UK Government

Government Cyber Action Plan

CP 1473

Government of the United Kingdom

Department for Science, Innovation and Technology

Government Cyber Action Plan

Presented to Parliament
by the Minister of State for Digital Government and Data
by Command of His Majesty

January 2026

CP 1473

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at: correspondence@dsit.gov.uk

ISBN 978-1-5286-6152-2
E03515734 01/26

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty's Stationery Office

Contents

Foreword

Ministerial Foreword

The first duty of this Government is to keep the country safe; that never changes. In today's volatile world, security extends beyond physical borders into the digital realm. Hostile states and criminal groups are actively probing our defences, seeking to disrupt our way of life and undermine our national interest.

We must be clear eyed about what is at stake. We are more connected than ever before, and that progress brings immense benefits to our economy and our society. Modern, secure digital services can transform lives by making government faster, more responsive, and more accessible for everyone. Whether you are accessing healthcare, need advice to start a business, claiming benefits or verifying identity, digital transformation enables us to deliver the efficient, citizen-focused services that people rightly expect.

This is central to the Prime Minister's Plan for Change and our mission to renew the state. These are not optional extras; they are the critical infrastructure of modern British life.

As we innovate and expand, the surface area for risk grows with it. Cyber attacks have inflicted real damage on our institutions. Whether the goal is financial theft or strategic disruption, the intent to strike at the heart of our public sector is real. Even when we are not facing hostile attacks, too many systems are prone to accidental failures. We cannot build a secure future on fragile foundations.

Cyber risk is a challenge facing not just government, but our entire society. The Cyber Security and Resilience Bill will protect more essential and digital services from cyber attacks, requiring them to have appropriate and proportionate measures in place to manage risks, and better prevent disruption to healthcare, drinking water providers, transport and energy. Our response for government is the Government Cyber Action Plan, which will hold government and the public sector to equivalent standards.

The Department for Science, Innovation and Technology (DSIT)'s State of Digital Government Report set out publicly that the cyber risk to government is critically high. To meet the threats we face we must transform how we approach cyber security in government. The Government Cyber Action Plan is a core deliverable within the Roadmap for Modern Digital Government, part of broader activity to strengthen public sector infrastructure. It sets out how government will take proactive, risk-led action with clear accountability, mandatory requirements, and comprehensive central support.

The newly formed Government Cyber Unit, backed by over £210 million of central investment, will drive the plan forward, setting much stronger central direction, backing departments with expert support whilst demanding measurable progress. This investment works twice as hard for us: by raising standards in government, we drive skills and innovation across the economy, reinforcing our leadership alongside our international partners.

Too often, however, we are let down by underlying existing infrastructure which is not adequately resilient. Our legacy systems often cannot be defended by modern cyber security measures. We know that historical underinvestment in both technology estates and proportionate cyber security measures have left us with a significant technical debt whilst the threat we face is rapidly evolving and is the most sophisticated it has ever been.

Every public sector leader bears direct accountability for this effort, departments must urgently invest in replacing legacy systems and fixing foundational vulnerabilities.

We are not starting from scratch; we are scaling what works, learning from successes across the public sector and our international partners. This plan will go further than we have before, prioritising cyber resilience and ensuring we have strong central leadership driving cross-government response. It will enable departments, through central services and targeted support, and will see the launch of a new Government Cyber Profession which will not only ensure we continue to attract and retain the best talent but also support development skills throughout the UK.

This is more than just a change; it is a steadfast commitment to defending the state and protecting the daily lives of working people. By fixing these foundations, we will build a government that is resilient, secure, and ready for national renewal.

Rt Hon Ian Murray
Minister of State for Department for Science, Innovation and Technology

1

Introduction

Introduction

The Prime Minister has been clear that the government exists to unite the country behind a shared purpose: to protect citizens, back public services, and secure opportunities for every family. In that spirit, this document sets out the practical, measurable steps we will take to rapidly improve the cyber security and resilience of the government and the public sector, to keep the British people safe and confident in digital government.

The digitisation of public services offers huge advantages to the UK: we can deliver services that are more efficient, convenient and better value for money for taxpayers. However, realising these benefits relies on securing public services so that they are trustworthy and resilient. Without achieving this, increasing digitisation exposes us to increasing levels of cyber and digital resilience risk.

The Government Cyber Action Plan defines how we will secure **public services so they are trustworthy and resilient**, as part of the broader Roadmap for a Modern Digital Government.

The scale of the challenge

As the National Security Strategy 2025 sets out, protecting the UK and promoting British interests is becoming more difficult. We are increasingly targeted by state threats and organised crime groups who seek to exploit our vulnerabilities. The UK has experienced repeated, systemic failures in our digital resilience and we know from experience that these pose unacceptable costs to UK citizens, from compromised personal data, to loss of access to basic public services.

When digital systems fail, whether through a malicious cyber attack or a non-malicious outage, the impacts are immediate and profound. The cyber attack on Synnovis, which halted blood testing and forced the cancellation of surgeries across London, demonstrated how quickly a digital disruption can escalate into a major healthcare emergency. Similarly, ransomware incidents affecting local councils have incapacitated social care systems, leaving frontline workers unable to access vital information to protect vulnerable individuals. These failures are not hypothetical risks, they are recurring realities that result in service breakdown, harm to the public and erosion of trust in these services by the communities who rely on them.

Since launching the Government Cyber Security Strategy (GCSS) in 2022, we have taken important steps to understand complex government systems and reduce cyber risk.[1] We established the Government Cyber Coordination Centre (GC3) to enable a single, whole of government response to incidents, threats and vulnerabilities. Our Secure by Design approach builds resilience into implementing future government digital services.[2] Our new assurance framework, GovAssure, has, for the first time, given us an objective picture of resilience levels across government systems.[3] These initiatives have delivered real improvements and given us the tools to understand the scale of the challenge we face.

[1] Government Cyber Security Strategy: 2022 to 2030

[2] Department of Science, Innovation and Technology (DSIT), Government Digital Service (GDS) (2025), State of digital government review

[3] Cabinet Office (2022), The UK Government Resilience Framework: 2023 Implementation Update

That challenge is significant, and cyber risk to the public sector is currently critically high.

The State of Digital Government Review in January 2025 identified the systemic challenges underpinning our current resilience status as:

- institutionalised fragmentation
- persistent legacy, cyber security and resilience risks
- siloed data
- under-digitisation
- inconsistent leadership
- a digital skills shortfall
- diffuse buying power
- outdated funding models

GovAssure's first year results found significant gaps in departments' cyber security and resilience, including widespread low maturity in fundamental controls such as asset management, protective monitoring, and response planning. Nearly a third (28%) of the government technology estate is estimated to be legacy technology, and therefore highly vulnerable to attack.

In addition, the UK Government's ability to defend against threats is not keeping pace with an ever evolving threat environment. The National Audit Office has highlighted the challenge of defending our digital estate from sophisticated cyber threats by nation states and organised crime groups, and the National Cyber Security Centre's (NCSC) Annual Review 2025 sets out the evolution of the threat environment and the continued targeting of the public sector by both state and criminal actors.[4]

Malicious cyber attacks and non-malicious digital resilience failures alike continue to disrupt government as demonstrated by the 2023 British Library ransomware attack and 2024 CrowdStrike outage respectively.

Case study – British Library ransomware attack (2023)

In October 2023, the British Library was hit by a major ransomware cyber-attack by the Rhysida gang.

Key impacts:

- most online systems were shut down
- data was stolen, encrypted, or destroyed
- all users were locked out

The attack revealed serious weaknesses due to underinvestment in technology and cyber defences. Recovery is ongoing and the Library is now planning major upgrades.

[4] National Audit Office (January 2025), Government Cyber Resilience

Case study – 2024 CrowdStrike outage

In 2024, a major IT outage caused by a CrowdStrike software update, disrupted thousands of services across the UK.

The incident:

- cost the UK economy between £1.7 and £2.3 billion
- despite not being a cyber-attack, it required a cross-government response
- exposed vulnerabilities similar to those seen in malicious incidents
- showed how single supplier dependency can create widespread disruption

A radical shift

Given this context, we now recognise that the target set out in the GCSS for **all government organisations to be resilient to known vulnerabilities and attack methods** is not achievable by the original target date of 2030. To protect our critical national infrastructure, defend public institutions and maintain public confidence in essential public services, we must achieve a radical shift in approach and a step change in pace.

We've learned from international and industry partners that a strong, centralised approach, with clear direction and active leadership can make a huge national impact. We have worked with departments and NCSC to define and pilot what this will look like for the UK public sector.

The Government Cyber Action Plan sets out a new way forward. It was developed by the Department for Science, Innovation and Technology (DSIT), in close consultation with departments, public sector organisations, industry partners and the Government Cyber Advisory Board (GCAB).

It builds on the outcomes and approach of the GCSS by setting clear expectations of how government organisations of all kinds should manage cyber security and resilience through more measurable objectives and outcomes. These are set out at a high level in the 'Who is responsible for what' section at the beginning of each chapter.

2

Approach

Scope

The Government Cyber Action Plan sets out how the whole of government will operate differently to manage the cyber security and resilience threat we face, enabled by a strong, active centre in the Government Cyber Unit.

Central functions

Department for
Science, Innovation
& Technology

Department for Science, Innovation and Technology (DSIT): the government department responsible for driving forward a modern digital government for the benefit of its citizens. The DSIT Permanent Secretary owns cross-government technology risk, including cyber risk. DSIT supports the DSIT Permanent Secretary in managing this risk.

The Government Cyber Unit: the central unit within DSIT responsible for driving cyber security and resilience transformation across government and the public sector. The Government Cyber Unit is led by the Government Chief Information Security Officer (CISO), and will be the strong, active, centre that drives this action plan through clear direction, stronger accountability, and targeted support to departments. The Government Cyber Unit will manage government-wide cyber risk on behalf of the DSIT Permanent Secretary.

Government Cyber Coordination Centre (GC3): part of the Government Cyber Unit, and jointly sponsored with the National Cyber Security Centre. It coordinates the cross-government response to cyber threats, vulnerabilities and incidents. Its role is primarily operational, and enables cyber teams across government to defend as one.

Cabinet Office

Government Security Group (GSG): part of the Cabinet Office responsible for the oversight, coordination and delivery of protective security across government. The Government Cyber Unit will work closely with GSG to ensure a coherent approach.

National Cyber
Security Centre
a part of GCHQ

National Cyber Security Centre (NCSC): the UK's National Technical Authority (NTA) for cyber security. NCSC is the authoritative voice on technical cyber security and threat assessment, providing expert advice and guidance. It coordinates the majority of nationally significant cyber incidents and supports the defence of the UK's most critical systems. NCSC will work alongside the Government Cyber Unit, providing specialist expertise and guidance to support government-wide cyber security and resilience.

The UK's other NTAs, the **National Protective Security Authority (NPSA)** for physical and personnel security and the **UK National Authority for Counter-Eavesdropping (UK NACE)** for technical security, may also contribute to government cyber security and resilience. Where they do, it is broadly expected that they would follow the model outlined for NCSC, and it will be explicitly called out where this is not the case.

Departments: organisations accountable to UK Ministers responsible for putting government policy into practice, which may be ministerial or non-ministerial. Departments remain accountable for their own cyber security and resilience.[5] Most departments also have 'lead government department' responsibility for other organisations, sectors, or systems. Wherever this is the case, they are accountable for the cyber security and resilience of those too. Departments must also contribute to government-wide cyber security and resilience.

The Government Cyber Unit will work directly with departments to ensure they are able to meet all of these responsibilities. This will include clarifying how these responsibilities should be met in practice, as well as offering support and services, in collaboration with NCSC and other partners.

Arm's-length bodies (ALBs): a category of public bodies that are a critical delivery arm of the government, providing public services and goods across the United Kingdom. ALBs are closely aligned, but distinct from, the ministerial departments which sponsor them, their 'lead government department' (LGD). This includes executive agencies, non-departmental bodies, and non-ministerial departments, which will be collectively referred to as 'ALBs'.

ALBs are accountable for their own cyber security and resilience to their LGD via pre-existing sponsorship mechanisms. The Government Cyber Unit will generally work through sponsor departments to ensure that ALBs are able to meet their cyber security and resilience responsibilities, but where it makes sense to do so the Government Cyber Unit may work directly with ALBs in alignment with LGD activity.

Wider public sector organisations: organisations publicly funded to deliver services, usually at a local or regional level, for example National Health Service (NHS) trusts or local authorities.

Wider public sector organisations are accountable for their own cyber security and resilience to the LGD for their sector via pre-existing sponsorship mechanisms, for example the Department of Health and Social Care is the LGD for the health and care sector.

LGDs are accountable for sector-wide cyber security and resilience. The Government Cyber Unit will work with LGDs to ensure sector-wide cyber security and resilience is appropriately managed, and where it makes sense to do so, may work directly with wider public sector organisations in alignment with LGD activity.

Departments, ALBs, and wider public sector organisations will be referred to collectively throughout this document as 'government organisations'.

[5] This is derived and set out in Functional Standard 007: Security

Devolved governments: While cyber security - within the wider remit of national security - is a reserved matter, within Scotland, Wales and Northern Ireland, certain devolved public services are the responsibility of the respective governments.

Devolved governments will seek to ensure that the providers of public services for which they have oversight are resilient to cyber risks and will collaborate with UK Government on UK-wide cyber security and resilience issues.

The UK Government recommends that devolved governments support and align with the ambitions of the Government Cyber Action Plan. Devolved governments will consider this where it does not affect their ability to exercise devolved powers and functions as they see fit. UK Government will continue to lead on national security and collective issues which are reserved, collaborating with devolved governments.

UK Government and devolved governments will proactively collaborate and share relevant information (as permitted by law) in order to effectively manage the UK's cyber security.

Strategic suppliers: designated as government's 'strategic suppliers' due to the scale and/or criticality of the services they provide to the government. The government takes a joined-up approach to strategic suppliers in order to act as a single customer and ensure a single and strategic view of the government's need is communicated. The Government Cyber Unit will establish formal 'strategic partnerships' with strategic suppliers with cyber security and resilience requirements built into them, enabling the Government Cyber Unit to hold strategic suppliers to account for management of the government-wide cyber risk they hold.

All suppliers: every supplier that delivers for government holds some cyber risk. Government organisations are responsible for managing the cyber risk posed by suppliers they use. This document will set out clear expectations for how suppliers should interact with their government customers around cyber security and resilience.

Objectives

The ultimate goal of the Government Cyber Action Plan is to achieve the aim set out within the Digital and AI Roadmap of 'securing public services so they are trustworthy and resilient'. In order to achieve this within the current challenging threat and resilience context, we have identified four strategic objectives.

These objectives will guide our action and help us to prioritise where we can have the greatest systemic impact on the current unacceptable level of cyber security and resilience risk faced by government:

Better visibility of cyber security and resilience risk

We will measure what matters, using data sources from across the government to truly understand government-wide and departmental cyber risks. Better visibility will underpin action and help us to prioritise where we can have the greatest impact.

Addressing severe and complex risks

We will identify and assess severe and complex risks across government, and invest in central levers and capability improvements to remediate where these cannot be addressed by departments acting individually.

