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

CLOUD ENABLEMENT, MIGRATION AND SUPPORT SERVICES

SERVICE DEFINITION

JANUARY 2026

Table of contents

1 Introduction

1.1 Document structure

This Service Definition sets out the details of Cloud Enablement, Migration and Support Services delivered by Empiric Professional Services (EPS) under the G-Cloud 15 Framework. It is designed to give public sector buyers clear, practical insight into what our service does, how it is delivered and the assurance measures that underpin it.

Our aim is to help organisations move to the cloud confidently and operate securely, while maintaining cost control and flexibility across platforms. This document explains the functionality, security, governance and support options available and outlines how to engage with us through G-Cloud.

To make navigation simple and procurement decisions easier, the Service Definition is organised into 3 sections:

Service overview	Delivery and assurance	Credentials and procurement
Covers: • Functionality • Key advantages • Compliance measures	**Covers:** • Operational approach • Security and governance standards • Support options	**Covers:** • Our experience and credentials • How to procure via G-Cloud 15

Each section is structured to help buyers quickly find the information most relevant to their stage in the procurement process. This includes assessing technical fit, understanding delivery assurance and confirming compliance and pricing.

1.2 How to use this document

This Service Definition is designed to guide public sector buyers through every stage of their G-Cloud procurement journey, from early evaluation to contract award and ongoing delivery management.

Where to start?

- **Exploring options:** If you're assessing whether our service meets your organisation's needs, start with *Section 2: Service description*. It explains our scope, approach and the benefits we deliver, helping you compare solutions with confidence
- **Preparing for contracting:** For due diligence and planning, *Section 3: G-Cloud alignment information* sets out how we work under G-Cloud, including onboarding steps, service levels, support models and exit arrangements
- **Assuring Security and compliance:** Public sector buyers need certainty on data protection and governance. *Section 4: Security and data governance* details our information security framework, compliance standards and business continuity measures
- **Confirming Supplier Credentials:** When you need background on who we are and how to engage, *Section 5: About EPS* provides company information, relevant experience and procurement routes through the G-Cloud framework

2 Service description

2.1 About our service

We help public sector organisations move to the cloud with confidence, delivering Cloud Enablement, Migration and Support Services through the G Cloud 15 Framework. Our goal is to ensure our customers operate securely, efficiently and cost-effectively every step of the way. With over 20 years of experience in complex technology transformation, we bring deep sector expertise and a proven track record across government, healthcare, education and regulated environments.

Our services are tailored for organisations looking to modernise their infrastructure, reduce operational risk and fully realise the benefits of hybrid and multi-cloud models – without being tied to a single vendor. From readiness assessments and migration planning to ongoing optimisation and governance, we handle the complexities so customers can focus on delivering their services with confidence. Our approach ensures operations stay fully secure and compliant with UK Government standards, including ISO 27001 and Cyber Essentials.

Alongside private and hybrid solutions, our consultants bring hands-on experience with all major cloud platforms, including but not limited to:

This vendor-agnostic approach ensures impartial advice and optimised outcomes, enabling customers to get the most from their chosen platforms while avoiding lock-in. Ensuring cloud adoption aligns with business processes and user needs, we also support integration with enterprise systems such as:

- ✓ Enterprise Resource Planning (ERP)
- ✓ Customer Relationship Management (CRM)
- ✓ Human Resource Information System (HRIS)

2.2 What makes EPS different?

- **Vendor-agnostic approach**: Enabling flexibility and impartial advice, we work across all major cloud platforms
- **Outcome-focused delivery**: Every engagement is structured to reduce risk, accelerate timelines and improve long-term operating maturity
- **Public sector expertise**: Ensuring alignment with government priorities for security, sustainability and cost transparency, our consultants bring hands-on experience in regulated environments
- **Embedded knowledge transfer**: We strengthen internal capability through structured training and collaborative delivery, leaving organisations better equipped for future change

2.3 Delivery framework

With EPS, moving to the cloud doesn't have to be risky or overwhelming. We follow a structured, repeatable process that accelerates outcomes while ensuring governance and compliance at every step. From readiness assessments through to post-migration optimisation, we support the full journey so organisations can adopt the cloud securely, sustainably and with complete cost control.

Our 5-phase delivery model is as follows:

Discover

We start by understanding where you are today. Your goals, constraints, readiness and what success looks like. This helps us define a realistic scope and capture the right requirements from day 1.

Design

To align everything with government standards and your organisation's priorities, we shape the architecture, security controls and migration plan together.

Migrate

To minimise disruption and support a smooth transition, we take a risk-aware approach when it's time to move. This includes planning carefully, supporting cutover and staying close with hypercare.

Optimise

Once workloads are live, we work with you to improve performance, control costs through FinOps practices and identify opportunities for continuous improvement.

Embed

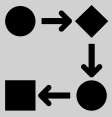
Finally, to build lasting capacity, we stay with you beyond go-live and make sure your teams have the skills, knowledge and governance structures to run confidently in the cloud.

2.4 Service features / benefits

Our service is designed to give organisations confidence in how they adopt, run and govern cloud environments. Below, we have highlighted what we deliver and the practical benefits our customers see as a result.

