

Cloud security engineering & assurance service

Service overview

The Cloud Security Engineering & Assurance Service supports public sector organisations to design, implement and assure secure cloud environments used to deliver live digital services. The service focuses on embedding proportionate security controls, governance and assurance mechanisms that align to organisational risk appetite, regulatory obligations and public accountability.

The service is suitable for organisations adopting or operating cloud services that require confidence in security posture, compliance and ongoing assurance.

Scope of the service

drie works with customers to engineer and assure cloud security controls that are appropriate to their operating context and maturity. The service focuses on implementation and assurance rather than advisory-only activity.

Depending on requirements, the service may include:

- Assessment of existing cloud security posture and risks
- Design of cloud security architectures and controls
- Identity and access management configuration
- Network, platform and data security controls
- Security configuration hardening and guardrails
- Logging, monitoring and alerting configuration
- Support for audit preparation and assurance activities
- 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 to reduce risk and enable early validation of controls.

Engagements are typically time-boxed, with regular checkpoints to review progress, manage risk and confirm alignment with organisational security 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 central to this service. Controls are implemented to support confidentiality, integrity and availability, including role-based access controls, encryption, environment segregation and audit logging.

The service supports alignment with organisational security policies and UK regulatory requirements, including UK GDPR. It also supports assurance activities through documented controls and evidence but does not provide formal certification or act as a regulatory authority.

Customer responsibilities

The customer is responsible for defining security requirements, risk tolerance and compliance obligations. The customer retains ownership of systems, data and security decisions, and is responsible for operating security controls once implemented unless additional managed security services are agreed.

Timely access to systems, information and stakeholders is required to support effective delivery.

Service outputs

Outputs are agreed as part of the service scope and may include implemented security controls, configuration artefacts, security documentation, assurance evidence and operational guidance. Outputs are designed to support ongoing assurance and audit readiness.

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