Improving responsiveness to fast moving events

We will integrate and enhance our capability to respond more effectively to rapidly evolving cyber and digital resilience threats, vulnerabilities, and incidents. Better preparedness will improve recovery times and reduce harm.

Rapidly increasing government-wide cyber resilience

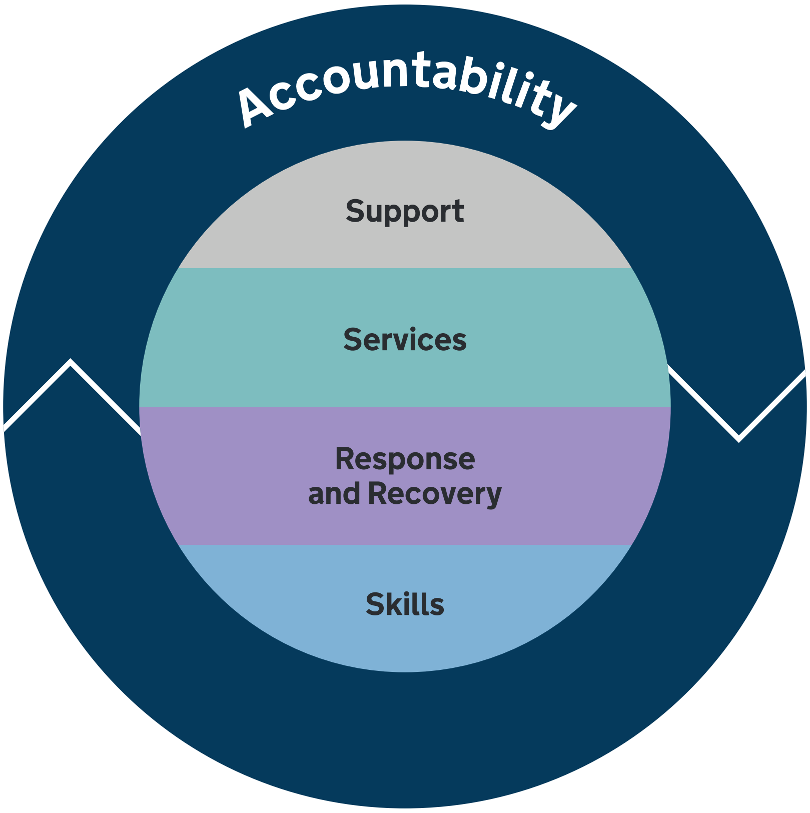
Departments and public bodies will transform their resilience capabilities through high-quality central services and support. We will focus on remediating our most significant vulnerabilities, such as our legacy technology, and will operationalise knowledge sharing and continuous improvement across the system.

Achieving these objectives will deliver tangible benefits. The public will see faster service recovery and better communication when things go wrong. Departments will get more hands-on support and practical guidance. This will include a central governance model, a wider services offer, routine cross-government exercises, and a clearer system for recruiting, attracting, and retaining cyber staff through career pathways, apprenticeships, secondments, and industry partnerships.

This is not just a technical transformation. It is a cultural and operational shift in how the government views resilience. Every leader, every public sector organisation, every supplier has a role to play. Together, with clarity of purpose and shared accountability, we can deliver a government that is more secure, more resilient, and able to protect the services on which citizens depend.

Delivery strands

The Government Cyber Unit will drive progress towards these strategic objectives by working with NCSC, departments, devolved governments, and suppliers across five delivery strands: **Accountability, Support, Services, Response and Recovery, and Skills**.



Accountability

Cyber risks at all levels of government must be actively owned and effectively managed, with those responsible held to account for effective management. This strand sets out responsibilities and accountability mechanisms to ensure they are met.

Support

Government organisations do not have access to the capability, skills and capacity needed to meet their cyber security and resilience responsibilities. This strand sets out how support will be provided, prioritised, and accessed to bridge this gap.

Services

Government organisations face cyber security and resilience challenges that could be addressed at scale, there are few services to enable this and those that do are not well understood or accessed. This strand outlines how scaled cyber services will be developed, delivered, and accessed to address this.

Response and Recovery

As well as proactively reducing risk, government must be able to quickly and effectively manage incidents when they occur. This strand sets out the responsibilities for cyber security and resilience incidents at all levels, that will enable us to collectively minimise their impact.

Skills

The demand for cyber security and resilience skills across government is growing faster than the supply of available talent. Leaders, functional professionals, and the wider workforce lack understanding of cyber risks and business impact. This strand outlines the establishment of the first Government Cyber Profession, which will attract, upskill, retain, and support government cyber professionals.

Delivery phases

The system-wide transformation for government cyber security and resilience requires a system-level response and all government organisations will have a role in the delivery of the new operating model.

The Government Cyber Unit will lead cross-government delivery in the key phases, outlined below.

Building

Phase 1: Building

By April 2027, we will build a new model for government cyber by:

- building critical functions to establish the Government Cyber Unit
- establishing refreshed accountability and governance for government cyber risk
- standing up prioritised central services and support functions
- setting clear targets and standards for government organisations
- launching a new cyber profession for government
- directing action across government in response to fast-moving events, through structures defined in a Government Cyber Incident Response Plan

Scaling

Phase 2: Scaling

By April 2029, we will scale and leverage this new model by:

- using government-wide cyber risk visibility to make data-driven decisions and a compelling investment case for managing severe and complex cyber risks
- delivering a pipeline of cyber support and services to help departments meet their responsibilities
- scaling and maturing response and recovery capability to address concurrent major cyber events
- developing high-impact, sector-wide role-based learning pathways for top high-risk cyber specialisms
- departments fully operating within governance and reporting structures for themselves, their ALBs, and sectors
- departments delivering costed cyber improvement plans in line with defined central and local cyber risk appetites, drawing on central support and services

Improving

Phase 3: Improving

From April 2029 and beyond, we will use the model to continuously improve government-wide cyber security and resilience by:

- enabling decision-making and prioritisation at all levels of government through sharing central cyber data insights, including evidence-based investment in cross-government platforms, services and infrastructure to address critical risks
- offering central cyber support and services at scale based on identified needs and strategic fit in a sustainable pipeline and lifecycle
- leveraging Government Cyber Profession as engine for transformation through career framework and sector recognised accreditation standards
- departments proactively assuring cyber risk across their supply chains, enabled by central management of strategic suppliers
- supporting national security and growth objectives and underpins government missions through increased resilience

Priorities for delivery over the next 12 months are set out at the end of each delivery strand chapter. Further detail on implementation phases and plans for measurement set out in **Chapter 9: Implementation**.

Cultural change

To deliver effective transformational change, embedding the right culture is vital.

Improving the interaction between people, processes, and technology across government requires a whole- system approach to make it easier and more rewarding for staff to adopt the right security behaviours. Defending organisations by improving security culture is therefore of vital importance.

There are a number of core cultural behaviours the Government Cyber Action Plan will embed across the public sector as follows.

Defend as One

Government and public sector teams view cyber and digital resilience as a collective mission, delivered in collaboration and partnership across their organisations. Government organisations collectively address government-wide cyber risk, even where it is not a priority for an individual organisation.

Data and decision making

Senior leaders are empowered through data sharing and understanding, using accurate data and information across organisations to enable effective government-wide risk management decision-making.

Proactive ownership

Senior leaders understand and meet their accountabilities, and drive change across all layers of government. Senior leaders also set the tone for the importance of security and accountability, including continuous risk management cycles of review, collaboration, innovation and assurance.

Transparency

Leaders create open and inclusive environments where sharing risks, issues, ideas and data is encouraged, lessons are learned and best practice is shared.

Empowered workforce

Our teams have the capability and career paths to deliver sustainable change through investment in tools, training and systems.

Safe environment

Individuals have the capability to report vulnerabilities and threats, feel safe to do so and feel confident to question and challenge without fear. Constructive behaviours are recognised and rewarded, while poor ones are addressed.

Case study: ‘Just Culture’ in health and care sector information governance and cyber security

In 2024, NHS England published guidance on adopting a just culture in relation to information governance and cyber security in health and care settings.[6] It aims to foster openness and fairness when assessing incidents and near misses.

It recognises that events can only be identified, managed, and learned from when individuals do not fear retribution for mistakes, and sets what organisations and individuals throughout the health and care sector must do to promote and sustain this culture.

[6] NHS England (2024), A just culture guide for information governance and cyber security

3

Accountability

Accountability overview

Cyber risks at all levels of government must be actively owned and effectively managed, with those responsible held to account for effective management. This strand sets out responsibilities and accountability mechanisms to ensure they are met.

The objectives of the Accountability strand are:

Better visibility of cyber risk: increase visibility of government-wide cyber risks through accountability mechanisms and reporting.

Addressing severe and complex risks: establish central accountability for risks that departments or organisations cannot reasonably be expected to manage.

What needs to change?

Current accountability structures have failed to achieve the right level of resilience. Responsibilities for cyber risks are unclear at all levels of government, including across the supply chain. Leaders lack visibility and understanding of the risk and resilience levels within their purview, and the actual and potential impact on business delivery and critical services.

The government needs to reset its relationship with cyber risk by ensuring that it is visible, understood, owned and actively managed.

Addressing this challenge

We will set clear expectations and direction for the management of cyber risk at all levels of government. Risk owners will be held accountable for appropriate oversight and management of cyber risk. Clear risk appetites will be set at all levels, with performance monitored and assured.

Who will be responsible for what

Departments will:

- understand, manage and report against the cyber risks of their department, ALBs, and wider public sector in alignment with government-wide risk appetites and direction
- meet specified Accounting Officer (AO) responsibilities through establishing roles and responsibilities, governance structures, strategies, plans and processes to support accountability and risk management
- apply mechanisms to ensure suppliers appropriately manage government risks

ALBs and wider public sector organisations will:

- understand, manage and report against cyber risk in alignment with government-wide and LGD risk appetites and direction
- apply mechanisms to ensure suppliers appropriately manage government risk

The Government Cyber Unit will:

- understand and manage government-wide risk on behalf of Government Technology Risk Owner through mandatory policy and assurance against requirements
- provide departments with specific direction and practical support on how to manage their risk within central and local appetites
- engage strategic suppliers to ensure resilience outcomes are met and standards raised

NCSC will:

- provide authoritative technical advice and assessment on management of risk and advise the Government Cyber Unit on setting policies, standards, and baseline appetites

Suppliers will:

- understand and proactively manage risk in alignment with direction and expectations set out by their contracting authorities or, for strategic suppliers, in line with strategic partnerships expectations

Cyber risk

Cyber risks facing the government and the public sector reflect the scale and complexity of government itself. Many risks are government-wide because they could affect multiple organisations, systems or services across the public sector. These risks must be managed to prevent business impacts across areas or the emergence of national security issues.

Managing cyber security and resilience across such a wide landscape of public bodies and supply chains is a major challenge, particularly when determining who should be responsible for, and involved in, the management of these risks.

Risk categorisation

There are many different cyber risks that can disrupt the delivery of public services. Some have common root causes or relate to common issues, and some have far reaching impact across the public sector digital estate and government organisations cannot fully address these issues in isolation.

To date we have not adequately identified and addressed government-wide risks, instead relying on risk management at an organisational level. To rectify this and to ensure risks are owned and managed appropriately, we have defined **government-wide** cyber risks, owned and managed centrally by the Government Cyber Unit and **organisational** cyber risks, owned and managed locally by individual organisations.

Building on the definitions in Government Functional Standard 007: Security, we outline these risk categories at a high level on the following page.[7] The examples are indicative, not exhaustive. Organisations should assess their own risks, vulnerabilities and impacts.

As outlined in **Chapter 2: Approach**, national security is a reserved matter, but devolved governments will seek to secure the cyber security of devolved public services for which they have oversight.

The UK Government owns UK-wide cyber risks in reserved areas, including heightened severity and incidents occurring in devolved nations that have wider implications for the rest of the UK e.g. common dependencies or nation state targeting. Both UK and devolved governments will work together in response to these cyber risks and, where practicable, agree their management.

Cyber risk ownership will be transferred between governments where agreed. Pre-existing arrangements for national security risks and issues will continue to apply. Where UK Government owns risks in reserved areas which affect devolved nations, these will be managed in collaboration with the relevant devolved governments in line with the Defend as One principle.

[7] Government Functional Standard GovS 007: Security

Category	Government-wide risk (Central risk)	Organisational risk (Local risk)
Definition	Risks with severity/complexity that would be unmanageable by a single organisation.	Risks that primarily affect an individual organisation, and should be managed by that organisation.
Examples	Advanced, persistent threat targeting such as nation state. Common weaknesses causing aggregate risk, such as a known vulnerability that could be exploited at scale. Common dependencies, such as technology platforms or major suppliers. Risks created by widespread adoption of novel technologies, such as generative AI.	Moderate capability targeting Insider threat, data breaches Technology misconfigurations.
Ownership	Government Technology Risk Owner.	Departmental Accounting Officer.
Management	The Government Cyber Unit will actively manage these risks by directing cross-government activity and delivering support and services against centrally set baselines for across government cyber risk.	Departments, led by CISO and CDIO or equivalents, will manage these risks, enabled by Government Cyber Unit support, including direction and support for locally defined risk baselines in line with central minimums. Local risk management will include oversight and assurance of risks held by connected ALBs, public sectors, and supply chains.

Government-wide cyber risk

Government-wide cyber risk ownership

Government-wide cyber risk will be owned by the DSIT Permanent Secretary as Government Technology Risk Owner. The Government Cyber Unit will manage this risk on behalf of the Government Technology Risk Owner (GTRO).

Government-wide cyber risk governance

Organisational risk, issues and incidents will be reported to the Government Cyber Unit for central oversight and management of government-wide risk. Reporting will enable prioritisation, escalation and decision making on risks to improve resilience across government.