Cloud readiness assessments: Start by building a clear picture of your readiness before decisions are locked in, across people, technology and security

✓ **Reduces migration risk through structured cloud readiness and planning**



Migration planning and cutover support: Careful dependency mapping and hands-on cutover support to help protect critical services during transition

✓ **Improves service stability during critical cloud transitions and cutovers**

Cost management and governance: Apply practical FinOps and governance controls

✓ **Prevents cloud overspend and improves long-term cost control and accountability**

Collaborative delivery: Our teams work alongside yours, embedding governance and sharing knowledge throughout the engagement rather than at the end

✓ **Builds business confidence throughout complex technology change programmes**

Risk-aware migration execution: Migrations are sequenced based on risk, complexity and dependencies, allowing progress without unnecessary exposure

✓ **Accelerates migration timelines while maintaining control and reducing operational risk**

Security and compliance assurance: Security controls and governance are aligned with UK government principles and recognised standards from the outset

✓ **Strengthens security controls and simplifies ongoing compliance and assurance**

Performance monitoring and insight: Provide clear visibility across hybrid and multi-cloud environments through monitoring and analytics

✓ **Enables faster issue resolution and better-informed operational decisions**

Knowledge transfer and capability building: Structured handover and targeted training, so internal teams are equipped to operate cloud services confidently

✓ **Strengthens internal cloud capability**

Post-migration hypercare: Dedicated stabilisation support to address issues quickly once services go live

✓ **Reduces service outages during and after migration activities**

Continuous improvement: Continue to refine processes, tooling and governance as cloud usage evolves

✓ **Increases cloud operating maturity and ensures value is sustained over time**

What is hypercare?

Hypercare is an intensive post-go-live support phase that stabilises new services quickly before transitioning to standard operations.

2.5 Service scope

- **Service type:** Cloud Support (Cloud Enablement, Migration and Support Services)
- **Add-on or extension:** This is a standalone service designed to support cloud adoption and optimisation across public sector organisations
- **Cloud deployment model:** Public, Private and Hybrid
- **Multi-cloud support:** Yes, we provide vendor-agnostic support across AWS, Microsoft Azure and Google Cloud, as well as private and hybrid environments
- **Integration with enterprise systems:** Supports alignment with ERP (SAP, Oracle, Dynamics), CRM (Salesforce, Dynamics 365) and HRIS (Workday, SuccessFactors) to ensure continuity during migration
- **System requirements:** Requires timely access to customer systems, environments and stakeholders; work in regulated or secure environments is subject to appropriate security clearances and government-approved tooling

2.5.2 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, typically in UK-based public cloud regions aligned to public-sector data residency requirements.

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

We do not host customer production data or operate proprietary cloud platforms.

2.5.3 Service constraints

To provide secure and compliant services, we work within a small number of practical considerations. These reflect the realities of operating in public sector and regulated environments and we manage them openly with our customers from the outset.

- **Access and dependencies:** To keep delivery on track, we need timely access to systems, environments and key stakeholders. Where progress depends on third-party vendors, infrastructure readiness or client-side decision-making, we work collaboratively to manage these dependencies. This helps mitigate impacts on schedules and deliverables.
- **Secure and regulated environments:** Work in secure or regulated environments is delivered by appropriately cleared staff (up to developed vetting) and in line with UK Government security policies, networks and approved tooling. These controls are essential to protecting sensitive systems and information and may shape how and when activities are carried out
- **Delivery model**: We use a hybrid delivery model (remote by default, with on-site presence where security constraints, workshops or governance activities require it). On-site work is planned in line with local access procedures, health and safety requirements and site-specific governance
- **Operational hours:** We typically align delivery to UK business hours (09:00–17:30, Monday to Friday, excluding public holidays). To protect service continuity and minimise operational risk, we can agree out-of-hours support in advance for high-risk or time-critical activities, such as migrations or cutovers

2.5.4 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.

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 two 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.
User permissions	Standard user accounts are sufficient for most activities; administrative rights are only needed for optional local integrations.
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.

Additional notes

- Compatibility is aligned with the platforms you already support
- We impose no additional hardware or software requirements beyond your existing environment
- Any engagement-specific needs, such as API keys or licences for external systems, will be clearly defined in the Statement of Work

2.6 Reselling

EPS does not resell third-party cloud platforms or services. Our focus is purely on consultancy and technical enablement, delivering expertise directly within your own infrastructure and approved environments.

We do not provide licences, subscriptions or hosted components and we do not act as a reseller under the G-Cloud framework. This allows customers to retain full control over their technology stack and remain fully compliant with G-Cloud rules. All work is carried out using customer-owned platforms, cloud services and tooling.

Where integrations with third-party platforms are required (including AWS, Azure, or Google Cloud) we act as an independent delivery partner. We provide configuration, migration and operational support, working alongside customers' existing services without reselling or bundling them.

2.7 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 complex infrastructure and migration programmes, rather than an automated system. This approach gives our customers confidence that issues are resolved efficiently and correctly, while integrating smoothly with their existing service management processes.

