IBM Technology

G-Cloud 15
IBM – Hashicorp Terraform Enterprise

Service Definition Document

Email: ukcat@uk.ibm.com
Contact: Anne-Marie Wheeler

Contents

Overview

Service Description

This Service Definition describes HashiCorp Cloud Platform (HCP) Vault, a managed cloud service that provides secure secrets management, encryption as a service, and identity based access control for applications and infrastructure. HCP Vault enables UK public sector organisations to centrally manage sensitive data such as credentials, API keys, tokens, and certificates, supporting secure digital service delivery while meeting governance, audit, and compliance requirements. HashiCorp Vault enables the UK Government to centrally eliminate credential-based cyber risk across all digital services by replacing static secrets, shared credentials, and manual key management with identity-based, policy-driven, and fully auditable security controls. It provides a single, cloud-agnostic security control plane for secrets, encryption, and access to sensitive data—reducing the likelihood and impact of breaches, improving audit outcomes, and enabling secure digital delivery at national scale.

What is the service is?

HCP Vault is HashiCorp's fully managed, enterprise-grade secrets and encryption platform delivered as a cloud service. The service provides a secure system of record for secrets and cryptographic operations, enabling applications, platforms, and users to authenticate, retrieve secrets dynamically, and encrypt or decrypt sensitive data without embedding secrets in code or configuration files. HCP Vault removes the operational burden of deploying, securing, scaling, and maintaining Vault infrastructure while providing enterprise controls, availability, and support.

How Terraform Works (Enterprise Context)

Terraform uses a **declarative model** to manage infrastructure:

- Infrastructure is defined as code using human-readable configuration files
- Providers translate those definitions into API calls against target platforms
- Terraform calculates the difference between the current and desired state
- Only the required changes are applied

HCP Terraform enhances this model by providing a central execution and governance layer, ensuring that infrastructure changes are consistent, secure, and traceable across teams and departments.

Core Terraform Capabilities Delivered by HCP Terraform

Remote Execution and Controlled Change Management

HCP Terraform executes Terraform plans and applies in managed, ephemeral runtime environments operated by HashiCorp. This ensures:

- Consistent execution environments across teams
- Isolation of runs to prevent cross-contamination
- Removal of cloud credentials from developer laptops
- Controlled promotion of changes through approval workflows

This model supports separation of duties between infrastructure authors, reviewers, and approvers — a key requirement in public sector environments.

Secure State Management

Terraform maintains a state file that represents the current known configuration of infrastructure. Loss or corruption of this state can result in operational risk.

HCP Terraform provides:

- Encrypted state storage at rest and in transit
- Automatic state versioning and recovery
- Locking to prevent concurrent modifications
- Centralised access control over sensitive infrastructure metadata

This eliminates the risks associated with locally stored or unmanaged state files.

Workspaces and Environment Isolation

HCP Terraform uses workspaces to logically separate infrastructure by environment, application, department, or security boundary.

Workspaces enable:

- Clear separation of development, test, and production environments
- Departmental isolation within shared platforms
- Fine-grained role-based access control
- Clear ownership and accountability for infrastructure resources

This model aligns well with UK Government operating structures and shared service environments.

Policy as Code and Preventative Governance

HCP Terraform enables organisations to define and enforce policies that govern how infrastructure can be provisioned.

Policies can be used to:

- Prevent deployment of resources in unauthorised regions
- Enforce encryption, logging, and network security controls
- Require tagging and cost-allocation standards
- Block non-compliant configurations before deployment

Policies are evaluated automatically as part of the Terraform workflow, enabling preventative controls rather than reactive remediation.

Private Module Registry and Standardisation

HCP Terraform provides a private registry for Terraform modules and providers.
This enables platform teams to:

- Publish approved, security-hardened infrastructure patterns
- Version and manage reusable components
- Reduce duplication and configuration drift
- Enable delivery teams to consume compliant infrastructure by default

For UK Government, this supports “build once, use many times” approaches across departments and programmes.

Version Control Integration and Collaboration

HCP Terraform integrates natively with enterprise version control systems, enabling infrastructure changes to follow standard software development lifecycle practices.

This includes:

- Automated plan generation on code changes
- Review and approval via pull requests
- Controlled application of changes on merge

- Full traceability from code change to deployed infrastructure

Auditability and Assurance

All actions within HCP Terraform are logged and traceable, including:

- Who initiated a change
- Who approved or rejected it
- What infrastructure was modified
- When the change occurred

This supports audit, assurance, and compliance reporting requirements without additional tooling.

Why HCP Terraform is Needed for UK Government

UK Government organisations operate complex hybrid estates while being subject to strict security, governance, and audit obligations. Traditional manual provisioning and fragmented automation approaches result in inconsistent configurations, elevated operational risk, and limited visibility.

HCP Terraform addresses these challenges by:

- Standardising infrastructure delivery across departments
- Embedding governance and security into deployment workflows
- Reducing reliance on manual processes
- Improving audit readiness and operational assurance
- Enabling platform-led operating models at scale

Service Options

HCP Terraform is provided as a fully managed SaaS offering operated by HashiCorp.
Service options include:

- Deployment in European regions to support data residency requirements
- Integration with major public cloud providers
- Integration with enterprise identity providers and CI/CD pipelines
- Enterprise support and commercially backed service levels

Value Proposition for UK Government

- Consistency: Standardised infrastructure across programmes and departments
- Security: Centralised control of credentials, state, and execution
- Governance: Preventative policy enforcement aligned to public sector standards
- Auditability: Full traceability of infrastructure change activity
- Efficiency: Faster delivery through reusable modules and automation
- Scalability: Supports multi-department and whole-of-government platforms

Conclusion

HCP Terraform provides UK Government organisations with a secure, governed, and enterprise-ready platform for Infrastructure as Code. By combining Terraform's declarative infrastructure model with a managed control plane, HCP Terraform enables scalable digital transformation while maintaining the levels of control, assurance, and resilience required in the public sector.