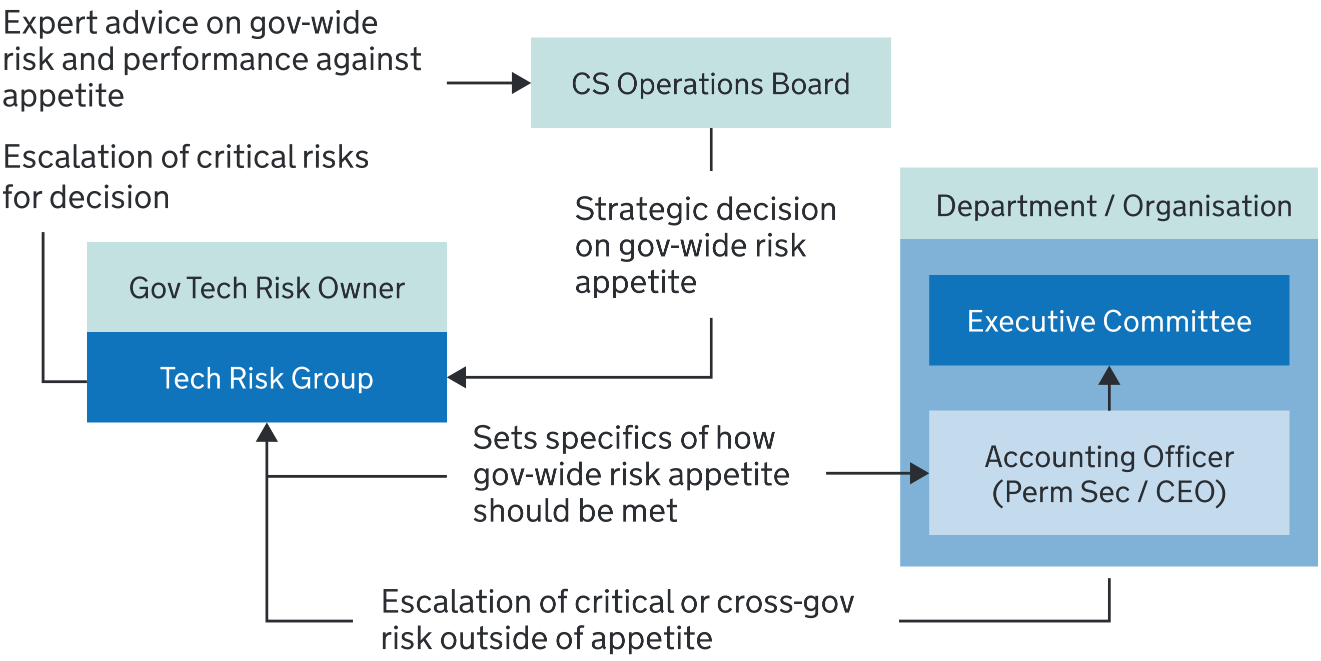
To support leadership, oversight and management of risks including advice and decision making, the GTRO will chair the Government Technology Risk Group (TRG).

The TRG will discuss aggregate risk and risk priorities from across government. It will generate recommendations and advice for the Civil Service Operations Board to manage government-wide cyber risk and support central decision making. It will provide an escalation route for cyber risks outside of appetite, and will hold Accounting Officers to account for appropriate management of organisational cyber risk.

Government-wide cyber risk appetite

The TRG will support the Civil Service Operations Board to set a government-wide cyber risk appetite and take action to identify and address cross-government risks. In support of this, the Government Cyber Unit will set direction and mandatory policy, assure against requirements, and provide departments with support and services to assist the management of local risk.

Departments and organisations not managing their own, ALB, or wider public sector cyber risks appropriately will be held to account by the TRG, with the Civil Service Operations Board facilitating further decision making and escalation when required.


Expert advice on gov-wide risk and performance against appetite
CS Operations Board
Escalation of critical risks for decision
Strategic decision on gov-wide risk appetite
Department / Organisation
Gov Tech Risk Owner
Tech Risk Group
Executive Committee
Sets specifics of how gov-wide risk appetite should be met
Accounting Officer (Perm Sec / CEO)
Escalation of critical or cross-gov risk outside of appetite

Data reported on risk and assurance, including information from GovAssure, will be assessed by the Data & Insights function, with prioritised and critical risks escalated to the TRG.

Organisational cyber risk

Organisational cyber risk ownership

The Accounting Officer is the senior official (Permanent Secretary or CEO) with overall accountability for an organisation. This includes personal accountability for the cyber risk of that organisation.

For LGDs, that accountability also extends to the ALBs and sectors which fall under their financial responsibility. For all government organisations, it extends to appropriate assurance of the cyber security and resilience of their suppliers.

Organisational cyber risk governance

The Government Cyber Unit will develop stronger channels for visibility and escalation of cyber risks to take action where government-wide cyber risk is generated. The TRG will hold those responsible for risk management in organisations and departments to account.

To discharge their accountability effectively, Accounting Officers will need to be supported by board members and senior management with sufficient understanding of cyber risk to effectively manage the risks. To support Accounting Officers to meet their accountability, specific responsibilities have been defined below.

Accounting Officer responsibilities:

- set cyber risk strategy including risk appetite and activities aligned to business covering department, ALBs, public sector, and supply chain, including ensuring that controls to remain within risk appetite are implemented and effective
- appoint an informed board member with expertise in cyber security and resilience, who understands risks to business objectives and the central risk strategy and appetite
- appoint a senior, capable individual with authority to manage organisation-wide cyber security (referred here as ‘Chief Information Security Officer’, CISO) and digital resilience (CISO or digital resilience equivalent)
- appoint a senior, capable individual with authority for organisation-wide digital and information technology (referred here as ‘Chief Digital and Information Officer’, CDIO)
- ensure escalation of risks outside cross-government risk appetite to Government Technology Risk Owner
- ensure routine reporting to departmental board from CISO and CDIO on the current state and progress of cyber risk across the department, ALBs, public sector, and supply chain

Organisational cyber risk appetite

Government organisations will set their own organisational cyber risk appetites, within government-wide cyber risk appetite. LGDs should set cyber risk appetites for their ALBs and/or public sectors to operate within. Organisational cyber risk appetites and strategies should reflect the organisation’s context and business objectives. The Government Cyber Unit will support government organisations to understand and meet their responsibilities.

Lead government department model

Lead government department (LGD) model

LGDs are responsible for the oversight of Arm's Length Bodies (ALBs) and other wider public sector organisations. This includes accountability for the cyber security and resilience of these organisations.

Arm's Length Bodies (ALBs)

The 2024 Government Security Policy: Security Functional Accountability set out LGD accountability for ALB cyber security and resilience, which led to closer engagement from LGDs on the security oversight of their ALBs.[8]

We are building on this by further defining the responsibilities of LGDs towards their ALBs, with a focus on stronger engagement and assurance of their cyber risk.

LGDs accountable for ALBs cyber responsibilities:

- account for and report on ALBs' cyber risk along with their own, using the Cyber Assessment Framework (CAF) outcomes and appropriate CAF profiles for cyber security and resilience
- ensure that ALBs manage their cyber risk within applicable appetites and escalate government-wide risks to Government Technology Risk Owner via the Government Cyber Unit

Wider Public Sector

Some departments have LGD accountability for parts of the wider public sector, for instance the education sector or local government.

Although individual organisations remain responsible for their own cyber security and resilience and may have a degree of autonomy or independence, LGDs are accountable for sector-wide cyber security and resilience, including setting and ensuring compliance with appropriate standards. A step-change is required in how wider public sector risk is managed.

[8] Government Security Policy: Security Functional Accountability 2024

LGDs accountable for wider public sector cyber responsibilities:

- account for and report on sector-wide cyber risk along with their own, using CAF outcomes and appropriate CAF profiles for cyber security and resilience
- ensure that sector-wide cyber risk is managed and government-wide cyber risks are escalated to Government Technology Risk Owner via the Government Cyber Unit.
- set a sector-wide cyber risk appetite and assess performance against it
- develop appropriate mechanisms for mandation, audit and review across sector to ensure organisations can be held to account for organisational cyber risk management
- collaborate with other LGDs to minimise duplicative cyber risk reporting burdens on wider public sector organisations

Suppliers

All organisations must also assure the cyber security and resilience of their supply chain.

Organisational responsibilities for suppliers:

- government organisations are responsible for applying appropriate mechanisms (including good procurement practices, contractual security and resilience terms and audit and review processes) to ensure that supply chain organisations understand their accountability and responsibility for government cyber security and resilience

Priority next steps

Building

Accountability priorities for Delivery Phase 1: Building the Model

The Government Cyber Unit will:

- better understand and manage government-wide cyber risk on behalf of the Government Technology Risk Owner by establishing new risk management roles, structures, processes and governance
- set direction and develop practical support for local cyber risk management
- engage strategic suppliers to ensure resilience outcomes are met and standards raised

Departments, ALBs, wider public sector organisations and suppliers, will:

- better understand, manage and report cyber risk of their department, ALBs, and wider public sector in alignment with government-wide risk processes
- consider appropriate mechanisms to ensure suppliers appropriately manage government cyber risk

For further information on implementation see **Chapter 9: Implementation**.

4

Support

Support overview

Government organisations do not have access to the capability, skills and capacity needed to meet their cyber security and resilience responsibilities. This strand sets out how support will be provided, prioritised, and accessed to bridge this gap.

The objectives of the Support strand are:

Increased UK Government cyber security and resilience: common support enables government and public sector organisations to implement requirements more quickly and easily.

Improved management of severe and complex risk: targeted support for government organisations to address the most critical cross-government risks.

What needs to change?

Government organisations frequently tackle the same challenges in isolation, leading to significant variance in implementation, duplicated effort, and increased costs. Many struggle to meet their cyber security and resilience responsibilities due to lacking the specialist capability, skills and capacity needed to implement improvements. Some struggle to understand and access existing support.

Addressing this challenge

Building on improved visibility and accountability for risk, the Government Cyber Unit will lead collective action with and across government organisations to put in place shared solutions to common challenges.

We will establish a partnering team to proactively harness and share government's collective knowledge, and develop strategic partnerships with suppliers which will position us to better leverage government's scale.

Drawing on good practice from industry and internationally we will deliver government-wide support. This will be based on risk, need, cost effectiveness and overall benefit; including technical advice and guidance, products and change programmes, which will be complemented by services and skills outlined in **Chapter 5: Services** and **Chapter 7: Skills**.

Who will be responsible for what

Departments will:

- access and adapt central support as necessary to understand their gaps and meet their cyber security and resilience responsibilities
- provide and/or sponsor the provision of support to their ALBs and public sector organisations

ALBs and Wider Public Sector will:

- access and adapt support from their LGD and/or the Government Cyber Unit as necessary to meet their cyber security and resilience responsibilities

The Government Cyber Unit will:

- establish a partnering function to help government organisations understand and access support
- prioritise and deliver government wide support to enable government organisations to meet their cyber security and resilience responsibilities
- understand demand for support, and prioritise government-wide provision

NCSC will:

- provide expert technical advice to inform coordinated guidance, products and advice
- provide support themselves where they are best placed to do so

Suppliers will:

- work with contracting authorities to optimise value for the government from use of technology solutions or, for strategic suppliers, with the Government Cyber Unit through strategic partnerships

Support offer

The support offered to government organisations will help them to meet the responsibilities outlined in **Chapter 3: Accountability**. We will deliver two broad categories of support:

Common support: Guidance and products available to government organisations; drawing on best practice and industry expertise and driving progress on common outcomes.

Targeted support: Technical advice and hands-on delivery support, tailored specifically to an individual government organisation.

Common support

Sharing approaches and lessons learnt, will reduce duplication or inconsistency between organisations. This will build on our existing offer of readily available products that make it easier for government organisations to address common challenges more efficiently.

Common support will be aligned to NCSC advice and will be made as widely available as possible including on security.gov.uk. Examples include:

- leading change programmes
- providing technical advice and guidance on common and future challenges, such as the transition to post-quantum cryptography
- CAF-aligned control libraries
- more standardised security architectures

We will develop strategic frameworks such as supplier partnerships and commercial frameworks.

Most support products will be optional and it will be the choice of the organisation to adopt and adapt appropriately to their requirements, but some may be mandated.

Common support offering: secure cloud application configurations

Best practice advice will be provided on security controls for cloud environment productivity tools used in UK Government, in line with policy and NCSC advice. The guidance will enable government organisations to implement appropriately secure configuration of tools and reduce risk.

Targeted support

Advice or delivery focused on individual or small groups of government organisations and tailored to their specific environment and needs.

Targeted support could include deploying technical experts to assist in the remediation of identified issues, including where they do not currently have access to the capability, skills and capacity to do so. This could include addressing the challenges and risks of common technologies, as well as those faced when adopting novel technologies, such as generative AI.

Targeted support will be prioritised on a need, risk, cost effectiveness and benefits basis.

The Government Cyber Unit will engage with departments. Departments are expected to either provide required support to their ALBs and wider public sector organisations themselves, or sponsor the provision of Government Cyber Unit support where appropriate.

Targeted support offering: cyber uplift team

The cyber uplift team are technical experts deployed into a government organisation to remediate identified vulnerabilities. These would be tactical deployments executed in collaboration with the organisation, who would retain responsibility for the remediation.

Following a successful 2024/25 pilot, the Government Cyber Unit will scale up this offering into a live service.

Support access

Government organisations are not currently able to access the support they need. Where central support is provided, the complex landscape means it is often not used by the lower maturity organisations who need it most, as they struggle to identify what is available and the value it could add.

Improving access

The Government Cyber Unit will make it easier for government organisations to find and access cyber security and resilience support in one place, whether it is provided by the Government Cyber Unit, NCSC, third party providers, or others. Support to ALBs and wider public sector organisations may be provided by their LGD or the LGD may sponsor support from the Government Cyber Unit.

Partnering

The Government Cyber Unit will establish a Partnering function that will direct government organisations to the support offerings that are most likely to enable them to make improvements, wherever those offerings are delivered from.

The Government Cyber Unit's Partnering function will also ensure government organisations are able to take up the appropriate support. It will act as the primary interface between the Government Cyber Unit and its stakeholders, concentrating on relationship building, understanding needs and priorities and driving collaboration.

Government and public sector organisations will access support to:

- **identify and understand gaps:** build an understanding of where their cyber security and resilience falls short of their responsibilities, and develop prioritised improvement plans to fill these gaps
- **implement improvements:** deliver changes identified in prioritised improvement plans, for example by accessing hands-on technical support from the Government Cyber Unit or NCSC, as appropriate

Responding to need

The Government Cyber Unit will understand the need and provision available and monitor what support is most frequently needed and accessed. Where there is a shortfall in the support available to government organisations, the Government Cyber Unit will take steps to reduce this gap, which may include commissioning new support, funding the expansion of existing support, directly providing new and/or expanded support, or facilitating development of new commercial frameworks.

Government organisations will remain responsible for accessing support as needed to meet their cyber security and resilience responsibilities.

Prioritisation

Increased visibility will enable the Government Cyber Unit to prioritise and target support where it will have the greatest impact. In alignment with strategic goals of improving government-wide resilience and managing severe and complex risks.

The Government Cyber Unit will prioritise support on a risk, need, cost and benefit basis.

The Government Cyber Unit's primary customer group will be departments, with departments expected to either provide required support to their ALBs and wider public sector organisations themselves, or sponsor the provision of Government Cyber Unit support where appropriate.

Devolved governments and public sector organisations will be included in this prioritisation in the same way as all other UK Government organisations. That is, central UK Government support will be prioritised on a risk basis regardless of where they are in the UK.

Devolved governments will work collaboratively with UK Government to ensure public sector organisations access appropriate support.

Priority next steps

Building

Support priorities for Delivery Phase 1: Building the Model

The Government Cyber Unit will:

- establish a partnering function, building CISO community and engagement model to drive collaboration on shared outcomes
- determine the delivery model, community of expertise and prioritised requirements to establish a technical advisory function
- improve existing support through expansion of cyber uplift, a roadmap for transitioning to post-quantum cryptography, and strategic partnership agreements with suppliers

Departments, ALBs and wider public sector organisations and suppliers will:

- consider available support and identify potential improvements coordinating with ALBs and wider public sector organisations

For further information on implementation see **Chapter 9: Implementation**.

5

Services

Services overview

Government organisations face cyber security and resilience challenges that could be addressed at scale, there are few services that exist to enable this and those that do are not well understood or accessed. This chapter outlines how scaled cyber services will be developed, delivered, and accessed to address this.