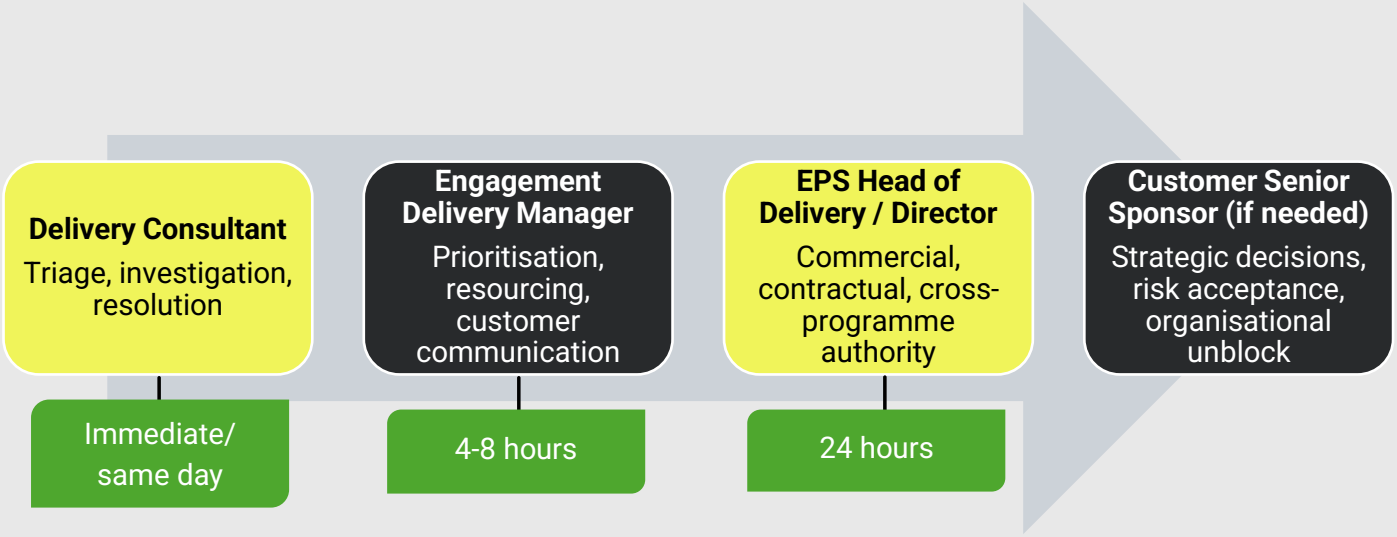
Support is accessible through channels customers already use, including email, scheduled calls and collaboration tools such as Microsoft Teams or Slack. Avoiding the need for a separate system, where formal ticketing is required, we work directly within customers' platforms (like ServiceNow, Jira or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

2.7.1 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 one 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.

2.7.2 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 also review accessibility feedback gathered during user-centred design workshops and hypercare phases, 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.

2.8 How users work with our service

2.8.1 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.

2.8.2 Desktop application

Our service does not require users to install any dedicated desktop application. We work within our customers' existing cloud 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

2.8.3 Mobile

To avoid forcing users to install or manage another app, we deliver the service entirely through customer-approved platforms and tools. Giving users flexible access wherever they are, these platforms are typically mobile-responsive and work seamlessly on iOS and Android devices.

To let users stay informed and productive on the move, we enable access to dashboards, reports and service updates through existing web interfaces and collaboration tools. For example, this includes ServiceNow, Jira and Microsoft Teams, with no additional configuration required.

Ensuring information remains easy to read and use on smaller screens, we optimise all documentation for mobile viewing, providing content in HTML and accessible PDF formats that work consistently across devices.

2.8.4 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.

2.8.5 API

To reduce risk and avoid introducing unnecessary dependencies, we do not provide a proprietary API as part of our consultancy 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.

To support practical integration needs without overcomplicating the environment, we use available APIs for setup, configuration, reporting and data management where required.

Making integrations easy to understand and maintain, we rely on vendor-provided API documentation and supplement it with clear HTML and PDF guidance for the specific integration activities we deliver.

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.

2.8.6 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.

2.8.7 Customisation

To give buyers flexibility without locking them into custom development, we avoid introducing a proprietary interface and work within customer-approved platforms and tooling. These platforms already offer rich configuration options, allowing organisations to tailor the service using standard, well-supported capabilities rather than bespoke builds.

Buyers can adapt the service to fit their operating model, including:

- Branding such as logos, colours and terminology
- User roles, permissions and workflow rules
- Notifications and approval routes
- Dashboards, reports and data fields

Most configuration can be carried out directly by buyer administrators using native platform tools. Where more complex changes or integrations are required, we provide expert support to ensure alignment with governance, security and platform best practice.

