment through to retirement, configuration items are recorded and version-controlled in the customer's Configuration Management Database. This enables rapid rollback where required and helps identify dependencies to prevent unintended knock-on effects.

To prevent security issues being introduced through change, we assess the security impact of all updates before release. To embed security and compliance in day-to-day delivery, we review changes against customer security policies and compliance frameworks.

4.7 Information security management and certifications

EPS operates a proportionate information security management framework designed to support secure delivery within customer-owned, security-assured SaaS environments.

EPS currently holds Cyber Essentials certification, providing independent validation of baseline technical security controls. This includes protection against common cyber threats such as malware, insecure configuration and unauthorised access.

EPS does not currently hold ISO 27001, ISO 20000-1 or ISO 9001 certification. However, internal policies, delivery controls and working practices are designed to align with recognised public-sector security good practice and to operate effectively within customer governance, audit and assurance frameworks.

Security accountability

EPS operates a role-based accountability model. Information security and data protection accountability sits with senior management, supported by an Information Security Lead function responsible for:

- Maintaining security and acceptable-use policies
- Maintaining alignment to Cyber Essentials controls
- Coordinating security incident response and escalation
- Supporting customer assurance and audit activity
- Maintaining security records and evidence

Clear escalation routes exist to senior management for any material security risk or incident.

Audit trail and evidence model

EPS maintains controlled records of security-relevant activity, including:

- Current Cyber Essentials certification and supporting evidence
- Controlled versions of security and acceptable-use policies
- Access approval and onboarding records
- Governance action logs
- Incident and near-miss records
- Risk and issue registers
- Clean-down confirmations where applicable

Records are held in controlled document management systems with access restrictions and version control.

Review and assurance cadence

EPS operates a structured internal security review cycle, including:

- Annual review aligned to Cyber Essentials renewal
- Management review of risks, incidents and improvements
- Event-driven reviews following incidents or material change
- Engagement-level assurance aligned to customer audit and accreditation requirements

EPS supports customer-led audits, assurance and compliance reviews relevant to the services delivered.

Third-party assurance alignment

EPS delivers services within customer SaaS environments that are typically subject to formal external assurance regimes such as ISO 27001, SOC 2 and government accreditation frameworks. EPS aligns delivery practices to these standards and operates in line with customer audit, security and reporting obligations.

4.8 Secure development and cryptography

Although EPS does not develop or operate commercial SaaS products, our consultants regularly develop automation scripts, configuration artefacts, integration components and deployment tooling. These are done to support service delivery within customer-owned SaaS environments and controlled test facilities.

All development activity is performed within customer-owned environments and governed by customer security, assurance and change frameworks. EPS applies secure development and cryptographic controls proportionate to risk and aligned to public-sector and NCSC-aligned security expectations.

Secure SDLC practices

Where EPS undertakes scripting, automation or configuration development, the following secure development practices are applied:

- Secure design and pre-implementation review aligned to customer security architecture
- Use of controlled, auditable repositories within customer environments
- Peer code review and technical assurance prior to deployment
- Static analysis and dependency scanning where supported by customer tooling
- Separation of development, test and live environments
- Secure configuration baselines and hardening standards
- No hard-coded secrets or credentials
- Formal change control, testing, approval and rollback procedures
- Logging and auditability of automation activity

These practices integrate with customer DevSecOps pipelines, service management processes and accreditation frameworks.

OWASP Top 10 alignment

EPS aligns all development activity to the OWASP Top 10 risk categories. Where scripting or API-integrated components are delivered, OWASP risks are assessed and controlled during design, code review and assurance stages, including:

- Injection and input validation risks
- Broken authentication and access control
- Security misconfiguration
- Vulnerable and outdated components
- Sensitive data exposure
- Logging, monitoring and error-handling weaknesses

Cryptographic controls

EPS does not define cryptographic standards independently. All cryptographic controls are implemented in accordance with customer security policy and NCSC-aligned guidance. Where not explicitly mandated by the customer, EPS defaults to recognised good practice aligned to NCSC guidance.