The core objectives of the Services strand are:

Increased visibility of risks across government: prioritise the development of new central services which can transform visibility of government-level risk at scale.

Increased HMG cyber security and digital resilience: bring central service provision and access into one place via the establishment of central service coordination.

Improved responsiveness to fast moving events: improve capabilities to detect threats and manage vulnerabilities at scale.

What needs to change?

While examples such as NCSC's Protective Domain Name Service (PDNS) and the Government Cyber Unit's Vulnerability Monitoring Service demonstrate that cyber risks can be addressed at scale, barriers mean that the provision and adoption of services are not sufficient, especially for less mature organisations.

There is no strategic approach to the development of new cyber services at scale for government organisations. This results in undetected and unmanaged government-wide cyber risks.

Addressing this challenge

We will identify where government-wide risks could be addressed, or response improved, by services at scale.

Where services are available, we will ensure that they are readily accessible to those who need them most, that they deliver clear benefits, and we will support their adoption.

Where there are gaps in provision, we will prioritise and commission or deliver them once and well, aligning to the Government Digital Service (GDS) design principles and service standard.

Who will be responsible for what

Departments will:

- identify and access relevant cyber services to meet their cyber security and resilience responsibilities
- provide services where agreed with the Government Cyber Unit to be best placed to do so
- coordinate and sponsor priority needs of their ALBs and wider public sector organisations

ALBs and wider public sector will:

- identify and access relevant services to meet their cyber security and resilience responsibilities

The Government Cyber Unit will:

- coordinate a coherent central service portfolio to deliver impact on strategic priorities, including commissioning and decommissioning services, designing delivery and funding models, and setting a framework of mandation requirements or incentives to drive uptake
- innovate and deliver scaled services, either directly or via partners
- ensure that centrally provided services are easily accessible to target organisations

NCSC will:

- inform investment decisions made by the Government Cyber Unit service via specialist NCSC input on service standards and good practice
- innovate to support the creation of new and enhanced services to address cyber risks
- provide services where they are uniquely placed to do so and advise on the sustainability of these

Suppliers will:

- work with the Government Cyber Unit and government organisations to provide services at scale

Service coordination

The Government Cyber Unit will take a strategic approach to the provision of services at scale in order to meet its objectives. Services may be delivered by different organisations, but the Government Cyber Unit will maintain a comprehensive view of their overall effectiveness and accessibility.

Gap analysis

The Government Cyber Unit will work with government organisations to build and maintain an understanding of their service needs according to the risks they manage. The Government Cyber Unit will compare their requirement with the availability of services, taking into account provision by both public and private sector sources.

Service coordination

Through a new 'Service Coordination' function, the Government Cyber Unit will play a strengthened role in ensuring that scaled services collectively meet organisational needs, and can be accessed in the right place at the right time, and are delivering value as measured by agreed key performance indicators.

Where scaled services that could address the identified gaps already exist and demonstrate value, the Government Cyber Unit will explore how their effectiveness and uptake can be increased, as outlined in the 'improving access' and 'uptake approach' sections later in this chapter.

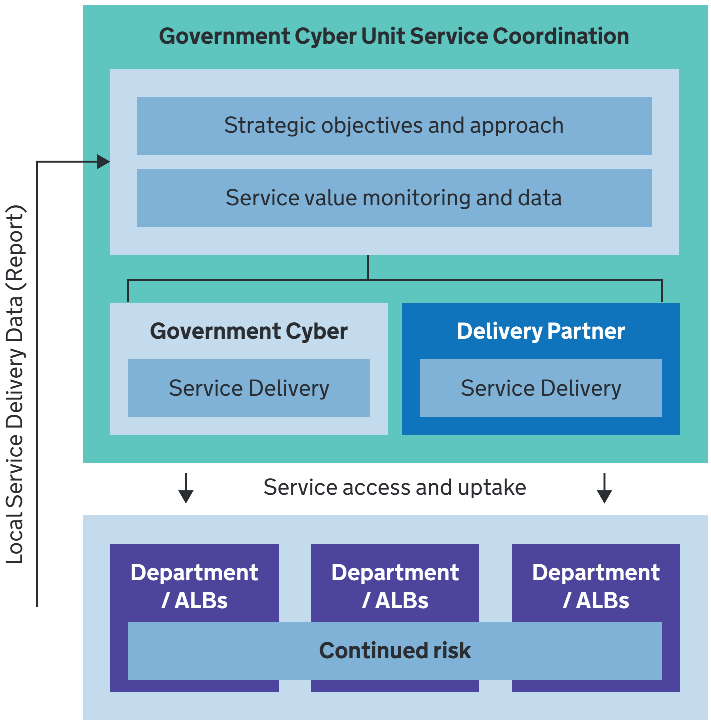
Where services fail to deliver value or to diminishing returns, the Government Cyber Unit will consider options for scaling down or decommissioning.

Where new opportunities are identified to address gaps through scaled services, the Government Cyber Unit will work with partners to test and later in this chapter.

Delivery model

Under our vision for a single consistent approach, scaled services may be delivered by different partners. This could include the Government Cyber Unit or GC3, NCSC, private organisations, or other government organisations.

The Government Cyber Unit will ensure that accessing these services is a seamless end-to-end experience, regardless of who delivers them. This is outlined in more detail in the 'improving access' section of this chapter.


Government Cyber Unit Service Coordination
Strategic objectives and approach
Service value monitoring and data
Government Cyber
Service Delivery
Delivery Partner
Service Delivery
Service access and uptake
Department / ALBs
Department / ALBs
Department / ALBs
Continued risk
Local Service Delivery Data (Report)

Service access

Existing cyber security and resilience scaled services are typically deployed in a complex landscape that makes it more challenging for government organisations to access the right service at the right time.

Improving access

The Government Cyber Unit will make it easier for government organisations to find and access cyber security and resilience services in one place. This will include maintaining a service finder that makes it easier for government organisations to find and access what they need by bringing together information about services available to organisations, what benefits can be expected from their use, what costs or resources are required and how to access them.

Although services will be delivered from multiple partners, the Government Cyber Unit will oversee a seamless end-to-end experience in which government organisations can go to one place to understand what services are available to them, and be supported to adopt them. This will include clear information on responsibilities between service providers and recipient organisations.

Uptake approach

The Government Cyber Unit will form a view of which services should be prioritised for uptake. The Government Cyber Unit's Partnering function, outlined in **Chapter 4: Support**, will facilitate take-up of these services by relevant organisations.

Funding models and incentives will be developed to encourage uptake by government organisations, for instance, free or subsidised access to services.

Where demand exceeds availability, the Government Cyber Unit may need to prioritise access and where appropriate, work with partners to grow capacity.

Where scaled services have proven their effectiveness in achieving strategic goals, the Government Cyber Unit may use the structures outlined in **Chapter 3: Accountability** to make use of these services opt-out only, or even mandated for some or all government organisations. This may be done to ensure that organisations collectively meet their cyber security and resilience responsibilities, or may be primarily focused on achieving government-wide cyber security and resilience goals, such as increased government-wide visibility.

Prioritisation

Given resource limitations, although there will be some exceptions, the Government Cyber Unit will primarily prioritise new services to departments. Departments will be expected to provide required services to their ALBs and wider public sector organisations themselves, or sponsor the provision of Government Cyber Unit services where appropriate.

Devolved governments and public sector organisations will be included in this prioritisation in the same way as all other UK Government organisations. That is, central UK Government support will be prioritised on a risk basis regardless of where they are in the UK. Devolved governments will work collaboratively with UK Government to ensure public sector organisations access appropriate support.

Protective Domain Name Service (PDNS)

One of NCSC's widely deployed Active Cyber Defence capabilities. PDNS prevents access to domains known to be malicious, and provides support to resolve issues. It is mandated for use by departments but is available to other government organisations.

The data is also used to inform and support government-wide cyber incident response functions in the event of a cyber attack.

Service development

The Service Coordination function will determine the need for and also commission new, scaled cyber security and resilience services in government and the public sector.

Service discovery

Informed by ongoing analysis of the gap and feedback from government organisations, the Government Cyber Unit will continually reassess where scaled services could achieve strategic goals, such as addressing government-wide cyber risks or objectives. For example, this might be to address an aggregated cyber risk arising from common weaknesses, or to promote increased visibility of cyber risks across government.

Service innovation

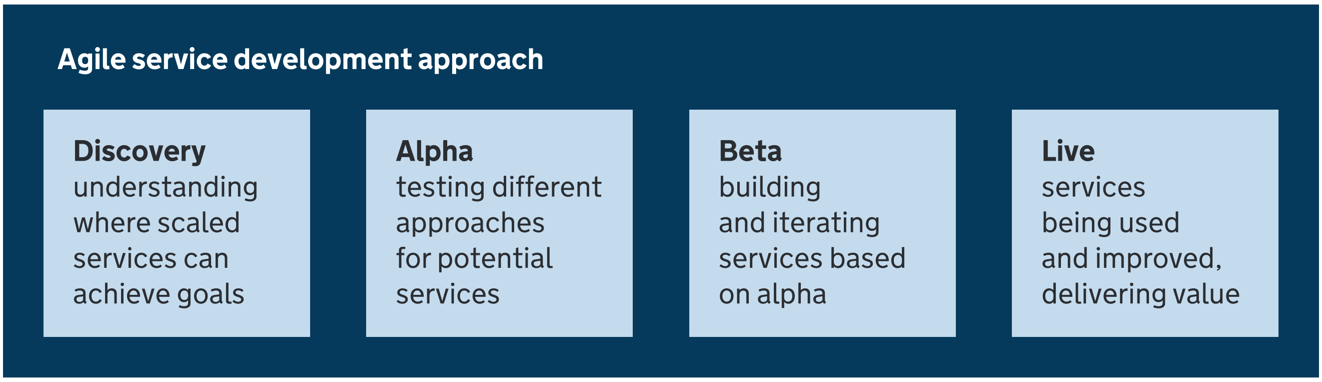
When an opportunity to address cyber security and resilience challenges at scale is identified, our approach to new services will align to the GDS service standard and design principles. The Government Cyber Unit will work with organisations to understand their needs, provide a joined up experience and use agile ways of working to ensure services innovate and improve as requirements and priorities evolve.

Innovation will involve determining if a service could exist to solve that problem and testing before moving to live delivery. As part of this, the Government Cyber Unit innovate new services to meet the identified opportunity, working with NCSC or drawing from private and government organisations with relevant skills and experience.

Service delivery

For those services that are successfully proven in testing, the Government Cyber Unit will make an assessment of which organisation is best placed to deliver it, considering the different advantages and expertise that may enable them to be effective. This could be NCSC, a private provider, or a government organisation. The Government Cyber Unit may also choose to deliver scaled services itself where it is best placed to do so.

As part of the design, delivery and management of new services, the Government Cyber Unit will clearly articulate the benefits, intended impact and key performance indicators. Delivery partners will be accountable to the Service Coordination function for their service delivery through a service level agreement.



Agile service development approach

Discovery understanding where scaled services can achieve goals

Alpha testing different approaches for potential services

Beta building and iterating services based on alpha

Live services being used and improved, delivering value

Priority next steps

Building

Services: priorities for Delivery Phase 1: Building the Model

The Government Cyber Unit will:

- scale existing proven services and develop a service finder to facilitate access
- establish a service coordination function and service delivery model and function to enable the future innovation of new services
- build an initial understanding of gaps in provision and access requirements

Departments, ALBs and wider public sector organisations and suppliers will:

- consider available services to adopt and identify potential improvements, coordinating with ALBs and wider public sector organisations

For further information on implementation see **Chapter 9: Implementation**.

6

Response and Recovery

Response and recovery overview

As well as proactively reducing risk, government must be able to quickly and effectively manage incidents when they occur. This strand sets out the responsibilities for cyber security and resilience incidents at all levels, that will enable us to collectively minimise their impact.

The objectives of the Response and Recovery strand are:

Improved responsiveness to fast moving events: help government and public sector better respond to and recover from major incidents through clearer responsibilities and improved capabilities at all levels.

Increased visibility of risks across government: harness incident and vulnerability data at scale to better understand systemic risks, strengthen defences and improve resilience outcomes.

What needs to change?

Our adversaries see government as a single target, yet its constituent parts typically respond to threats, vulnerabilities and incidents in silos. Effort is duplicated and uncoordinated, and intelligence and insights are not shared; this reduces the effectiveness and efficiency of our response both now and in future.

Addressing this challenge

To address this we will significantly invest in the Government Cyber Coordination Centre (GC3) across the full lifecycle of: prepare; detect; respond and recover; and, learn and improve.

We will build on existing successes such as the Vulnerability Reporting Service and deliver more Security Operations services from the centre.

We will unlock more value from the work already being delivered across government and better enable communication and collaboration between Security Operations teams. We will improve and expand coordination capabilities to ensure an effective cross-government response where one is needed.

Who will be responsible for what

Departments will:

- manage organisational cyber incidents across the full lifecycle, drawing on support where appropriate
- ensure ALBs and sectors for which they have responsibility have suitable cyber incident response and recovery arrangements in place for the full lifecycle

ALBs and Wider Public Sector will:

- manage organisational cyber incidents across the full lifecycle, drawing on support where appropriate

The Government Cyber Unit will:

- set the framework for and coordinate cross-government cyber incident response and recovery across the full lifecycle through the GC3, in partnership with NCSC

NCSC will:

- continue to lead national level cyber incident response and related public messaging in collaboration with Cabinet Office, involving the Government Cyber Unit and GC3 where government is impacted
- work with the Government Cyber Unit and GC3 on development of technical advice and guidance, provide intelligence-led threat assessment products, and industry accreditation schemes
- coordinate cooperation with cyber security industry partners and international cyber partners

Suppliers will:

- proactively report and cooperate on cyber incident response and recovery impacting government organisations
- engage directly with the Government Cyber Unit and GC3 on government-wide incidents, where appropriate particularly if a strategic supplier

Prepare

Preparation is the foundational step in an effective response to cyber incidents. However, we know that government organisations consistently struggle to develop effective response plans, and to embed these through exercising. We will work with departments to address this, using the structures and levers outlined in this document.

We will similarly work to ensure that cross-government response plans, structures and capabilities are in-place and embedded, and to ensure that we understand how and when to activate national- level plans, structures and capabilities.

Organisational

Organisations are responsible for ensuring they are prepared to rapidly, effectively and expertly manage potential cyber and resilience issues impacting their organisation, as well as ALBs and public sectors for which they are responsible. This includes developing, exercising and continually improving robust plans at every level, covering likely and high-risk scenarios.

The Government Cyber Unit will hold departments to account for ensuring that they and their ALBs and sectors are adequately prepared for incidents, in line with broader accountability mechanisms set out in **Chapter 3: Accountability**.

Government-wide

The Government Cyber Unit will support government departments in effectively preparing for potential cyber and resilience incidents, primarily through scalable central services such as guidance, templates, and exercising packs, as well as specialist central capabilities.

GC3 will also work to ensure that the relevant structures and capabilities are prepared to deliver a cross-government response where it is required. This will include publishing and exercising cross-government plans; for example, the Government Cyber Incident Response Plan (G-CIRP) which defines the overarching structures, and roles and responsibilities, for responding to cross-government cyber incidents.