2.8.8 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

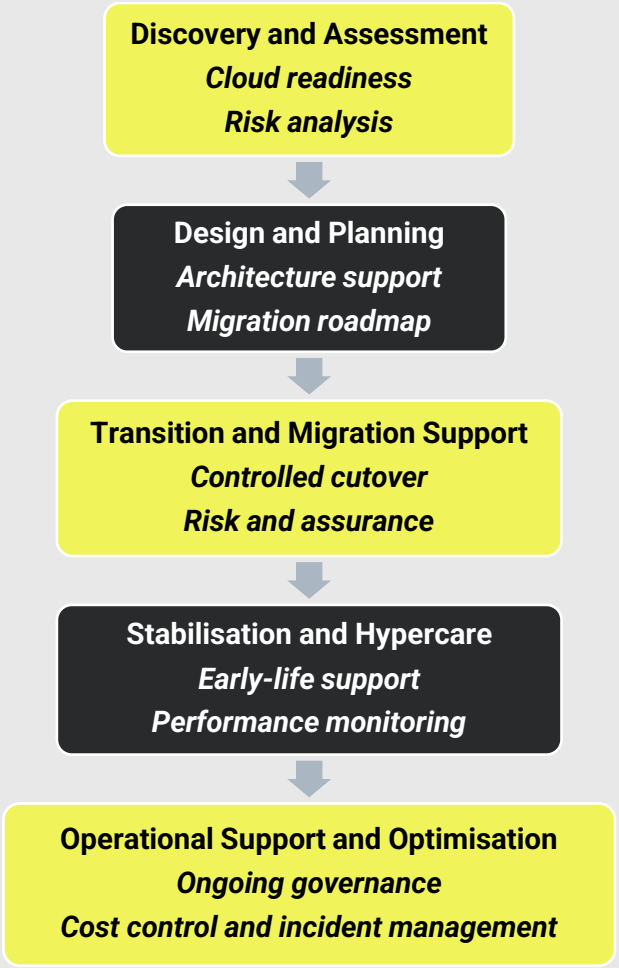
3.1 Section introduction

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

To support complex public-sector cloud 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. **Discovery and Assessment**

This phase focuses on understanding the customer's current environment, objectives and delivery context. We work with stakeholders to assess cloud readiness, organisational/technical constraints and key dependencies. Activities typically include service and stakeholder discovery, high-level review of existing platforms and processes and identification of security, assurance and compliance considerations.

Supporting informed decision-making, outputs from this phase inform scope, priorities and delivery approach. They typically include a cloud readiness assessment, initial risk and dependency log and recommendations.

2. **Design and Planning**

Building on discovery, this phase supports the development of target-state direction and a practical delivery plan. We provide architecture and design support to help buyers evaluate options, clarify assumptions and align proposed approaches to government standards and organisational needs.

We work collaboratively to define a phased migration roadmap, delivery plan and governance approach, including roles, responsibilities, reporting and assurance arrangements. This ensures delivery is structured, transparent and aligned to your internal controls and approval processes.

3. **Transition and Migration Support**

This phase supports the controlled transition of services into cloud environments. Our role focuses on coordination, assurance and service readiness rather than tooling or hosting provision. We help plan and manage transition activities, including cutover approach, risk mitigation, dependency coordination and engagement with technical and operational stakeholders.

Helping buyers reduce disruption and maintain service continuity throughout transition, we support go-live readiness through structured checkpoints, assurance inputs and clear escalation routes.

4. **Stabilisation and Hypercare**

Following transition, we provide early-life support to help stabilise services and embed new ways of working. This includes heightened service oversight, close monitoring of incidents and service performance and regular reporting to operational and delivery stakeholders.

Ensuring that operational teams are supported, during this phase we focus on rapid issue triage, trend analysis and knowledge capture.

5. **Operational Support and Optimisation**

Once services are stabilised, we provide ongoing operational support aligned to ITIL principles and buyer service management frameworks. This includes incident and service support, governance and assurance activities and regular service reporting.

We work with buyers to support continual improvement, cost and performance reviews, and evolving service needs. This ensures cloud services remain controlled, transparent and aligned to organisational objectives throughout the contract term.

3.2 Onboarding and offboarding processes

3.2.1 Onboarding

Ensuring there is a shared understanding of what the service will deliver and how we will work together, once the contract is signed, a named service contact is assigned, and onboarding begins immediately. The first step is a kick-off discussion to confirm objectives, success measures, delivery approach and key contacts.

We then provide an orientation pack and onboarding information, giving the buyer clear guidance on the service, ways of working, support routes and security expectations. This is followed by the setup of all required technical access, including user accounts, system/network access and any agreed tools or platforms.

Where the service involves working from buyer locations, site induction and workplace orientation are completed, including health and safety briefings and local operating procedures. If required, security identity checks are completed, and physical or logical passes are issued before any service activity begins.

On the agreed start date, a formal welcome and mobilisation session takes place. This includes stakeholder introductions, confirmation of priorities, and agreement on immediate next steps. The service then moves into active delivery, supported by early-life support to ensure everything is operating smoothly.

To establish governance and readiness for delivery, our step-by-step process includes:

1. Client business, mission and workplace orientation

We work with the customer to understand their business objectives, mission, operating environment, delivery constraints, and workplace culture. This ensures resources are aligned to outcomes from the outset.

