



G-Cloud 15

Environment Management and Security Services

January 2026

Contents

Transforming Business using the Cloud.....	3
Environment Management & Security Services	5
Environment Management and Security Services Description	5
1. Cloud, hybrid and on-premise environment management	6
2. Release, deployment and configuration management strategy	6
3. Secure patching, upgrades and platform lifecycle management	6
4. Multi-phase release planning and controlled deployments.....	6
5. Change, configuration and asset management (CMDB).....	7
6. Cloud and SaaS security assurance and accreditation support	7
7. ITIL-aligned service management and operational governance.....	7
8. Infrastructure, platform and environment security management	7
9. Technical Design Authority and architecture assurance support	7
10. Agile delivery using PwC BXT methodology (Business, Experience, Technology)	7

Transforming Business using the Cloud

PwC works with Central and Local Government organisations to enable business and service transformation through the effective use of cloud technologies. Cloud adoption is no longer a purely technical decision, it is a strategic enabler that underpins modern operating models, digital services, and secure, resilient public services.

For most organisations, the focus has shifted from whether to use cloud to how to adopt and operate cloud services in a way that delivers measurable outcomes, maintains trust, and meets regulatory and security obligations.

Cloud technologies can help organisations reduce cost, improve resilience, remove technology constraints and accelerate innovation. However, these benefits are only realised when cloud services are implemented and managed within a clear operational, security, and governance framework.

Typical cloud transformation opportunities include one or more of the following:

- Implementing cloud, hybrid, or on-premise environments to support modern application and service delivery
- Optimising existing services through the use of public cloud and SaaS platforms
- Enabling new digital services and operating models using cloud-native capabilities
- Moving to consumption-based pricing models that align cost with actual usage and demand.

Successful cloud adoption requires more than migration alone. It demands a coordinated approach to environment management, release and deployment control, security assurance and operational governance across the full-service lifecycle.

Key considerations that must be addressed include:

- **Alignment of business and technology objectives:** Confirming cloud solutions support business outcomes, service users and operational needs, rather than simply replicating existing ways of working
- **Service availability and resilience:** Designing and operating environments to minimise disruption, protect critical services and manage operational risk
- **Shared responsibility and operating models:** Understanding how responsibilities for security, support, and operations are distributed across cloud service providers, suppliers, and internal teams.

- **Data handling and protection:** Applying appropriate data classification, handling, and protection controls that reflect how data flows across cloud and hybrid environments
- **Privacy and regulatory compliance:** Checking data residency, processing, and access comply with GDPR and organisational policies
- **Technology lifecycle and future readiness:** Managing patching, upgrades, and architectural decisions to reduce technical debt and support future change.

A careful assessment of organisational needs, cloud service models, and supplier controls is required to address these considerations and select the most appropriate path to cloud adoption and operation.

As a trusted advisor, PwC provides structured frameworks and deep public sector experience to support clients across the intersection of **Business, Experience, and Technology**. We tailor our approach to each organisation's context, providing support:

- Across the full lifecycle from strategy through to delivery and live operation
- Through targeted interventions to address specific challenges during implementation or service operation.

Environment Management and Security Services

This section describes in more detail the service features and benefits included within this service definition document.

Environment Management and Security Services Description

Our Environment Management and Security Services provide a structured, secure and consistent approach to managing cloud and hybrid environments, supporting reliable delivery of digital services across the full-service lifecycle. The service helps organisations reduce operational risk, improve service stability and meet government security and compliance expectations.

The service covers the governance, processes, controls and tooling required to manage environments effectively from design and build through transition into live service and ongoing operations. It supports programme and project delivery by ensuring environments are appropriately configured, controlled, monitored and secured.

The services are aligned to ITIL best-practice and include environment management, release and deployment management, configuration management (CMDB), access control, security hardening and operational readiness. We provide assessment, strategy definition, service design, transformation, transition and ongoing managed support.

Our service supports cloud platforms and services used across the public sector and aligns with relevant government standards, including security, risk management and service assurance requirements. Support levels, service scope and delivery approach are agreed with buyers to meet organisational needs.