Under the blueprint for modern digital government, DSIT will develop a cross-public sector view of technical resilience.

Exercising for Government

GC3 will build a capability to support government organisations in carrying out their own exercises through centrally-developed methodologies, scenarios and exercise packs, and through providing hands-on support.

National

The NCSC and Cabinet Office are jointly responsible for publishing the National Cyber Incident Management Framework (NCIMF), which sets out the structure and approach for the national response to cyber incidents. This is embedded through NCSC's national exercising strategy and Cabinet Office's National Exercising programme. NCSC also provides a range of guidance on preparing for incidents, including developing and exercising response plans, and assure exercising providers through the Cyber Incident Exercising (CIE) scheme.

Detect

Rapid detection, triage and investigation of cyber threats and potential resilience issues is key to reducing their impact, as is the rapid sharing of intelligence across organisations. However, we know that these capabilities are often both immature and siloed; this hinders the response at every level, and can unnecessarily exacerbate the impact of incidents.

To resolve this, we will create clear structures for detection across government and the public sector and provide central services which enable foundational capabilities and collaboration between organisations, and work with NCSC to address systemic challenges.

Organisational

Organisations are responsible for detecting, triaging and investigating potential cyber and resilience issues impacting their services, systems and data, and activating the appropriate response and recovery plans.

The Government Cyber Unit will hold departments to account for ensuring that they and their ALBs and sectors have adequate capabilities, in line with broader accountability mechanisms set out in **Chapter 3: Accountability**.

Sector-wide detection

LGDs are encouraged to explore opportunities for delivering detection at scale across the ALBs and public sector organisations they are responsible for (drawing on existing successes such as NHS England’s highly scalable monitoring of NHS Microsoft 365 instances).

This might include passing through wider government and national capabilities, augmenting these for the context of the specific constituency, or as a last resort building bespoke capabilities.

Government-wide

The Government Cyber Unit will create clear structures for detection across government and the public sector, better enabling collaboration and interoperability.

The Government Cyber Unit will provide central services that enable foundational capabilities across organisations, local effort to be focused on where it can deliver the most value, and collaboration between organisations. As well as improving capabilities and reducing risk within organisations, this will enable better central understanding of risk across government and ensure we are focusing investment where it is most needed.

Detection for Government

GC3 will build a centralised library of intelligence-driven detection content that departments can consume to detect threats for common platforms. This will help departments to meet minimum standards, and reduce duplication of effort. More mature organisations will be able to augment the library with rules specific to their technology and risks, and to contribute rules so others can benefit.

National

NCSC will publish and deliver a **national detect strategy**, which will set out the national approach for detection of adversarial activity, intrusion and vulnerability on key networks, better enable collaboration (for example, government's existing strategy to "defend as one") to address the systemic challenges which inhibit effective detection.

The Government Cyber Unit will work closely with NCSC to ensure the strategy addresses the UK Government and public sector challenges, and to apply the strategy through sector-specific initiatives such as Detection for Government.

Respond and recover

Increasing technical complexity, increasing integration of government services and IT, and an increasing cyber threat means that incidents require an increasingly complex and involved response.

Recovery can be even more complex, requiring sustained investment and effort long after the initial incident has left boardroom agendas. Therefore, while departments will remain responsible for managing incidents impacting their organisations, we will provide the central structures to enable coordination, collaboration and communication across impacted organisations, and maintain central capabilities that can be deployed to provide direct support where it is needed.

We will apply the principle of subsidiarity throughout, ensuring that decisions continue to be made at the lowest possible level while providing coordination at the highest necessary level.

Organisational

Government organisations affected by an incident, either directly or through their ALBs or sectors, are responsible for coordinating their response as guided by their incident response plans (and overarching plans such as the G-CIRP and NCIMF as required).

The Government Cyber Unit will hold departments to account for ensuring that they and their ALBs and sectors conduct this action, in line with broader accountability mechanisms set out in **Chapter 3: Accountability**.

Government-wide

GC3 will work with departments to ensure they are taking the right action during incidents in order to manage risk to their own organisations and wider government. Where incidents exceed the capabilities of individual departments to manage, GC3 will provide additional support, either centrally or by enabling mutual aid from other departments.

Where incidents have a cross-government impact, or otherwise require cross-government working, GC3 will provide the structures, processes, and where necessary coordination, to enable a cohesive and collaborative response.

Where government organisations cannot access the right expertise to support their investigation and response to a cyber incident, GC3 will provide a panel of centrally managed NCSC-accredited cyber incident response providers of last resort. GC3 may also deploy this capability to assure an organisation's response to an incident, and ensure that risk both to that organisation and wider government is being appropriately managed.

Retainer for Government

Where a cross-government response is required, GC3 will lead this while working closely with NCSC and wider colleagues across government, including GSG. The overarching structures, and roles and responsibilities, for cross-government response will be documented in the G-CIRP and a suite of supporting documentation.

National

In line with the structures and responsibilities already outlined in the National Cyber Incident Management Framework (NCIMF), the NCSC will coordinate the response to nationally significant cyber incidents, working closely with colleagues in Cabinet Office and wider government.

Similarly, DSIT will coordinate the response to national significant resilience incidents, again working closely with colleagues across government. Where necessary, the Cabinet Office will provide overarching whole-of-government crisis management through COBR.

Learn and improve

The lessons identified during incidents can prevent the repetition of past mistakes, improve preparedness, and reduce the impact of future incidents. However, to achieve this we must ensure that lessons are identified, prioritised, implemented, and embedded, as well as being shared to ensure that others can benefit from them.

We know that this rarely happens, and the lessons identified during incidents are often not fully recognised let alone exploited. We will fix this by creating the structures, capabilities, and most importantly culture, to enable effective lesson management across government during incidents.

Case study – Irish Health Service 2021 cyber attack[9]

When hit by a catastrophic cyber attack in 2021, the Irish Health Service Executive (HSE) adopted a principle of radical transparency. During the incident HSE provided regular, public updates as to the severity of the impact and their efforts to respond and recover.

Following the incident, HSE published a comprehensive, independent – and most importantly public – post-incident review which has been widely praised and proven invaluable for many organisations in planning their own response and recovery efforts.

Organisational

Government organisations are responsible for identifying, prioritising, implementing, and embedding lessons from incidents, and sharing them through a principle of radical transparency to ensure that others across government and the public can benefit from their experience.

The Government Cyber Unit will hold departments to account for ensuring that they and their ALBs and sectors conduct this action, in line with broader accountability mechanisms set out in **Chapter 3: Accountability**.

Government-wide

GC3 will identify lessons from cross-government incidents, enable the dissemination of relevant lessons across government (wherever they are identified), and directly apply lessons where they relate to GC3 capabilities.

The Government Cyber Unit will review lessons identified across government, and work with departments to apply these across government using the structures and levers outlined in this document.

Alongside reviews at the operational level, in line with Accounting Officer responsibilities outlined in **Chapter 3: Accountability**, GC3 will ensure that lessons are learned from cyber and digital resilience incidents at the highest level. GC3 will convene cross-government incident reviews at which Accounting Officers, and supporting roles, from organisations affected by incidents share lessons with their counterparts.

[9] Irish Health Service Cyber attack December 2021

National

Where incidents require a national response, post-incident reviews will be coordinated by the functions leading that response using their existing structures (e.g., NCSC through NCIMF, and Cabinet Office through the Amber Book).

Furthermore, the Cabinet Office, through the UK Resilience Academy, is responsible for embedding effective lesson management across government and the public sector by providing guidance and support.

Priority next steps

Building

Response and recovery priorities for Delivery Phase 1: Building the Model

The Government Cyber Unit will:

- publish the Government Cyber Incident Response Plan (G-CIRP) to provide the overarching framework, structure, roles and responsibilities for cyber incident response within government
- establish a clear mandate and structure for GC3 to direct response and recovery action across government and expand remit to cross-government digital resilience incidents
- improve existing support through enhanced threat and vulnerability notification services and a panel of NCSC-accredited cyber incident response "providers of last resort"
- pilot and define longer-term plans for services that enable government organisations to more effectively detect, triage and investigate cyber threats, including a central library of intelligence-driven detection content that departments can consume

Departments, ALBs and wider public sector organisations and suppliers will:

- update their response and recovery plans to align with the G-CIRP, and embed through exercising or testing
- review their capabilities and processes and identify potential improvements, coordinating with ALBs and wider public sector organisations

7

Skills

Skills overview

The demand for cyber security and resilience understanding and skills across government is growing faster than the supply of available talent. Leaders, functional professionals, and the wider workforce lack understanding of cyber risks and business impact. This chapter outlines the establishment of a dedicated Government Cyber Profession, which will attract, upskill, retain, and support government cyber professionals.

The core objectives of the Skills strand are:

Increased HMG cyber and digital resilience: attracting, upskilling, retaining and supporting cyber and digital resilience talent and making the public sector an attractive employer for professionals.

Improved management of severe and complex risks: transforming how government manages risk by improving awareness, understanding, activities and unlocking appropriate funding.

What needs to change?

The cyber skills gap is an industry-wide issue with approximately half of businesses (49%) and 58% of government organisations reporting a basic cyber skills gap resulting in vulnerable services and costly outsourcing.[10]

Specific public sector challenges include pay and inconsistent approaches to career development. Leaders and enabling professions also suffer from an insufficient understanding of cyber security and resilience, leading to de-prioritisation, underinvestment and inadequate security rigour in general business practices.

Addressing this challenge

The Government Cyber Profession will provide a government-wide approach in which the best talent is attracted and retained, and leadership and the workforce are upskilled and supported.

Who will be responsible for what

Departments will:

- recruit cyber and digital professionals through entry schemes and recruitment programmes
- upskill and retain staff through learning and development, career pathways, job opportunities, allowances, and competitive pay
- raise awareness of cyber security and resilience at leadership and board levels, embedding a strong security culture throughout their organisations

[10] Cyber security skills in the UK labour market 2025

ALBs and wider public sector organisations will:

- forecast and share local resourcing needs for cyber and digital resilience
- collaborate with LGDs to develop and implement resourcing plans, including shared resource models

The Government Cyber Unit will:

- establish and lead the first cross-government Cyber Profession, enabling better talent management and collaboration
- drive recruitment efforts to attract people into government with competitive total job offers and via centrally led schemes align public sector salaries with private sector benchmarks
- develop and deliver training to attract, reskill and upskill staff, leaders, and professionals across disciplines

NCSC will:

- support accreditation of cyber and digital professionals via the UK Cyber Security Council
- provide expert guidance to support the attraction, retention and development of a diverse technical workforce

Profession

The Government Cyber Unit, with NCSC support, will establish the Government Cyber Profession: the first dedicated government profession for cyber security and resilience, aligned to both the Government Security Profession and the Government Digital and Data Profession.

The profession will take a coordinated, government-wide approach to managing cyber talent that addresses structural skills challenges by taking advantage of being one of the UK's largest employers of cyber professionals, with a truly unique mission and set of opportunities. The profession will aim to make the government the best place to work for cyber professionals.

Head of Profession

The new profession will be led by a Head of Profession, this head will be responsible for championing the profession across government, ensuring its development, promoting best practices, and advocating for the appropriate role for the profession in improving public services.

All Chief Information Security Officers (CISOs) or equivalent across central government will have a dotted line to the Head of Profession, who will input into recruitment decisions, and provide coaching support and feedback on performance.

The Head of Profession will be supported in this role by heads of specialism that will play a similar function for specified cyber domains.

Skills Pipeline

The Government Cyber Profession will seek to address known structural issues in the recruitment and retention of cyber professionals, such as workforce shortages and skills gaps, through mechanisms including entry schemes, pay frameworks, job families, learning and development schemes, and career pathways.

The profession will manage and operate a **skills pipeline** across four stages:

1. **Attract:** bringing the best professionals to government and the public sector.
2. **Upskill:** ensuring all our professionals have the skills they need.
3. **Retain:** maintaining an attractive offer that prevents loss of the professionals we invest in.
4. **Support:** making government the best place to work on cyber security and resilience.

This four stage pipeline is further outlined in the following pages.

Cyber Resourcing Hub

To support the Head of Profession, The Government Cyber Unit will operate a **Cyber Resourcing Hub** for all cyber recruitment across departments, and will work with LGDs to ensure the right support for ALBs and wider public sector organisations.

The hub will support government organisations to make best use of the various tools at their disposal for effective recruitment and retention of cyber security and resilience professionals, such as pay uplifts and talent schemes.

Cyber Resourcing Hub

A central hub will provide job descriptions, vacancies, reserve lists, and tailored hiring advice for cyber security roles. It will support organisations by directing them to appropriate recruitment and retention mechanisms to achieve their goals, including talent schemes (including apprenticeships and specialist fast stream programmes), sharing resources, and pay uplifts.

Community

As well as more active, government-wide management of cyber talent, the profession will create a community and network based on support and sharing, helping cyber professionals across government connect, and share ideas and best practice.

Attract and upskill

Addressing the skills gap is vital to addressing technology threat and vulnerability. This operating model will set direction, coordination and acceleration of skills initiatives to boost government's technical ability and capacity.

Expanding on efforts to strengthen resilience through building a sustainable and diverse workforce, we aim to attract, upskill, retain and support individuals to ensure that there are people across government equipped to tackle cyber security risk and resilience now and in the future.

Attract

In order to attract the professionals needed into government, we need to build an appealing offer and recruit effectively. The Government Cyber Profession will set out and maintain a competitive **total employee offer**, that will make the government an attractive employer and career path for the best talent. The total employee offer will be more competitive with the private sector, as well as emphasising benefits where government typically out-competes the private sector such as pensions and flexible working.

The profession will also focus on establishing more effective entry routes to government cyber roles. This will include promoting better, and more consistent, use of education and early talent schemes, apprenticeships and fast stream programmes, as well as secondments and exchanges across government and private industry.

TechFirst

Government's technology skills package, investing £187m to bring digital skills and AI learning into classrooms to prepare citizens for careers of the future, including supporting 4,000 graduates, researchers and innovators in AI, cyber security and computer science through TechGrad, TechExper and TechLocal and TechYouth programmes.[11]

Through the Resourcing Hub, DSIT will also promote the use of more accessible and intuitive application processes for those applying from outside the civil service, as well as career switchers, and individuals from underrepresented groups such as individuals from ethnic minority backgrounds and women.

Upskill

As well as attracting the best professionals to government, we must foster an environment in which we make the most of the potential that already exists. This includes creating the right learning and development opportunities for existing cyber professionals, as well as creating opportunities for people without cyber backgrounds to develop expertise and make use of transferable and complementary skills. The profession will support the development of individuals and will set out appealing learning and development (L&D) opportunities for progression and career pathways.

The Resourcing Hub will support understanding and assessment of resources, with methodologies promoted for assessment of technical expertise of staff, using gap analysis and accreditation and certification of professionals.

[11] PM launches national skills drive to unlock opportunities for young people in tech

Retain and support

Retain

In order to keep the talented and skilled professionals in government, we need to build an attractive offer to retain individuals. As mentioned in 'Attract', the Government Cyber Profession will set out and maintain a competitive total employee offer which will establish the government as an attractive continued employer with satisfying career paths for talented individuals.

