Government Cyber Action Plan

Task Summary January 2026

Purpose

The Government Cyber Action Plan sets out a major reform of how cyber security and digital resilience are managed across UK central government and the wider public sector. It responds to critically high levels of cyber risk caused by legacy technology, fragmented accountability, skills shortages, and increasingly sophisticated cyber threats.

Overall Aim

To ensure public services are secure, trustworthy, and resilient, so that essential services can continue to operate during cyber-attacks or major digital failures.

Strategic Objectives

1. Improve visibility and understanding of cyber and digital resilience risk across government.

2. Address the most severe and complex risks that cannot be managed by individual organisations alone.

3. Strengthen preparation, response, recovery, and learning from cyber incidents and major outages.

4. Rapidly raise the baseline level of cyber resilience across the public sector.

Delivery Model

The plan is delivered through five strands: accountability, central support, shared cyber services, incident response and recovery, and skills development. Accounting Officers are personally accountable for cyber risk, supported by stronger central coordination and intervention where risks are high.

Government Cyber Unit

A new Government Cyber Unit within DSIT, led by the Government CISO, acts as the central authority for managing cyber risk. It sets mandatory standards, coordinates incident response, oversees strategic suppliers, and manages over £210 million of central investment.

Implementation Timeline

Phase 1 (to March 2027): establish governance, services, and the Government Cyber Profession.

Phase 2 (2027–2029): scale services and mature response capabilities.

Phase 3 (2029 onwards): continuous improvement and sustained resilience.

Key Message

Cyber security is treated as a core leadership and operational responsibility, on a par with finance, safety, and national security. The plan represents a system-wide shift from siloed assurance to collective defence and resilience.