

Azure Landing Zone Assessment

G-Cloud

January 2026

Table of Contents

1	Service Overview
2	Our Approach
3	Getting Started
4	Your Responsibilities
5	Security & Compliance
6	Support & Exit
7	Why Appvia
8	Contact Us

Azure Landing Zone Assessment

Comprehensive technical assessment of your Azure environment against NCSC Cloud Security Principles and Microsoft Cloud Adoption Framework. Independent assurance for UK public sector organisations.

1 Service Overview

Appvia's Azure Landing Zone Assessment provides independent assurance that your cloud infrastructure meets government security standards. We evaluate your environment against the NCSC 14 Cloud Security Principles and Microsoft Cloud Adoption Framework.

What you get:

- **NCSC gap analysis** — Assessment against all 14 Cloud Security Principles
- **CAF alignment review** — Microsoft Cloud Adoption Framework methodology
- **Security controls evaluation** — CIS Benchmarks and Azure security baseline
- **Supply chain assessment** — Aligned with NCSC Principle 8
- **Risk identification** — Prioritised findings with mitigation strategies
- **Remediation roadmap** — Actionable recommendations by risk priority
- **Evidence pack** — Documentation for SIRO and IAO sign-off
- **Cost optimisation** — Recommendations for operational efficiency

This assessment supports business case approvals and provides assurance for Senior Information Risk Owners.

2 Our Approach

We follow a structured assessment methodology to provide comprehensive, actionable insights.

How we assess:

Our certified Azure engineers review your environment using Azure Advisor, Microsoft Defender for Cloud, and manual configuration review. We evaluate:

Area	What we assess
Security	RBAC, encryption, network controls, logging, Defender for Cloud
Compliance	NCSC principles, CIS benchmarks, Azure security baseline
Architecture	Management groups, subscriptions, networking, resilience
Operations	Backup, DR, change management, incident response
Cost	Resource utilisation, reservation coverage, waste

Deliverables: - Executive summary for senior stakeholders - Detailed technical findings report - Risk-prioritised remediation roadmap - Evidence pack for compliance sign-off

3 Getting Started

A typical assessment takes 2-4 weeks depending on environment complexity:

Phase 1: Discovery We gain read-only access to your Azure environment and conduct initial automated scans. We gather documentation and interview key stakeholders.

Phase 2: Assessment Deep-dive analysis of security controls, architecture patterns, and operational practices. We validate findings and identify root causes.

Phase 3: Reporting We present findings to technical and senior stakeholders, deliver the evidence pack, and agree remediation priorities.

Prerequisites: - Reader access to Azure subscriptions under assessment - Access to relevant documentation (architecture diagrams, policies) - Availability of security and platform team members for interviews

4 Your Responsibilities

To ensure successful service delivery, you will need to:

- Provide timely access to required resources, stakeholders, and information
- Make appropriate subject matter experts available for design and integration discussions
- Ensure business users are available for acceptance testing as agreed
- Procure necessary software licenses and subscriptions
- Empower your project team to make decisions in a timely manner
- Review and approve deliverables based on agreed acceptance criteria
- Provide Reader access to Azure subscriptions under assessment
- Share relevant architecture documentation and security policies
- Make security and platform team members available for interviews
- Identify stakeholders for findings presentation

5 Security & Compliance

This service supports workloads classified up to **Official-Sensitive** where appropriate controls are in place.

Our security credentials:

- **ISO 27001:2013** and **ISO 9001:2015** certified
- **Cyber Essentials Plus** certified
- **75%+ of our team hold SC clearance**
- All access to customer environments is logged and auditable
- Data remains within UK regions unless explicitly agreed

We operate in alignment with GDS, NCSC, and CDDO security principles.

6 Support & Exit

Ongoing Support

- Dedicated Service Delivery Manager as your primary contact
- Regular service reviews with clear reporting on performance and incidents
- Defined change management aligned with ITIL best practices

Knowledge Transfer

We embed knowledge sharing throughout our engagement: - Documented runbooks and operational procedures - Regular knowledge sharing sessions with your team - Post-incident reviews that share learnings

Exit Process

When the engagement ends, we ensure an orderly transition: - Complete documentation of all configurations and procedures - Knowledge transfer sessions as required - 90-day standard notice period - No disruption to your services during handover

7 Why Appvia

We're a UK-based SME with deep expertise in cloud platforms and a strong track record delivering for UK government.

Cloud Partnerships

- AWS Advanced Tier Services Partner & Public Sector Partner
- Microsoft Azure Solutions Partner
- Google Cloud Partner

Open Source Credentials

- Creators of Terranetes (CNCF project for Terraform on Kubernetes)
- Developers of Wayfinder, a self-service cloud platform

Public Sector Experience

We understand the unique requirements of government and public sector organisations, from security clearance to GDS service standards.

"Appvia have helped us realise our cloud-first strategy with excellent product solutions. The security, governance and peace of mind brought in by the cloud landing zone has dramatically accelerated our journey to cloud-native adoption."

— **Peter Macchiocci**, Bank of England, Head of Platform Engineering

8 Contact Us

To discuss your requirements or request a detailed proposal, contact our Public Sector Team.

Phone: 020 3917 2888

Email: sales@appvia.io

Website: www.appvia.io

When you get in touch, please include: 1. The name of this service 2. Your organisation name 3. Your contact details 4. A brief description of your requirements

We'll arrange a discovery call to understand your needs and provide a tailored response.

Appvia helps organisations build, secure, and innovate across cloud, data platforms, and AI by blending practical engineering expertise with real-world experience.



About Appvia

Appvia helps organisations build, secure, and innovate across cloud, data platforms, and AI by blending practical engineering expertise with real-world experience. Drawing on our background in creating open source CNCF projects like Terranetes and our self-service developer platform, Wayfinder, we bring that industry know-how and expertise into your organisation to help unlock the true value of the Cloud. As an AWS Advanced Tier Partner and a Microsoft Solutions Partner, we specialise in delivering secure, scalable cloud-native platforms and services, including containerisation, FinOps, modernisation, and AI integration.

Build, secure, and innovate in the cloud | www.appvia.io



This document contains information that may be privileged or confidential and is the property of Appvia Ltd.

Public Copyright 2026 Appvia Ltd. All rights reserved.