We want to draw on the uniqueness of public sector working, including the importance of delivering and supporting public services that facilitate the lives of our friends, family and communities and make real world impacts, driving growth but also protecting the services we all rely on to work and live.

The profession will create an environment for continuous development and collaboration, utilising the unique position of government and the public sector, as an employer with a wide landscape of policy areas and options with the ability to move across teams, policy areas and departments and work on mission focused work.

The profession will maintain and refresh the total employee offer of public sector working, to ensure pay, via pay frameworks, and other benefits (flexible working, pensions etc), remain competitive and can rival the private sector, so that talent is not lost to private industry.

Through the Resourcing Hub, The Government Cyber Unit will make use of the excellent partnerships with the UK Cyber Security Council and NCSC and others to support professionalisation of job titles and formal training, professionals certification and NCSC accreditation.

Support

To foster a positive cyber professional culture and ecosystem that helps people to deliver and thrive in cyber security and resilience, the profession will provide support and services that help people, teams, departments, professions and organisations.

It will develop targeted support packages to help leaders understand cyber and digital resilience, the importance of it and the impact on business and delivery, and how to use resources and skills to manage it. It will raise awareness of technology and resilience and the wider roles and responsibilities that connect to cyber and digital security.

The Resourcing Hub will drive recruitment and diversity and inclusion across government and the public sector. It will support organisations to better identify current and future skills gaps and target solutions to minimise use of contingent labour and fill gaps with diverse, new and existing resources. The hub will work towards options for a single employer model to set itself as the place for effective recruitment, upskilling and retention of technical and non-technical professionals.

Leadership and workforce

Cyber security and resilience is everyone's responsibility: all of us are affected by it and have a part to play in ensuring it enables business objectives. It is therefore vital that all roles have a working understanding of cyber risk and how it applies to their role. This is particularly important for leadership roles so that they can make informed cyber risk decisions, and for functional professionals such as Commercial, Finance, and HR, due to the cyber risk functional roles typically manage.

Leadership

An environment where cyber security and resilience is effectively managed is only possible when its importance is communicated from the top. As such, leaders including Accounting Officers, executive teams and board members, need to be informed and have a clear understanding of the risks facing their organisations and services, and manage them responsibly. Specific Accounting Officer responsibilities are set out in **Chapter 3: Accountability**.

The Government Cyber Unit will provide targeted support and learning on cyber security and resilience for leaders to enable them to better understand their responsibilities and how to meet them. This will be embedded into onboarding and ongoing development for these roles.

Functional professionals

To support and enable security and resilience through business functions, functional professionals need to build appropriate cyber considerations into business practices and processes. The Government Cyber Unit will provide support and training for functional professions tailored to their roles. This will be particularly important for Commercial and Finance professionals due to the high amount of cyber risk that is held in supply chains, and primarily managed through procurement and commercial activity.

L&D initiatives will be targeted to support supply chain security, supporting commercial and procurement professionals to embed appropriate cyber knowledge and understanding into processes to assure the cyber security and resilience of government suppliers.

Commercial Security College

Structured learning and development to support contracting authorities to embed appropriate security knowledge and understanding into their commercial approaches.

Everyone

To ensure effective security and build resilience, all staff need to have an awareness of security risks and issues and uphold department and organisation security policies.

The Government Cyber Unit will raise awareness and understanding of cyber security risks by providing guidance and support to government organisations on setting effective security policies and running organisational awareness campaigns.

It will also support non-cyber staff in wider business roles with information and learning on the use of strong passwords, avoiding phishing and other social engineering tactics, secure data handling, appropriate use of networks and devices and reporting of suspicious activity.

Priority next steps

Building

Skills priorities for Delivery Phase 1: Building the Model

The Government Cyber Unit will:

- establish and lead the Government Cyber Profession, appointing a Head of Cyber Profession and seeking heads of specialisms
- review central talent programmes and develop a clear plan for a new Cyber Resourcing Hub
- develop plans for raising awareness of cyber security including, induction programmes and mandatory training in cyber security, digital resilience and risk management for leaders, boards and wider workforces

Departments, ALBs, wider public sector organisations and suppliers will:

- recruit and retain professionals through competitive total job offers, entry schemes and recruitment programmes, upskilling, reskilling and supporting staff through learning and development and appealing career pathways
- raise awareness of cyber risk at leadership and board levels and across the workforce

For further information on implementation see **Chapter 9: Implementation**.

8

The Government Cyber Unit

Central functions

To achieve the transformation set out in this model, we will establish a set of central functions to deliver change across government. These functions will set direction, coordinate efforts and assure delivery, acting as an active centre to achieve maximum impact at scale.

We will create clear and transparent feedback channels so departments can share input. In turn, the central body will show how departmental input is shaping policies through forums and a structured feedback loop.

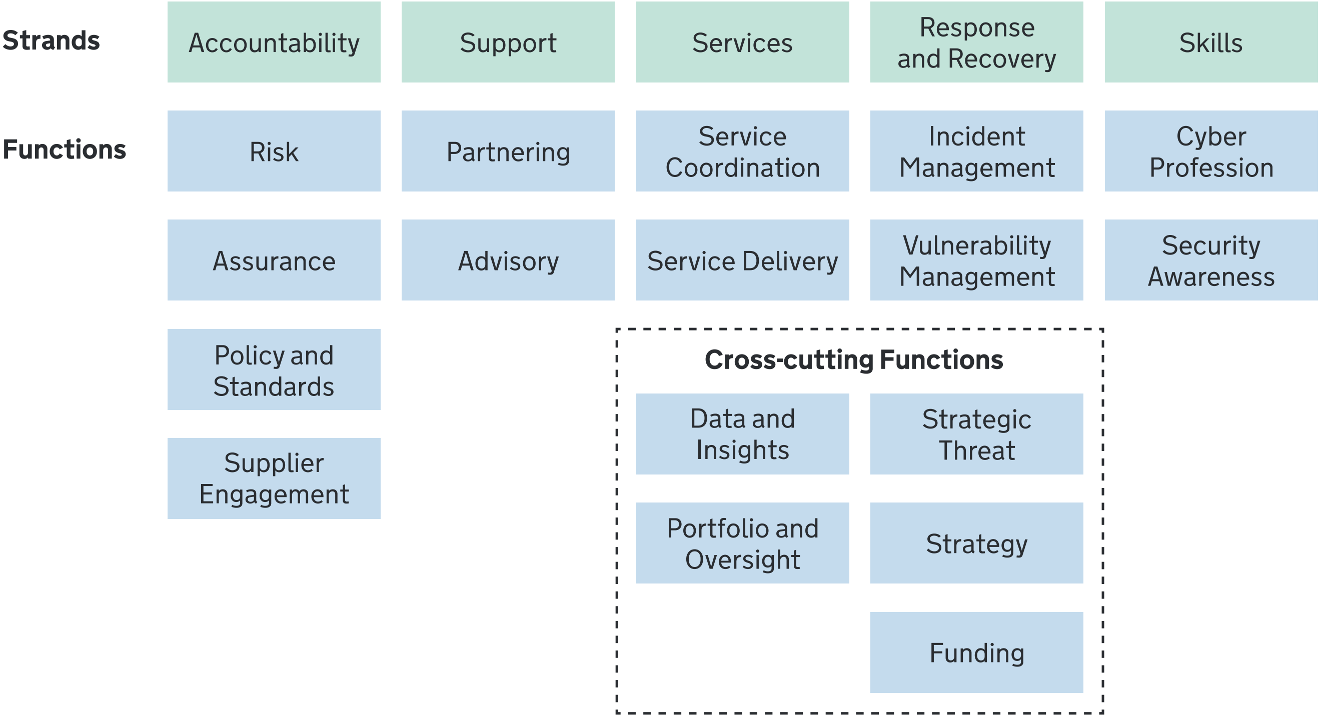
These new functions will give the Government Cyber Unit the right structures, resources and skills to lead in cyber security and resilience with a focus on continuous improvement.

Function	Objective
Strategy	Drive delivery of the Government Cyber Action Plan, set and review the strategic priorities for government and provide direction to government organisations.
Funding	Manage and allocate funds to the system to support their cyber initiatives, services and programmes.
Policy and Standards	Set and maintain mandatory policies and standards to ensure consistency and appropriate management of cyber risk.
Data and Insights	Collect, manage, aggregate and analyse data from public sector organisations, using these insights to improve decision-making. Create actionable insights which enhance resilience, and inform prioritisation and senior level comms.
Risk	Set and monitor performance against risk appetite at departmental level. Enable government-wide risk decision-making through assessments and recommendations. Manage escalation and mandate processes for government-level risks.
Assurance	Assure government, public sector, and key supplier performance against defined policies, standards, and mandates. Identify areas of low maturity or non-compliance to inform risk assessment, strategy and interventions.
Portfolio and Oversight	Manage the oversight of all projects, programmes, and initiatives delivered across the portfolio, ensuring delivery is managed, progress monitored and prioritised.
Services	Provide cyber security and resilience services to government organisations in a structured and standardised manner to build system resilience.
Operations	Help the system to prepare for, mitigate against, respond to and recover from cyber and technology incidents.
Partnering	Act as a single interface between DSIT and its stakeholders, concentrating on relationship building, understanding stakeholders' needs and priorities and facilitating collaboration.
Supplier Engagement	Oversee relationships with suppliers, making sure they meet their contractual obligations, provide high-quality services and contribute to the overall success of the system.

Function	Objective
Skills	Make sure that the system has the skills and capabilities it needs to deliver against its objectives.
Strategic Threat	Understand emerging threats, ensuring senior leaders across government are informed about cyber threats and their impact on business outcomes.
Advisory	Provide expert technical advice across all central functions and, on a prioritised basis, into departments.

How do the functions align and deliver the strands?

The functions align to enable the execution of the strands, ensuring that resources and expertise are effectively working towards the delivery of the strategic outcomes.



Function interactions

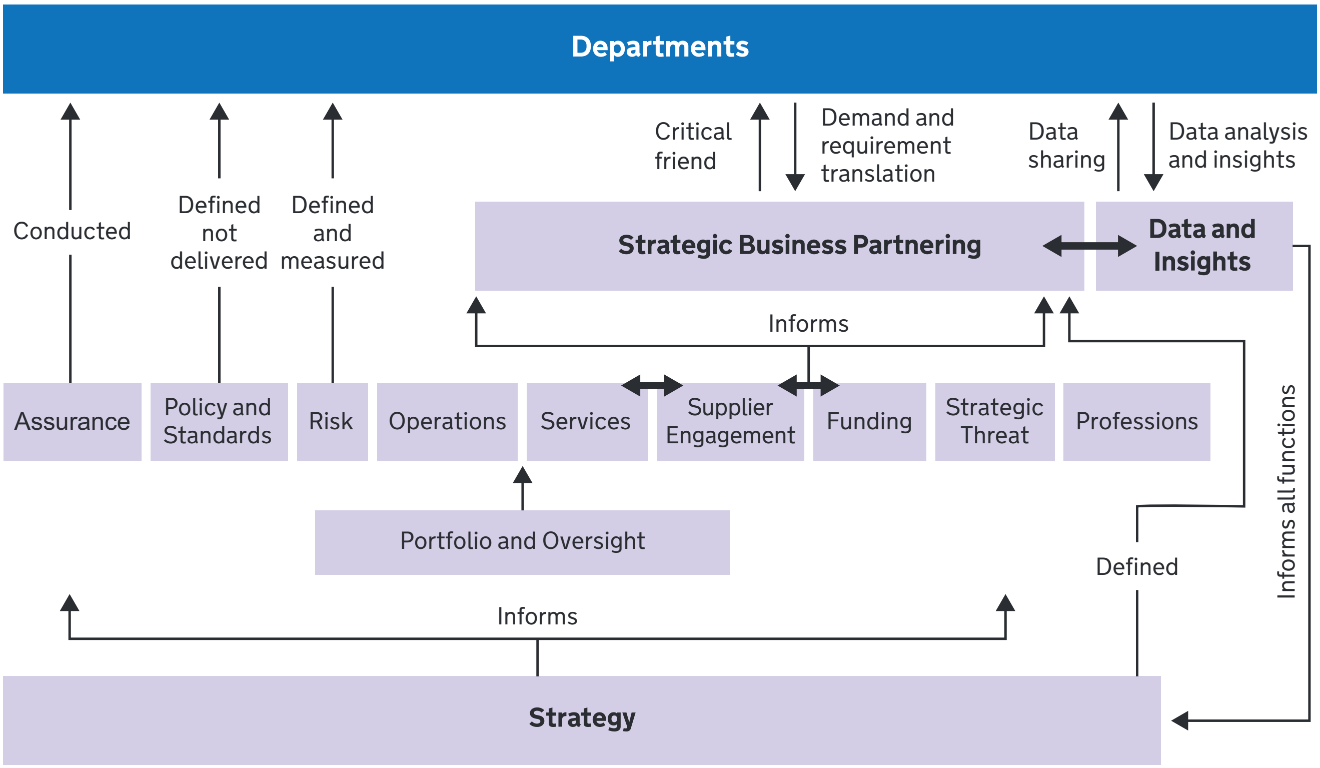
The central functions will not act in isolation but as part of an ecosystem working together to deliver the transformation change. The diagram below provides a high-level overview of how this will work in practice.

As well as showing the interactions between functions, the diagram references the main activities of each function. The direction of the arrows represents the direction of the interaction between functions. For example, the strategy set by Government Cyber Unit will inform the policies and standards that need to be implemented across public sector organisations.

Whilst they will be required to engage with central functions, departments, ALBs and other public sector organisations are empowered to tailor their own functions to their local needs. Public sector organisations are not expected to mirror Government Cyber Unit's functional interactions or to implement each function locally. Some capability will potentially be needed locally.

The functions within the diagram do not represent team or organisational structures within Government Cyber Unit.

Figure 11: Government Cyber Action Plan Functions Interactions



9

Implementation

Implementation targets

As set out in **Chapter 1: Introduction**, the Government Cyber Action Plan aims to deliver the Roadmap for Modern Digital Government aim of 'securing public services so they are trustworthy and resilient'. To deliver this, we will focus on achieving four strategic objectives through the strands of delivery described throughout the document.

Aim

Securing public services so they are trustworthy and resilient

Objective 1	Objective 2	Objective 3	Objective 4
Better visibility of cyber risk	Addressing severe and complex risks	Improving responsiveness to fast moving events	Rapidly increasing government-wide cyber resilience

Delivered through:

Accountability

Services

Support

Response & Recovery

Skills

Setting targets and monitoring delivery

To ensure we can effectively measure delivery, we have defined implementation milestones against each of these workstrands. We will use these milestones to hold ourselves and the wider government to account for delivering improvements in cyber security and digital resilience.

Milestones are aligned to the outcomes of the GCSS, which have been revised to better reflect the need to take action on digital resilience and to reduce dependency on legacy technology. We have also defined priority actions to be completed over the next 12 months, and will refresh these annually to ensure we are iterating our approach and focusing our action on where it can have the greatest impact.

Each milestone is supported by a comprehensive Performance Framework, which includes dedicated indicators to track progress and reflect the steps toward achievement. Every milestone and indicator is underpinned by a baseline, target, and data source, enabling us to measure progress, address risks early, and adjust course when needed.