Activities may include:

- Confirmation of scope and success measures
- Understanding operational priorities and delivery context
- Agreement of working practices and engagement model

2. Project overview and objectives (key outcomes)

A formal project kick-off is held to establish a shared understanding of:

- Project goals and key deliverables
- Roles and responsibilities
- Governance, reporting and escalation routes
- Milestones, dependencies and risks

3. Orientation pack and onboarding documentation

Providing clarity and consistency from day one, customers and users receive a structured onboarding pack which may include:

- Service overview and operating model
- Points of contact and support routes
- Security, compliance and acceptable use guidance
- Delivery processes and controls

4. IT equipment and system/network access

Where required, we support the setup of all technical and access prerequisites, including:

- User account creation
- Role-based access configuration
- Network and system connectivity
- Tooling and platform access

All access is provisioned in line with customer security policies and least-privilege principles.

5. Site orientation (if applicable)

Ensuring staff are compliant, safe and productive within the customer's environment, for on-site or hybrid delivery, we support:

- Site induction and health & safety briefings
- Facility access arrangements
- Local operating procedures and standards

6. Security pass and identity setup

Where required, we support buyer security processes, including:

- Identity verification
- Security pass issuance
- Compliance with physical and information security requirements

No service delivery begins until required clearances and access approvals are in place.

7. First day/welcome and service mobilisation

The first day of service includes a formal welcome and mobilisation session covering:

- Final confirmation of objectives and priorities
- Introductions to key stakeholders and delivery teams
- Review of ways of working and immediate next steps

8. Stakeholder introductions and integration

We facilitate introductions across relevant delivery, technical and business stakeholders to ensure:

- Clear ownership and communication routes
- Effective collaboration
- Rapid integration into existing teams and structures

9. Onboarding complete and transition to steady state

Once all onboarding activities are complete:

- The buyer confirms readiness
- The service transitions to steady-state delivery
- Ongoing support and service management processes are activated

3.2.2 Offboarding

To support a clean exit and continuity of service, our structed offboarding process will be jointly planned and agreed 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
    - 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 customer-approved cloud platforms and hybrid estates.

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 stays in the customer's environment throughout the engagement, which avoids vendor lock-in and keeps 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 environments rather than a shared hosting platform. 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 the customer's existing infrastructure and approved connectivity arrangements. 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 any configuration or migration activities do not compromise network integrity or data protection

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 during consultancy activities, we transmit information only through customer-approved channels. This protects sensitive information while keeping control firmly with the customer:

- 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: Ensures 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 and 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 regions, with them specifying:

- Location, for example, UK-only, UK/EU
- Retention
- Backup policies

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 use 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

To ensure availability remains under your control, we do not operate a hosted platform or network. All services are delivered within your infrastructure or chosen cloud environment. This means uptime and technical availability are governed by your own architecture, resilience controls and cloud or hosting service level agreements. We complement this by operating in ways that protect stability and prevent disruption.

Minimising the risk of unplanned service impact, all configuration, automation and migration activities are planned, risk-assessed, tested and delivered under your change control processes. Avoiding unnecessary change or new dependencies, we work within existing architectures and assurance boundaries.

To protect live operations, transitions and migrations follow phased approaches with rollback planning and service validation. Development, test and live environments remain clearly separated, with tightly controlled production access.

EPS guarantees 99.99% service availability during core service hours (09:00–17:30, Monday to Friday) for its migration, 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, cloud provider dashboards and formal escalation routes. Root cause analysis and corrective action planning are completed following any material incidents.

To reduce service risk further, activities affecting stability are subject to technical assurance and peer review. Reducing single-point-of-failure exposure, knowledge is protected through controlled documentation, structured handover and shared visibility.

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

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

Mailyn Sheikh, our Compliance Director, oversees governance of all management systems and reports to the board-level Quality and Security Committee.

3.6 Security

To protect the confidentiality and integrity of our service, we manage security under a comprehensive framework.

Giving customers confidence that their services and data remain secure at all times, we maintain strong leadership oversight of security activities. For effective leadership oversight, our Compliance Director manages all aspects of security and reports directly to senior management. Ensuring controls remain effective and aligned with regulatory and public-sector requirements, we hold governance boards regularly, perform scheduled audits and track security KPIs.

To reduce the risk of breaches and operational disruption, we enforce clear, practical security policies. These policies cover access control, encryption, incident response and system monitoring and every consultant follows them in every engagement. Embedding security into all service delivery, we comply with the UK Government Cloud Security Principles and the Software Security Code of Practice.

To ensure protections stay effective as threats evolve, we actively monitor systems and manage a live risk register. We perform regular penetration testing and vulnerability management, assign responsibilities to specific role and review controls on a structured cycle. This means we can address risks promptly before they can affect customers.

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 VPN or VDI solutions with multi-factor authentication. Providing full traceability, every action is logged within the customer’s own platforms.

3.6.3 Secure development

To reduce the risk of vulnerabilities being introduced during development or configuration, we design security into delivery from the outset. We follow a secure-by-design approach across the full lifecycle and align our practices with recognised public-sector assurance requirements.