Environment Management and Security Services Features

- Cloud, hybrid and on-premise environment management
- Release, deployment and configuration management strategy
- Secure patching, upgrades and platform lifecycle management
- Multi-phase release planning and controlled deployments
- Change, configuration and asset management (CMDB)
- Cloud and SaaS security assurance and accreditation support

Environment Management and Security Services Benefits

- Reduces operational, security and delivery risk
- Improves reliability and availability of digital services
- Enables safe and controlled change across cloud environments
- Supports compliance with government and regulatory security standards
- Improves visibility, governance and assurance across environments
- Reduces cost through efficient environment and release management

- ITIL-aligned service management and operational governance
- Infrastructure, platform and environment security management
- Technical Design Authority and architecture assurance support
- Agile delivery using PwC BXT methodology (Business, Experience, Technology)

- Accelerates secure cloud adoption and service transition
- Strengthens security controls across platforms and services
- Supports consistent delivery across programmes and suppliers
- Increases confidence in live service operations and support

Our view on the service features and benefits within this service definition document are presented below.

1. Cloud, hybrid and on-premise environment management

Our service helps to define and manage the environment landscape required to support delivery and live operation of the service across cloud, hybrid and on-premise models. This includes identifying environment types, intended usage, ownership boundaries, access controls, and coordinating environment usage during delivery and transition to live. The service focuses on orchestration, consistency and alignment with client hosting and operating models rather than hands-on infrastructure operation.

2. Release, deployment and configuration management strategy

We can work with you to define the approach, standards, controls and tooling used to manage configuration and deploy changes across your environments. This includes version control practices, repository structure, branching and merging strategy, promotion paths and quality assurance controls to make deployments traceable, repeatable, and aligned with agreed governance.

3. Secure patching, upgrades and platform lifecycle management

This approach establishes how your platform, application and dependency patches or upgrades are assessed, planned, and applied throughout the service lifecycle. This includes defining supported versions, aligning with vendor release cycles, assessing risk and impact and scheduling updates to maintain security, stability, and platform currency with minimal disruption.

4. Multi-phase release planning and controlled deployments

We can structure delivery into phased releases to support incremental delivery of value. This includes defining release objectives, sequencing, scope boundaries, release windows, dependency management, readiness checks and coordination of controlled deployments through the agreed route-to-live process.

5. Change, configuration and asset management (CMDB)

We can support the management of changes, configurations and assets through appropriate records and controls. This includes maintaining visibility of configuration items, their relationships, and changes across environments to support traceability, impact assessment, auditability and operational stability.

6. Cloud and SaaS security assurance and accreditation support

Our approach provides support for security assurance activities related to cloud and SaaS services. This includes aligning service controls to organisational and regulatory security requirements, supporting accreditation processes and providing evidence to demonstrate compliance within shared responsibility models.

7. ITIL-aligned service management and operational governance

We apply ITIL-aligned service management practices to support operational governance. This includes incident, problem, change, and service continuity considerations, ensuring services are operated in a controlled, predictable manner and aligned with client service management frameworks.

8. Infrastructure, platform and environment security management

We will work with you to define and apply appropriate security controls across infrastructure, platforms, and environments. This includes access control, segregation of duties, data protection, encryption, auditability, environment hardening and alignment with client security policies and shared security responsibilities.

9. Technical Design Authority and architecture assurance support

Our approach provides technical design authority and architecture assurance so your solutions aligns with agreed standards, non-functional requirements and strategic direction. This includes reviewing designs, validating technical decisions, managing deviations and ensuring consistency across the delivery lifecycle.

10. Agile delivery using PwC BXT methodology (Business, Experience, Technology)

We deliver services using PwC's BXT methodology, integrating business outcomes, user experience, and technology delivery. This approach supports iterative delivery, early value realisation and close collaboration with stakeholders while maintaining appropriate governance and control.



Confidential. This document does not constitute a Call-Off Contract for Services with PricewaterhouseCoopers LLP. Where we are engaged to provide Services, our Services will be governed by a subsequent Call-Off Contract that may be entered into between us. If you receive a request under freedom of information legislation to disclose any information we provided to you, you will consult with us promptly before any disclosure. All information contained in this document or otherwise provided or made available as part of any Award Procedure is confidential and may not be disclosed to anyone else without our prior consent.

© 2026 PricewaterhouseCoopers LLP. All rights reserved. 'PwC' refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.