By measuring and evaluating through our framework, we will be able to identify and cohere all the delivery across a broad range of delivery partners within a complex threat and technology environment. We also will be able to give leaders the view they need, and provide accurate information quickly as delivery progresses.

The framework will enable us to remain outcome focused, providing up to date information to inform agile working that adapts as things change. It will also give us up-to-date management information to drive responsive decision making, support visibility and drive progress and action.

Reporting and decision making

The National Audit Office (NAO) will receive bi-annual updates on progress against NAO recommendations to enable parliamentary scrutiny of government spending. Progress will also be reported regularly to senior cross-government governance at official level and to Ministers.

Implementation phases

The five strands will be delivered across three prioritised **phases of delivery**, outlined below. The four strategic objectives will be prioritised across the phases of delivery. All five strands will be delivered across all phases of delivery with specific implementation milestones setting out what will be achieved in each phase.

Building

Phase 1: Building

By April 2027, we will build a new model for government cyber by:

- building critical functions to establish the Government Cyber Unit
- establishing refreshed accountability and governance for government cyber risk
- standing up prioritised central services and support functions
- setting clear targets and standards for government organisations
- launching a new cyber profession for government
- directing action across government in response to fast-moving events, through structures defined in a Government Cyber Incident Response Plan

Scaling

Phase 2: Scaling

By April 2029, we will scale and leverage this new model by:

- using government-wide cyber risk visibility to make data-driven decisions and a compelling investment case for managing severe and complex cyber risks
- delivering a pipeline of cyber support and services to help departments meet their responsibilities
- scaling and maturing response and recovery capability to address concurrent major cyber events
- developing high-impact, sector-wide role-based learning pathways for top high-risk cyber specialisms
- departments fully operating within governance and reporting structures for themselves, their ALBs, and sectors
- departments delivering costed cyber improvement plans in line with defined central and local cyber risk appetites, drawing on central support and services

Improving

Phase 3: Improving

April 2029 and beyond, we will use the model to continuously improve government-wide cyber security and resilience by:

- enabling decision-making and prioritisation at all levels of government through sharing central cyber data insights, including evidence-based investment in cross-government platforms, services and infrastructure to address critical risks
- offering central cyber support and services at scale based on identified needs and strategic fit in a sustainable pipeline and lifecycle
- leveraging Government Cyber Profession as engine for transformation through career framework and sector recognised accreditation standards
- departments proactively assuring cyber risk across their supply chains, enabled by central management of strategic suppliers
- supporting national security and growth objectives and underpins government missions through increased resilience

Phase 1 – Building (by March 2027)

Accountability

Priority activities:

1. On behalf of the Government Technology Risk Owner, the Government Cyber Unit will establish new risk management roles, structures, processes and governance.
2. The Government Cyber Unit will set direction and develop practical support for local cyber risk management.
3. The Government Cyber Unit will engage strategic suppliers to ensure resilience outcomes are met and standards raised.
4. Government organisations and suppliers will manage and report on their cyber risk in alignment with government-wide risk processes.
5. Government organisations will also consider appropriate mechanisms to ensure suppliers appropriately manage government cyber risk.

Outcome	Milestones & activities
1. Government organisations deploy cyber security and resilience controls commensurate with their risk profile to ensure that risks to their functions are managed proportionately.	• Systemic cyber and resilience risks are escalated, discussed and understood through a new risk framework with data reviewed quarterly.
2. Government has established governance arrangements, escalation routes and clear accountability enabling effective management of cyber risks at all levels of government.	• The Government Cyber Unit will establish new risk management roles, processes and governance. [priority activity 1]
3. Government organisations have timely access to relevant and actionable cyber security and resilience data that enhances their ability to make effective risk management decisions at an organisational and cross-government level.	• The Government Cyber Unit provides departments with specific direction and practical support on how to manage their cyber risk within appetites. [priority activity 2]
4. Government assurance provides the government with the visibility it needs to make effective risk-management decisions and the confidence that it has appropriate cyber security and resilience measures in place to manage the risks to its functions.	• Government organisations will manage and report cyber risk in alignment with government-wide risk processes. [priority activity 4]

Outcome	Milestones & activities
5. Government has visibility and understanding of critical digital assets, including legacy, enabling it to identify and manage risks of the systems that it runs in a timely manner.	• The Government Cyber Unit will set out what proportion of critical and legacy IT systems it has assessed so far, and continue building the capacity to support departments in developing and implementing improvement plans. • The Government Cyber Unit will establish a mechanism to prevent departments from diverting funding away from critical and legacy IT systems.
6. Government understands and manages organisational and cross-government level cyber security and resilience risks and aggregate risks held within supply chains.	• The Government Cyber Unit will engage strategic suppliers to ensure resilience outcomes are met and standards raised. [priority activity 3] • Government organisations will also consider appropriate mechanisms to ensure suppliers appropriately manage government cyber risk. [priority activity 5]
7. Government has a clear understanding of the aggregate risks it faces at both the organisational and cross-government levels, enabling effective risk management.	• 75% of organisations have an actively managed risk register capturing internal and cross-government cyber security and resilience risks.
8. Government understands the threat it faces in order to plan appropriate mitigations, at both an organisational and cross-government level.	• Feedback from security leaders and senior decision makers demonstrates accessibility, relevance and value of the Government Cyber Unit government cyber strategic threat understanding outputs. Feedback is also used to continue to identify and address blockers to raise cyber strategic threat awareness across government.

Support and Services

Priority activities:

1. The Government Cyber Unit will map existing provision of core services and support and identify priority requirements across departments, establishing a technical advisory function and a CISO community to enable engagement.
2. It will also develop a service finder to facilitate access to services and establish a service coordination function. This will include a DSIT-NCSC strategic partnership providing a new framework for service collaboration with NCSC.
3. Government organisations and suppliers will identify their priority requirements, consider how they can adopt or share existing support and develop costed options for this.

Outcome	Milestones & activities
9. Government adopts a common approach to digital resilience and 'secure by design' to ensure that appropriate and proportionate measures are embedded within the technology government uses	• 100% of organisations follow and demonstrate adherence to the government Secure by Design approach so that security is built in from the start, reducing future risks and costs while strengthening resilience and public trust in government digital services. • 100% of organisations with government Critical National Infrastructure undergo regular assurance checks via Secure by Design integration within Digital and Technology Spend Controls so that security and resilience remains under constant review, reducing risks and strengthening trust in government digital services. • Quality and evaluation mechanisms track and support change initiatives to improve cyber security and resilience so that digital services and infrastructure remain robust against evolving threats.
10. Government technology is appropriately configured, with standard profiles for common technology and architectures being developed, adopted and continuously updated.	• 100% of departments have a local cyber security strategy and resilience strategy aligned to the Government Cyber Action Plan's Implementation plan endorsed by ExCo/seniors. • Define migration goals and governance by developing a government-wide approach for PQC migration, and develop a roadmap to ensure alignment across departments, ALBs, and CNI organisations.

Outcome	Milestones & activities
11. Strategic partnerships with the private sector and international partners are further embedded to enhance proactive defence at a global scale.	• Cross-government engagement mechanism is in place for strategic partnerships with academia and industry, including a register of key partners and thematic areas.
12. Shared capabilities, tools and services tackle frequently experienced cyber security and resilience issues across organisations at scale.	• 100% of central cyber and resilience services will develop an impact measure. • At least 70% of target organisations can measure and demonstrate impact from adopting central cyber security and resilience services. • Departments will identify their priority requirements, consider how they can adopt or share existing support and develop costed options for this. [priority activity 3] • The Government Cyber Unit will prioritise development of services to address the most severe risks maximising impact and progress towards strategic goals. [priority activity 1 and 2] • Introduce a service feedback and evaluation process, with 80% of target organisations rating cyber security and resilience services as meeting or exceeding expectations in terms of relevance, usability, and cyber security and resilience impact.

Response and Recovery

Priority activities:

1. The Government Cyber Unit will publish the Government Cyber Incident Response Plan (G-CIRP) to define structures, roles and responsibilities for cyber incident response in government
2. It will also redesign operations capabilities within GC3, scoping and establishing commercial arrangements for a Government CIR retainer and a single, cross-government incident repository to capture lessons learnt and generate insight
3. Government organisations and suppliers will update response and recovery plans to align with G-CIRP and review capabilities against arrangements for CIR provision
4. They will also engage on the development of common detection rulesets and taxonomy to lay the foundations for detection for government

Outcome	Milestones & activities
13. Government effectively detects and communicates activities targeting its networks, systems, and services in a timely manner, except for the most sophisticated ones.	• The Government Cyber Unit will redesign operations capabilities within GC3, scoping and establishing commercial arrangements for a Government CIR retainer and a single, cross-government incident repository to capture lessons learnt and generate insight. [priority activity 2]
14. Government effectively responds to cyber and resilience incidents, both organisationally and across government.	• GC3's established mandate and responsibilities cover both cyber and resilience incidents.
15. Government is well prepared to respond to cyber and digital resilience incidents.	• The Government Cyber Unit will publish the Government Cyber Incident Response Plan (GCIRP) to define structures, roles and responsibilities for cyber incident response in government. [priority activity 1] • % of government and public sector organisations with comprehensive cyber and resilience incident plans in place (a target percentage value will be set once we have a baseline figure).
16. Shared capabilities enable the understanding, detection and investigation of threats at scale across government.	• The Government Cyber Unit will redesign operations capabilities within GC3, establishing a single, cross-government incident repository to capture lessons learnt and generate insight. [priority activity 2]

Outcome	Milestones & activities
17. Government restores digital systems and assets affected by incidents and has mechanisms in place to ensure minimal disruption.	• The Government Cyber Unit will redesign operations capabilities within GC3, scoping and establishing commercial arrangements for a Government CIR retainer. [priority activity 2]
18. A culture of transparency and learning enables the rapid sharing of incident insights among departments, which are then applied across government to enhance collective security and resilience.	• A single, cross-government incident repository is operational, capturing data from both cyber and non-malicious disruptions. This repository will generate regular lessons learned reports and quarterly insight packs that are systematically shared across departments to drive improvements in resilience.

Skills

Priority activities:

1. The Government Cyber Unit will establish and lead the first cross-government Cyber Profession, appointing a Head of Cyber Profession and seeking heads of specialisms.
2. The Government Cyber Unit will also review central talent programmes and develop a clear plan for a new Cyber Resourcing Hub.
3. The Government Cyber Unit will develop plans for raising awareness of cyber security including, induction programmes and mandatory training in cyber security and resilience and risk management for leaders, boards and wider workforces.
4. Government organisations and suppliers will recruit and retain professionals through competitive total job offers, entry schemes and recruitment programmes, upskilling, reskilling and supporting staff through learning and development and appealing career pathways.
5. Government organisations and suppliers will also raise awareness of cyber risk at leadership and board levels and across the workforce.

Outcome	Milestones & activities
19. Public sector attracts, recruits, retains and continuously develops the cyber security and digital workforce it needs to be secure and resilient.	• The Government Cyber Unit will launch a cyber profession for government with a clear plan for roll out. [priority activity 1] • The Government Cyber Unit will review central talent programmes and government training programmes and set clear direction on priorities going forward. [priority activity 2 and 3]
20. Public sector leaders understand digital resilience and cyber security risks to their own organisation and are able to identify, own and manage their organisational risk and its wider impact across the public sector.	• Initial steps will be undertaken as part of the accountability priorities.
21. Public sector professionals across all functions and levels have an understanding of cyber security and resilience that equips them to appropriately manage risk in their roles.	• The Government Cyber Unit will develop mechanisms to raise awareness and understanding are developed. [priority activity 4]

Phase 2 – Scaling
(April 2027–2029)

Accountability

Outcome	Milestones
1. Government organisations deploy cyber security and resilience controls commensurate with their risk profile to ensure that risks to their functions are managed proportionately.	• Establish a robust control library adapted and piloted by at least five organisations in order to demonstrate appropriate use of the controls, commensurate with risk.
2. Government has established governance arrangements, escalation routes and clear accountability enabling effective management of cyber and resilience risks at all levels of government.	• All organisations implement defined governance structures with clearly documented roles and responsibilities for both cyber security and resilience. • In collaboration with The Government Cyber Unit, 100% of departments have implemented a risk appetite assessment, analysis and reporting process (to be automated) for cyber security and resilience risks based on severity and business impact.
3. Government organisations have timely access to relevant and actionable cyber security and resilience data that enhances their ability to make effective risk management decisions at an organisational and cross- government level.	• An established and resourced data insights capability (with staffing, an approved central data strategy and scoping of cross-government cyber data integration) supports informed decision- making to reduce cyber and resilience risk and guide prioritisation.
4. Government assurance provides the government with the visibility it needs to make effective risk management decisions and the confidence that it has appropriate cyber security and resilience measures in place to manage the risks to its functions.	• Departments are able to report to the central government on the cyber security resilience of organisations within their purview with reference to CAF objectives.
5. Government has visibility and understanding of critical digital assets, including legacy, enabling it to identify and manage risks of the systems that it runs in a timely manner.	• Outcome achieved in Phase 1.
6. Government understands and manages organisational and cross-government level cyber security and resilience risks and aggregate risks held within supply chains.	• Milestones included in later phases.

Outcome	Milestones
7. Government has a clear understanding of the aggregate risks it faces at both the organisational and cross-government levels, enabling effective risk management.	• Cross-government risk aggregation is used to support understanding and decision making to manage systemic risks.
8. Government understands the threat it faces order to plan appropriate mitigations, at both an organisational and cross-government level.	• Milestones included in later phases.

Support and Services

Outcome	Milestones
9. Government adopts a common approach to digital resilience and 'secure by design' to ensure that appropriate and proportionate measures are embedded within the technology government uses.	• 60-70% of government departments have completed a foundational Secure by Design capability assessment, facilitated by the central support function, to baseline their adoption of the common approach.
10. Government technology is appropriately configured, with standard profiles for common technology and architectures being developed, adopted and continuously updated.	• 100% of departments that will have established costed cyber security and resilience implementation plans for themselves, their Arm's Length Bodies (ALBs), and the wider public sector remit, and will have either secured funding or a clear understanding of funding implications. • 100% of departmental strategies and implementation plans are reviewed annually and updated in line with central threat assessment and digital resilience assessment, revised guidance and policy and in line with the central strategy/ Implementation Plan. • 80% of departments have developed and documented a standard security profile for at least two of their most common technology platforms (for example, a specific cloud service, a standard operating system), created in direct collaboration with the central support function. • Standard profiles for common technologies and architectures are developed.
11. Strategic partnerships with the private sector and international partners are further embedded to enhance proactive defence at a global scale.	• Milestones included in later phases only.
12. Shared capabilities, tools and services tackle frequently experienced cyber security and resilience issues across organisations at scale.	• An established pipeline for transitioning successful cyber security and resilience pilots into operational capabilities, as measured by the rate of adoption.

