

Cloud landing zone & platform engineering

Service overview

The Cloud Landing Zone & Platform Engineering Service supports public sector organisations to establish secure, standardised cloud foundations that enable safe and scalable delivery of digital services. The service focuses on creating well-governed platform environments that support consistent deployment, security, cost control and operational assurance across public, private or hybrid cloud.

The service is suitable for organisations at early or intermediate stages of cloud adoption, or those seeking to improve control and consistency across existing cloud estates.

Scope of the service

drie works with customers to design and implement cloud landing zones and shared platform components that are proportionate to organisational needs and risk appetite. The service focuses on implementation rather than ongoing operational management.

Depending on requirements, the service may include:

- Design of cloud landing zone architectures
- Account or subscription structure and environment segmentation
- Identity and access platform integration
- Network and connectivity configuration
- Security guardrails, policies and baseline controls
- Platform automation and infrastructure as code
- Standardised deployment patterns and templates
- Documentation and knowledge transfer

All activities are agreed in advance to ensure clarity of scope, cost and outcomes.

Delivery approach

Delivery follows established public sector digital delivery practices, aligned to the GDS Service Manual and agile principles. Work is delivered iteratively, allowing early validation of design decisions and progressive implementation of platform capabilities.

Engagements are typically time-boxed, with regular checkpoints to review progress, manage risk and confirm alignment with organisational objectives. Delivery is primarily remote, with on-site engagement available by agreement. The service may be delivered on a fixed-price or time-and-materials basis depending on scope and complexity.

Security, governance & assurance

Security and governance are embedded into platform design and delivery. This includes role-based access controls, secure network configuration, encryption, segregation of environments, policy enforcement and audit logging.

The service supports alignment with organisational security policies and UK regulatory requirements, including UK GDPR. Platform controls are designed to support auditability, accountability and ongoing assurance. The service does not provide formal certification or regulatory approval.

Customer responsibilities

The customer is responsible for defining platform standards, governance requirements and risk tolerance. The customer retains ownership of cloud accounts, data and service outcomes. The customer is also responsible for operating and maintaining the platform once delivered unless additional managed services are agreed.

Timely access to cloud platforms, identity systems and relevant stakeholders is required to support effective delivery.

Service outputs

Outputs are agreed as part of the service scope and may include implemented landing zones, platform configurations, automation templates, documentation and operational guidance. Outputs are designed

to support consistent service delivery and future platform evolution.

Exit and handover

At the end of the engagement, drie provides documentation and knowledge transfer to support continuity and sustainability. Any ongoing monitoring, retraining or support is subject to a separate agreement.

drie