To identify risks early and avoid rework later, we deliver all work through a structured Secure Software Development Lifecycle:

- Carry out threat modelling and risk assessment at the design stage

- Apply secure coding and configuration standards aligned with OWASP and NCSC guidance
- Use automated vulnerability scanning and code analysis

To prevent defects and misconfigurations from reaching live environments, we require peer review and configuration validation before any change progresses. Avoiding gaps between environments, we apply the same controls consistently across development, test and production.

To give buyers confidence that controls are working as intended, we support independent security assurance. We participate in penetration testing and vulnerability assessments and support secure development audits against recognised frameworks such as ISO 27034 and the CSA Cloud Controls Matrix. This allows us to effectively track findings through formal change control and remediate them in line with agreed priorities.

To maintain visibility and accountability, we document all security activities and integrate them into customer governance. We make outputs auditable within existing processes and provide regular reporting on security posture and remediation progress using customer-approved tooling.

3.6.4 Identity and authentication

To reduce the risk of credential compromise, we require multi-factor authentication (MFA) for all user access as a baseline. We support single sign-on and identity federation using customer-approved identity providers, allowing users to authenticate through existing platforms such as Azure AD or Okta. Our password policies are aligned with NCSC guidance, including complexity, expiry and lockout controls, where passwords are in scope.

To control high-risk actions and maintain accountability, we tightly manage privileged access. Administrative and management interfaces require elevated permissions and enforced MFA. We monitor and log privileged sessions in real time, integrating audit trails into customer governance and SIEM tooling. We also grant access strictly on a least-privilege basis and limit permissions to the scope and duration required for delivery.

To prevent persistent or inappropriate access, we enforce strong session controls. Sessions time out automatically and we require re-authentication for sensitive operations. Reducing the risk of accidental or malicious misuse, we use role-based access controls to separate duties.

3.7 Auditing

To give buyers clear visibility and control over activity in their environments, we provide comprehensive auditing and activity logging across all engagements. We log user actions, EPS consultant activity and system-level events using customer-approved tooling, with retention and access managed under client governance.

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, customer-approved cloud platform monitoring tools, ITSM systems and EPS service management reporting. Enabling proactive management of live cloud and hybrid infrastructure environments, these provide early visibility of service performance, risks and trends.

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

Metrics and reporting

To enable informed decision-making and maintain governance compliance, we provide actionable, public-sector-aligned performance metrics. The service and delivery team defines reporting scope and cadence with the customer and metrics typically include the following:

Service stability	Availability; incident trends; uptime performance
Delivery progress	Migration milestones; adherence to agreed plans
Cost performance	FinOps and GreenOps savings; forecast accuracy
Security posture	Patch compliance; vulnerability remediation status
Capability transfer	Training completion; adoption of delivered practices

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, our Compliance Director will lead the following governance activities:

- Review formal policies and operating procedures annually or more often in lien 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

To protect configuration integrity and ensure operational continuity during infrastructure software migration, we deliver a backup and disaster recovery approach tailored for hybrid and multi-cloud environments. This focuses on maintaining resilience during transformation activities and business-as-usual operations, without relying on hosted SaaS or clinical systems.

Overview

To safeguard critical public-sector services and comply with recognised standards, EPS operates under a Business Continuity and Disaster Recovery (BCDR) framework aligned with ISO 22301 and ISO 27001. The key points of this framework are as follows:

- Our Service and Technical Leads ensure recovery protocols are in place and coordinate activities during incidents
- EPS consultants work entirely within customer-owned environments. They follow customer governance, use approved tools and validate compliance throughout migration and operational phases
- Risk reviews conducted at key milestones and annual disaster recovery exercises as part of customer-led testing
- BCDR governance is fully integrated into EPS's delivery methodology

Backup strategy for hybrid and multi-cloud

Control	EPS approach
Configuration state protection	All migration tooling, scripts and configuration states are backed up within customer-approved repositories before any change
Cloud-native resilience validation	We verify replication and snapshot policies in AWS/Azure environments to meet agreed RPO/RTO targets
Incremental backups during cutover	Supports rollback capability and minimises risk during migration phases
Secure retention	All backups remain in customer-controlled environments; encryption enforced per customer policy

Disaster recovery integration

To restore essential services quickly and limit potential data loss, we integrate disaster recovery into migration planning and operational support:

- Recovery Time Objective (RTO): Typically under 24 hours for critical services
- Recovery Point Objective (RPO): Typically less than 1 business day

Continual improvement

To strengthen resilience for future engagements, we capture lessons learned from migrations and DR exercises and integrate them into the delivery framework. Guaranteeing a reliable service delivery, all activities align with public-sector governance frameworks and G-Cloud Call-Off Terms.

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

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

Technical and Administrator Training

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

Business Readiness and Adoption Workshops

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 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

Standards for consultancy day rate cards:

- **Consultant's working day:** 8 hours exclusive of travel and lunch
- **Working week:** Monday to Friday, excluding national holidays
- **Office hours:** 9:00am to 5:00pm Monday to Friday
- **Travel, mileage subsistence:** Included in day rate within M25. Payable at department's standard travel and subsistence rates outside M25
- **Mileage:** As for travel, mileage subsistence
- **Professional indemnity insurance:** Included in day rate

To align cost with outcomes and project needs, EPS offers 2 primary pricing models:

Outcome-based milestone pricing: Buyers only pay for results that are delivered and accepted, giving confidence that investment drives tangible outcomes. This approach works particularly well for structured migration projects, early-life hypercare and defined optimisation work packages, where clear deliverables and success criteria can be agreed upfront.