Response and Recovery

Outcome	Milestones
13. Government effectively detects and communicates activities targeting its networks, systems, and services in a timely manner, except for the most sophisticated ones. Note: Potentially expand the outcome to cover digital resilience.	• % of departments that reliably detect common and emerging cyber threats (a target percentage value will be set once we have a baseline figure). • % of identified cyber threats that are investigated rapidly, effectively, and efficiently, disaggregated by department (a target percentage value will be set once we have a baseline figure).
14. Government effectively responds to cyber and digital resilience incidents, both organisationally and across government.	• 100% of government and public sector organisations that report incidents using the common taxonomy and provide performance data against defined metrics. • GC3 is the established centre of excellence for digital resilience and cyber incident management, effectively coordinating the cross-government response to all digital resilience and cyber incidents.
15. Government is well prepared to respond to cyber and digital resilience incidents.	• 100% of organisations have developed and validated restoration readiness plans, including mapped dependencies, minimum restoration standards, and rehearsed procedures, ensuring preparedness to rapidly recover critical services following disruption.
16. Shared capabilities enable the understanding, detection and investigation of threats at scale across government.	• 95% of departments and key ALBs are utilising the centre's real-time, actionable intelligence and detection capabilities.
17. Government restores digital systems and assets affected by incidents and has mechanisms in place to ensure minimal disruption.	• 100% of organisations that assess and report on both cyber and non-malicious digital resilience restoration activities, using a common taxonomy that evidences performance against centrally defined metrics (e.g. Recovery Time Objectives (RTO) and Mean Time to Restore (MTR)).

Outcome	Milestones
18. A culture of transparency and learning enables the rapid sharing of incident insights among departments, which are then applied across government to enhance collective cyber security and resilience.	• A single, cross-government incident repository is operational, capturing data from both cyber and non-malicious disruptions. This repository will generate regular lessons learned reports and quarterly insight packs that are systematically shared across departments to drive improvements in resilience. • 75% of organisations evidence that at least one shared incident insight has been applied to their internal policies, controls, or playbooks within six months of publication, embedding lessons learned into practice.

Skills

Outcome	Milestones
19. The public sector attracts, recruits, retains and continuously develops the cyber security and digital workforce it needs to be secure and resilient.	• The Head of Cyber Profession is appointed and has established the necessary leadership and governance structures for the profession. These structures have endorsed the initial accreditation standards and a multi-year roadmap for the formal establishment of the career framework, ensuring alignment with wider sector recognition.
20. Public sector leaders understand digital resilience and cyber security risks to their own organisation and are able to identify, own and manage their organisational risk and its wider impact across the public sector.	• Develop high-impact, sector-wide role-based learning pathways for top high-risk professionals including people in technology and procurement, with at least 70% of targeted cohorts completing the pathway.
21. Public sector professionals across all functions and levels have an understanding of cyber security and resilience that equips them to appropriately manage risk in their roles.	• Milestones included in later phases only.

Phase 3 – Improving
(April 2029 and beyond)

Accountability

Outcome	Milestones
1. Government organisations deploy cyber security and resilience controls commensurate with their risk profile to ensure that risks to their functions are managed proportionately.	• Organisations are actively using effective and appropriate cyber security control libraries to inform risk-based decision-making.
2. Government has established governance arrangements, escalation routes and clear accountability enabling effective management of cyber security and resilience risks at all levels of government.	• Outcome achieved in Phase 2.
3. Government organisations have timely access to relevant and actionable cyber security and resilience data that enhances their ability to make effective risk management decisions at an organisational and cross-government level.	• Data insights drive evidence-based prioritisation of central government cyber security and resilience resources and programmes and are integrated into strategy delivery and governance, enabling improved risk management outcomes. Insights are routinely shared with departments to help them make similar prioritisation decisions.
4. Government assurance provides the government with the visibility it needs to make effective risk management decisions and the confidence that it has appropriate cyber security and resilience measures in place to manage the risks to its functions.	• 2/3 of the systems assessed by GovAssure meet 75% or more of the CAF profile outcomes.
5. Government has visibility and understanding of critical digital assets, including legacy, enabling it to identify and manage risks of the systems that it runs in a timely manner.	• Outcome achieved in Phase 1.

Outcome	Milestones
6. Government understands and manages organisational and cross-government level cyber security and resilience risks and aggregate risks held within supply chains.	• At least 90% of LGDs and 50% of ALBs undertake some type of assurance process of their supply chain. At a minimum this shall include an annual Cyber Essentials check. • 80% of new government contracts with a Managed Service Provider or Digital Service Provider will contain either framework or tailored security schedules (covering both cyber and digital resilience risks).
7. Government has a clear understanding of the aggregate risks it faces at both the organisational and cross-government levels, enabling effective risk management.	• Outcome achieved in Phase 2.
8. Government understands the threat it faces in order to plan appropriate mitigations, at both an organisational and cross-government level.	• Relative to a yet to be established baseline, an appropriate % of surveyed security leaders and senior decision makers report that they understand the strategic cyber threat landscape, measured through: (1) self-assessed awareness of strategic cyber threat landscape and the threat government faces; (2) self-assessed confidence to apply that threat awareness. • Prioritisation of mitigating actions and strategic decision making at both HMG and department level is demonstrably driven from integrated threat.

Support and Services

Outcome	Milestones
9. Government adopts a common approach to digital resilience and 'secure by design' to ensure that appropriate and proportionate measures are embedded within the technology government uses.	• Extent to which user-driven technical guidance and resources are publicly available to support cyber and digital resilience across services so that practical tools are widely accessible and consistent security practices exist across government.
10. Government technology is appropriately configured, with standard profiles for common technology and architectures being developed, adopted and continuously updated.	• The secure transition to Post-Quantum Cryptography (PQC) is supported by the provision of continuous monitoring and governance, facilitated cross-government collaboration, engagement with technology vendors, and the development of practical guidance.
11. Strategic partnerships with the private sector and international partners are further embedded to enhance proactive defence at a global scale.	• UK makes a reciprocated global contribution to cyber security, with at least five international partners adapting and implementing cyber security guidance, frameworks, or tools developed by the UK Government. • At least 5 private sector partners have implemented the new strategic partnership agreement.
12. Shared capabilities, tools and services tackle frequently experienced cyber security and digital resilience issues across organisations at scale.	• A sustainable pipeline and lifecycle for cyber security and digital resilience services is established, enabling services to be offered at scale based on identified needs and strategic fit.

Response and Recovery

Outcome	Milestones
13. Government effectively detects and communicates activities targeting its networks, systems, and services in a timely manner, except for the most sophisticated ones. Note: Potentially expand the outcome to cover digital resilience.	• 100% of departments actively sharing threat and risk information in near real-time to support a collective public sector response.
14. Government effectively responds to cyber and digital resilience incidents, both organisationally and across government.	• Key principles of communication, collaboration and coordination are embedded in all government and public sector organisations' response to cyber and digital resilience incident.
15. Government is well prepared to respond to cyber and digital resilience incidents.	• 100% of organisations that regularly exercise their digital recovery plans. • 100% of organisations that regularly exercise their incident response plans annually. • 100% of departments that have operationalised processes in place to enable effective and timely incident response, covering triage, alerting, escalation, notification, lessons learned, and access to relevant skills and capabilities.
16. Shared capabilities enable the understanding, detection and investigation of threats at scale across government.	• A mature, collaborative threat detection ecosystem is in place across the public sector, characterised by intelligence sharing, standardised detection practices, and modern Security Operations.
17. Government restores digital systems and assets affected by incidents and has mechanisms in place to ensure minimal disruption.	• GC3 acts as the operational hub for cross-government cyber and digital resilience recovery, coordinating the deployment of specialist surge support and managing national-level dependencies to accelerate the restoration of critical services. • Key principles of communication, collaboration, and coordination are embedded across organisations recovery activities, ensuring a coherent, transparent, and efficient restoration of services.

Outcome	Milestones
18. A culture of transparency and learning enables the rapid sharing of incident insights among departments, which are then applied across government to enhance collective security and digital resilience.	• Outcome achieved in Phase 2.

Skills

Outcome	Milestones
19. The public sector attracts, recruits, retains and continuously develops the cyber security and digital workforce it needs to be secure and resilient.	- The Government Cyber Security Profession is formally established with a recognised head of profession, career framework and sector recognised accreditation standards to improve attraction and retention rates.
20. Public sector leaders understand digital resilience and cyber security risks to their own organisation and are able to identify, own and manage their organisational risk and its wider impact across the public sector.	- 95% of senior leadership and others in mission critical roles have completed a mandatory programme of appropriate cyber security and resilience awareness learning, embedded into onboarding and ongoing development. - Develop high-impact, sector-wide role-based learning pathways for top high-risk professions including people, technology and procurement, with at least 70% of targeted cohorts completing the pathway.
21. Public sector professionals across all functions and levels have an understanding of cyber security and digital resilience that equips them to appropriately manage risk in their roles.	- 85% of risk owners across government have completed advanced cyber and digital resilience risk management training, with skills integrated into strategic planning cycles.

Glossary

Glossary

A

Accountability:

Answerable for outcomes, achievements and failures, in accordance with defined responsibilities, objectives and targets. Accountability includes ownership, responsibility and consequences.

Accounting Officer:

Individual with personal responsibility for managing an organisation, generally a permanent secretary or chief executive officer.

Arm's-length bodies (ALB):

A commonly used term covering a wide range of public bodies, including non-ministerial departments, non-departmental public bodies, executive agencies and other bodies, such as public corporations.

C

Cyber Assessment Framework (CAF):

A high-level framework developed by the National Cyber Security Centre. It represents an industry framework that is used by operators of essential services under the Network and Information Systems regulations as well as more widely across the private and public sectors, including Critical National Infrastructure (CNI) sectors.

Capability:

A capability is defined as "an ability to do something". It is a particular ability or capacity that the organisation possesses to achieve a specific purpose or outcome. Critically, a capability delineates what is done without attempting to explain how.

Cyber security assurance:

The process of ensuring that systems, networks, programs, devices, and data are protected from cyber-attacks through the application of technologies, processes, and controls. It involves assessing and verifying the effectiveness of security measures in place to identify and address vulnerabilities.

Cyber resilience:

The ability of an organisation to maintain the delivery of its functions and services and ensure the protection of its data, despite cyber security events.

Cyber security:

The protection of internet-connected systems (to include hardware, software and associated infrastructure), the data on them, and the services they provide, from unauthorised access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures or being manipulated into doing so.

D

Digital, Data and Technology (DDaT):

The specialist function of government that deals with information technology and transformation in this area.

Digital Resilience:

The ability of digital systems and technology to minimise disruption or loss of service by any cause, and the capability to recover or restore these services quickly when they are lost or degraded.

Disclosure for Government:

A route for members of the public to disclose vulnerabilities found in UK Government.

F

Function:

A grouping aligned across the system. Sets cross- government strategies, sets and assures standards, develops capability, gives expert advice, encourages continuous improvement, and develops and delivers commonly required services.

G

GovAssure:

The cyber security scheme for assessing government critical systems.

Government Cyber Advisory Board (GCAB):

A body composed of independent external experts to bring perspectives and expert input from industry and academia to addressing the challenges of Government cyber security.

Government Cyber Action Plan:

A strategic framework that sets out a radical shift in managing public sector cyber and digital resilience risks. It establishes a Target Operating Model with the Government Cyber Unit at the centre to deliver system-wide capability, supported by specific milestones and a performance framework to measure progress.

Government Cyber Coordination Centre (GC3): GC3 is part of the Government Cyber Unit, and jointly sponsored with National Cyber Security Centre. It coordinates the cross-government response to cyber threats, vulnerabilities and incidents. Its role is primarily operational, and enables cyber teams across government to defend as one.

Government Cyber Security Strategy (GCSS):

Strategy setting out the government's approach to building a cyber resilient public sector.

Government Cyber Unit: The central unit within DSIT responsible for driving cyber security and resilience transformation across government and the public sector.

Government Digital Service (GDS):

The digital centre of government. Serving the public, central government departments and the wider public sector to deliver technical capability within the digital space. GDS is part of the Department for Science, Innovation and Technology (DSIT).

Government Security Group (GSG):

The Cabinet Office unit responsible for the oversight, coordination and delivery of protective security within all central government departments, their agencies and arm's length bodies.

I

Impact:

A combination of the scope, scale and duration of harm resulting from an incident. In a cyber and digital resilience context this refers to a loss of confidentiality, integrity, or availability of information or a system which may disrupt the operations of government organisations or essential public services, or erode UK national security.

Initiative:

A deliberate action or set of actions proposed and/or taken to improve or enhance an organisation's capabilities or services. The specific approach taken will depend on the nature of the requirements and desired outcomes. Once an initiative is proven, it will become a new, or updated service or capability.

L

Lead government department (LGD):

A government department that has other public sector organisations within its purview. LGD is usually the department with primary policy responsibility for the risk and expertise for the area impacted by the emergency scenario.

Legacy systems:

Obsolete systems that can no longer be effectively supported or protected from attacks.

Lines of Defence (LOD):

A model for risk management which identifies three reporting lines within an organisation. The first line carries out risk management as part of operational activity, the second line sets policies and standards and monitors the first line for compliance, and the third line provides independent audit and oversight of risk management activities.

N

National Cyber Security Centre (NCSC):

The NCSC is the UK's 'technical authority' for cyber incidents. It is part of GCHQ, one of the UK's security services, and was formed in 2016 to provide a unified national response to cyber threats.

National Technical Authority (NTA):

Designation for a body considered to be the national authority on its area of expertise.

O

Organisation:

The government and public sector organisations to which the Government Cyber Action Plan applies. This includes departments, ALBs, and public sector bodies.

P

Product:

A service, physical item, or digital item that provides an agreed and specific outcome for a consumer that incorporates and needs software to realise that outcome, and is expected to require active management of the software and its required resources over its life cycle.

R

Risk appetite:

The amount of risk an organisation, or subset of it, is willing to accept.

Risk Management:

The steps an organisation takes to understand, identify, assess, and manage cyber and digital resilience risks, including risks to network and information systems supporting the operation of essential functions. This includes an overall organisational approach to risk management. Source: Government Cyber Security Policy Handbook.

Risk tolerance:

The threshold levels of risk exposure that, with appropriate approvals, can be exceeded, but which when exceeded will trigger some form of response or escalation (for example, reporting the situation to senior management for action).

Root Cause Analysis (RCA):

A systematic approach towards identifying the underlying causes for issues. This has been used in the context of a project to analyse GovAssure data and understand the root causes of departments not meeting the required profile.

S

Secure by Design:

The discipline of embedding cyber security into digital systems and services at every step of their lifecycle: from the planning of a service, to the procurement and configuration of technology and its decommissioning at the end of its operational life.

Service:

A service captures all the things that collectively deliver an outcome for users. Note: A service is a complete solution that brings together technology and non-technology elements to enable users to achieve a defined outcome.

V

Vulnerability:

Security flaws in software programs that have the potential to be exploited by attackers.

Vulnerability Reporting Service:

A service providing a mechanism through which an organisation can be alerted to security flaws by a member of the public.

W

Wider Public Sector (WPS):

Other public bodies which do not come under the central government classification.

UK Government

Department for Science,
Innovation and Technology
22-26 Whitehall
London
SW1A 2EG

ISBN 978-1-5286-6152-2
E03515734