Data in transit:

- TLS 1.2 minimum (TLS 1.3 preferred)
- Customer-approved cipher suites
- Certificate-based authentication, where supported

Data at rest

- AES-256 encryption or customer-mandated equivalent

- Use of platform-native encryption for storage, databases and backups
- Encryption of snapshots, backups and artefacts containing sensitive data

EPS automation and scripts do not store sensitive data in unencrypted form.

Key management

EPS does not own or manage cryptographic keys. All key management is performed using customer-approved key management services, such as HSMs, cloud KMS platforms and enterprise secrets management solutions.

EPS adheres to customer policies governing key generation, access control, rotation, expiry and revocation. EPS does not store passwords or keys in code or documents. Access credentials are pulled securely from the customer's approved systems at runtime and are not visible to users or written into logs.

Post-quantum cryptography alignment

EPS aligns to NCSC guidance on post-quantum cryptography and supports customer-led preparation and adoption. In practice, EPS:

- Monitors NCSC cryptographic transition guidance
- Designs services to support cryptographic agility
- Avoids deprecated cryptographic primitives
- Supports customer-led migration planning and implementation when post-quantum controls are mandated

All cryptographic changes are implemented under customer security authority, assurance and accreditation frameworks.

4.9 Identity and access management

EPS does not operate proprietary identity platforms or host customer SaaS environments. All identity and access management is governed by customer-owned identity platforms and approved access control frameworks.

EPS requires multi-factor authentication (MFA) for all privileged and administrative access. Where EPS consultants access customer systems, authentication and access controls are managed through customer identity platforms and enforced in line with customer security policies.

Supported authentication methods are determined by the customer environment and typically include:

- App-based authenticators
- Hardware-backed or platform authenticators, including FIDO2, where mandated
- Conditional access and device trust controls

Access is role-based and granted on the principle of least privilege. Administrative access is formally approved, time-bound where supported, and fully logged within customer audit frameworks.

EPS does not weaken or bypass customer MFA controls. All access activity is auditable and governed in line with public sector security requirements.

5 Supplier information

5.1 About us

EPS is a specialist technology consultancy born out of Empiric Solutions. We have over 20 years of experience delivering professional services to some of the most high-profile government and public sector organisations in the UK and Europe, including:

We bridge the gap between large, inflexible managed service providers and smaller specialist suppliers. In many programmes, customers usually choose between scale and flexibility, whereas EPS removes that trade-off. We provide the assurance and structure associated with major providers, while remaining agile enough to mobilise quickly, adapt to change and tailor delivery to what the programme actually needs.

Founded to support agile, cost-effective delivery across digital transformations, we operate from a global network of 6 offices located in:

- London
- Glasgow
- New York
- Tampa
- Cologne
- Amsterdam

Core specialisms and technology expertise

Our core specialisms include:

- **SaaS enablement, transformation and optimisation:** EPS delivers platform-agnostic SaaS enablement and transformation services across regulated public sector environments. We support organisations through the full SaaS lifecycle from early readiness assessment and design through to stabilisation, optimisation and operational handover. Our capabilities include:
    - SaaS readiness assessment and roadmap development
    - Business process redesign and automation within SaaS platforms
    - Data migration, validation and reconciliation
    - Post-go-live hypercare and service stabilisation
    - Performance optimisation and adoption enablement
    - Service transition into business-as-usual operations

All services are delivered within customer-owned SaaS platforms and aligned to customer security, governance and assurance frameworks.

- **Security, governance and operational assurance:** EPS specialises in delivering transformation activity within sensitive and regulated public sector environments. We embed security-by-design, governance and assurance into all engagements, including:
    - Alignment with customer security, accreditation and audit frameworks
    - Information security and access-control integration
    - Service governance, reporting and KPI frameworks
    - Risk, issue and dependency management
    - Incident, change and service management integration

This ensures that transformation strengthens operational resilience rather than disrupting live services.