Time & Materials (T&M): Buyers retain flexibility to respond to changing priorities and emerging needs without being tied to fixed deliverables. EPS bills using SFIA-aligned day rates, providing access to advisory expertise, operational support and ongoing consultancy. This approach allows buyers to adjust scope, workload and timing as the engagement evolves.

Roles and expertise

To ensure buyers can assemble the right team for their requirements, EPS deploys a mix of skilled roles tailored to each engagement, including:

- Consultants
- Technical Consultants

- Delivery or Project Managers
- Senior or Lead Consultants
- Programme Managers

The full SFIA rate card, including day rates and bands, is included in the Pricing Document.

What's included?

For T&M engagements, buyers benefit from access to experienced consultants, structured governance/reporting and knowledge transfer throughout delivery.

For Outcome-based engagements, we deliver agreed outcomes against defined acceptance criteria, supported by governance and assurance activities and the combined expertise needed to achieve results. This clarity reduces the risk of scope creep and ensures maximum value for investment.

Additional charges

EPS does not charge for standard components such as data storage, software licensing, premium support packages or hosting, as we do not operate customer environments.

Charges may apply for optional extras, such as:

- Bespoke or extended training programmes
- Specialist workshops (for example, cloud architecture deep dives)
- Out-of-scope activities approved via change control
- Additional resources beyond the baseline team

Free trials

Free trials are not offered for consultancy-based Cloud Support services. While formal discounts for educational organisations are not standard, EPS can consider rate adjustments on a case-by-case basis depending on engagement scope and duration.

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

To protect sensitive information while it moves between systems, we encrypt all data exchanged during consultancy activities using TLS 1.2+ for web access and API calls. Our consultants connect through secure VPN or VDI, with multi-factor authentication and single sign-on, in line with customer security policies. Where additional protection is required, we implement IPsec tunnels or other client-approved measures.

To prevent exposure or loss of production data, we do not store it on EPS systems. Any temporary working files, including documentation drafts or anonymised extracts, are stored only in secure collaboration tools and deleted within 30 days of project closure, or sooner if requested. Encryption at rest and key management remain entirely under the client's control within their infrastructure.

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

44.2 Data at rest, storage locations and physical security

To give buyers full control and ownership of their data, we do not host or store production information. All data remains within the customer's infrastructure or chosen cloud environment throughout the engagement. 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.

Where EPS consultants work remotely, physical data protection is maintained through customer-controlled devices and secure access models. In most cases, consultants use customer-provided equipment, which ensures data remains within the customer's physical and logical estate.

Access to customer systems is permitted only via customer-approved secure connectivity such as VPNs, zero-trust gateways or bastion services. Unmanaged devices are not permitted, and access is role-based, time-bound and fully logged within customer platforms.

To process and store data entirely within customer-managed infrastructure, where required, customers mandate the use of controlled virtual desktops or secure jump environments.

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.

4.3 Data sanitisation and disposal

To protect client information and minimise risk, we do not host or store production data and all customer data remains within their own environment. We apply strict data minimisation and clean-down practices for any temporary working materials, such as documentation drafts or anonymised extracts, used during delivery.

To ensure temporary files cannot be recovered, we securely delete all materials from our collaboration tools within 30 days of project closure, or sooner if requested. Our sanitisation processes follow NCSC guidance and use secure methods to make data irrecoverable. Written confirmation of deletion is available on request.

To prevent any residual risk from devices, we do not manage customer hardware or storage media. When we use our own devices for delivery, these are securely disposed of according to ISO 27001-aligned processes.

To ensure end-of-life equipment is handled responsibly and securely, all devices are destroyed or recycled through accredited providers in line with recognised standards. Assuring you that no data can be recovered, certificates of destruction 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 according to 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 and 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 reduce operational risk and keep services stable during change, we control all configuration and change activity through a structured, auditable approach. 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, review changes against customer security policies and compliance frameworks, with higher-risk updates escalated to the Technical and Service Delivery Team and the client for formal approval.

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 cloud and hybrid estates.

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 to 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 restriction 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

Third-party assurance alignment

EPS delivers services within customer cloud and hybrid estates 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 regimes and operates in line with customer audit, security and reporting obligations.

4.8 Secure development and cryptography

Although we do not develop or operate commercial SaaS products, our consultants regularly develop automation scripts, configuration artefacts, integration components and deployment tooling. This supports service delivery within customer-approved cloud platforms and hybrid infrastructure environments, including 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.

Post-quantum cryptography alignment

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

- Monitor NCSC cryptographic transition guidance
- Design services to support cryptographic agility
- Avoid deprecated cryptographic primitives
- Support 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

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

Cloud enablement, migration and optimisation

Many organisations are under pressure to adopt cloud while managing legacy estates, constrained budgets and live operational risk. EPS supports cloud and hybrid programmes that need to move forward without destabilising existing services.