- **Enterprise and digital transformation:** EPS supports end-to-end enterprise transformation programmes, combining strategic advisory with hands-on delivery capability. Our services include:
    - Operating model and service design
    - Programme and delivery management
    - SaaS platform optimisation and integration
    - Automation and DevSecOps enablement
    - Transition to service and early-life support

5.2 Relevant experience and testimonials

EPS has a proven track record of delivering complex SaaS enablement, transformation and operational stabilisation programmes across regulated public sector environments. Our experience spans enterprise business systems, mission-critical platforms and live operational services, supporting organisations to migrate, stabilise, optimise and embed new ways of working.

The following case studies illustrate how EPS has delivered measurable operational, governance and service performance improvements aligned to the outcomes sought by G-Cloud Lot 2b buyers.

Case study 1 - Enterprise SaaS transformation and operational stabilisation

Project: Large-scale enterprise business system transformation and optimisation (UK public sector)

Scope: EPS led a multi-year enterprise transformation programme for a major public-sector property and asset management organisation. We modernised and stabilised its core Horizon business system covering billing, asset management, procurement and supplier management. EPS delivered phased SaaS-style transformation governance, data migration, workflow automation, post-go-live stabilisation and operational handover.

Outcomes: Evidencing our capability in SaaS transformation delivery, hypercare, optimisation, governance and operational transition, key Lot 2b-aligned outcomes included:

- Migration and reconciliation of over 2 million financial and service-charge data records valued at over £100m
- Automation of manual business processes and billing workflows
- Post-go-live stabilisation and performance optimisation
- Structured governance, RAID management and board-level reporting
- Significant operational efficiency improvements and financial savings

Case study 2- Data migration, service transition and knowledge transfer

Project: Home Office – mission-critical service continuity and knowledge transfer

Scope: EPS delivered a structured data centre migration, stabilisation and operational knowledge-transfer programme for the Home Office Police Service Bus (PSB). The programme addressed risks associated with legacy platforms, knowledge loss and single points of failure, establishing formal service transition, training, governance and resilience frameworks.

Outcomes: Demonstrating our capability in service transition, operational handover, training, governance and risk management, key Lot 2b-aligned outcomes included:

- Formal service transition and operational readiness frameworks
- Structured knowledge transfer academies and training
- Centralised documentation, configuration guides and runbooks
- Reduction of operational risk and improved service continuity
- Improved throughput and resilience across live services

Case study 3 - Hypercare, training, stabilisation and live service optimisation

Project: Home Office – post-go-live stabilisation, training and live service optimisation

Scope: EPS delivered security-cleared hypercare, training and optimisation services for the Police National Computer Live Service. We stabilised live environments, improved fault handling, embedded new procedures and delivered structured training and adoption programmes.

Outcomes: Evidencing our capability in hypercare, adoption enablement, operational optimisation and live service governance, key Lot 2b-aligned outcomes included:

- Post-go-live hypercare and fault-resolution optimisation
- Business readiness and training enablement
- Improved operational procedures and service continuity
- Live-service support and early-life stabilisation

5.3 How to buy

EPS's services are available for purchase via the Crown Commercial Service (CCS) G-Cloud 15 Digital Marketplace. Customers can locate our listings on the Marketplace and select the service they require.

After a service has been chosen, the following process is followed:

1. The buyer and EPS agree a SOW that outlines the project scope, deliverables, timeline and pricing
2. A Call-Off Contract is raised under the G-Cloud 15 framework terms
3. A Purchase Order (PO) is issued to formally initiate the engagement

All procurements are carried out in accordance with public-sector procurement rules and the conditions of the G-Cloud 15 framework, ensuring transparency and compliance.

For enquiries or discussions prior to contract award, please contact our central team:

- **Email:** Jack.Richardson@e-ps.com
- **Phone:** +44 (0) 203 675 7773