We deliver cloud enablement, migration and optimisation across AWS, Microsoft Azure and hybrid environments, covering early strategy and architecture through to migration, performance tuning and operational integration. Our teams establish secure landing zones, modernise applications and infrastructure and support-controlled migration into customer-owned environments.

With our consistent focus on cost transparency, operational readiness and supportability, we ensure cloud platforms can be sustained once delivery teams step back.

Security, governance and operational assurance

EPS operates in environments where security, assurance and audit requirements are non-negotiable and often evolving during delivery.

Strengthening operational assurance, we work directly with customer security, risk and service management teams to integrate delivery with existing accreditation, governance and control frameworks.

Our support covers secure-by-design delivery, risk and dependency management and integration with incident, change and service management processes.

Data, digital and enterprise transformation

Digital and enterprise transformation programmes frequently span multiple technologies, suppliers and operating models. EPS provides continuity across these moving parts.

We support customers from early strategy and service design through programme delivery, system and application modernisation, data platform enablement and transition into live operation. Our teams operate across cloud platforms, enterprise systems and data environments, aligning delivery to customer capability, governance and delivery maturity.

This approach allows change to be delivered incrementally while maintaining continuity of critical services.

Additional delivery capability

To support complex delivery environments, EPS also provides:

- DevSecOps and automation engineering
- Infrastructure-as-code and platform tooling
- Technical and architectural assurance
- Service transition and early-life support
- Supplier and multi-partner integration
- Knowledge transfer and capability uplift

Mission and values

We guide our clients through the change required to innovate and differentiate in the digital age, where customer centricity and environmental sustainability are paramount for a business to thrive. We help our clients to ignite and interlink their Business, Technology and Sustainability strategies to adapt their operating model and achieve excellence.

Through this, we help to create a seamless personalised customer experience. This not only serves the individual needs of the customer, but also gives confidence they're playing their part in our shared responsibility to protect the world we live in. Everything we do is grounded in 3 core values that define how we think, how we lead change and how we deliver outcomes.

5.3 Relevant experience and testimonials

Recognised for our expertise, we have provided a project example for illustration below:

Home Office

The Home Office is a ministerial department of the Government of the UK, responsible for immigration, security and law and order. Within the Policing and Public Protection portfolio (PPPT), the organisation was operating on legacy platforms and outdated technologies.

The requirement was for a supplier capable of providing end-to-end cloud and infrastructure services to transform and consolidate existing environments. The objective was to create an optimal hybrid technology solution that brought together cloud platforms, data centres, storage and virtualisation in a unified way.

Following a detailed analysis and review process, the Home Office determined that all systems should first be transitioned onto an interim staging platform. This would stabilise the existing environment and prepare the estate for a longer-term strategic migration to Amazon Web Services. Due to limited internal expertise, external support was required to deliver a legacy data centre migration and infrastructure upgrade to a high-performing virtualised environment, covering:

- VMware
- A Citrix upgrade
- Lift-and-shift of selected platforms
- A Cisco UCS upgrade

Overcoming challenges

Given the importance and criticality of the services involved, we provided a phased, controlled approach. EPS was selected to support the transitioning, design, execution, migration, training and ongoing support of the virtual environment. We worked with the Home Office to define the next stages of engagement and delivery and confirmed the activities required to support the transition.

Our consultants delivered design, transition and documentation for Virtualised Desktop Infrastructure environments and services. To support the transition of legacy services, they designed and deployed VMware infrastructure solutions and provided consultation on backup protection. To reduce operational risk, we defined comprehensive automation for VMware and developed a structured migration plan. We also provided clear direction on upgrade and patching paths across Cisco UCS, EMC, VMware, Microsoft and related products, aligning all changes with the overall transition plan.

Ensuring business needs were accurately reflected in delivery, we translated high-level requirements into technical rollout activities and provided third-line problem diagnosis expertise throughout the programme. We supported the Technical Coordinator (Technical Architect) and Senior Engineers in establishing best practices for processes and documentation. We also oversaw the development of migration test scripts and supporting documentation covering on-premises, virtualised, and hosted cloud migration paths. To support sustainability beyond delivery, we led knowledge transfer activities and helped maintain valid licensing and certification levels with relevant vendors.

To enable informed planning and controlled delivery, we reviewed existing processes and built a detailed understanding of demand and scaling requirements. This pre-transition assessment shaped delivery by identifying which areas should transition first, where issues were likely to arise and how they could be addressed during implementation.

Successes

Leveraging our second- and third-line technical support, we delivered **99.95% service availability** and resolved **97% of incidents within SLA**, while maintaining business-as-usual operations throughout the transition.

The programme stabilised the legacy estate on a controlled interim platform, resulting in a:

- ✓ **45% reduction in high-severity incidents**
- ✓ **50% reduction in unplanned outages**
- ✓ **Measured operational risk reduction of approximately 40–50%**

The Home Office achieved a fully virtualised staging environment, providing a secure and resilient foundation for its longer-term migration strategy.

5.4 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