



HM Government

Government Cyber Security Strategy

Building a cyber resilient public sector

2022–2030

Contents

Foreword from the Prime Minister	6
Message from the Chancellor of the Duchy of Lancaster and Minister for the Cabinet Office	7
Executive Summary	8
Chapter 1: Context	12
The importance of government cyber security to national resilience	13
The challenges and opportunities for government	14
Chapter 2: Approach	18
Vision and Aim	19
Pillars	22
Objectives	25
Chapter 3: Managing cyber security risk	28
Governance and accountability	30
Assets and vulnerabilities	31
Data assets	32
Supply chain risk	32
Threat information	34
Cyber security data	35
Government cyber security assurance	36
Private sector and international partnerships	37
Chapter 4: Protecting against cyber attack	38
Secure technology and digital services	40
Cyber security controls	42
Secure configuration	44
Shared capabilities	44
Information and data security	46
Chapter 5: Detecting cyber security events	50
Detection within government organisations	52
Detection at scale	53
Chapter 6: Minimising the impact of cyber security incidents	54
Response preparation	56
Incident response	56
Incident recovery	57
Lessons learned	57

Contents

Chapter 7: Developing the right cyber security skills, knowledge and culture	58
Skills requirements	60
Attract and retain talent	61
Develop talent	62
Cyber security knowledge across other government functions	63
Cyber security culture	63
Chapter 8: Measuring success	64
Achieving the aim	65
Maintaining an appropriate measure of resilience	66
Underpinning key performance indicators	66
Chapter 9: Implementing the strategy	68
Implementation	69
Transformational proposals	70
Implementation plan	72
Annex: Cyber Assessment Framework	76
Glossary	78

Ministerial Forewords



Foreword from the Prime Minister

In the Integrated Review I make absolutely clear the importance of national resilience to the security and prosperity of the UK. Cyber resilience lies at the very heart of this. Few nations are better placed to navigate these challenges, but we must be willing and able to adapt to this new world emerging around us. Our National Cyber Strategy hits this head on - setting out how the UK will firmly establish itself as a democratic and responsible cyber power, able to protect and promote its interests as a sovereign nation in a world fundamentally shaped by technology.

To realise this ambition however, government itself must lead by example. As well as ensuring that government organisations can protect the services and functions that maintain and promote our economy and society, government must be an exemplar to the private sector, to ensure that the UK continues to enhance its reputation as one of the most secure and attractive digital economies in which to live, do business and invest in.

The challenge cannot be underestimated, but tackling it is imperative. That is why I am delighted to set out here the Government Cyber Security Strategy which sets out how we will ensure that all government organisations - across the whole public sector - are resilient to the cyber threats we face.



Message from the

Chancellor of the Duchy of Lancaster and Minister for the Cabinet Office

Government organisations - and the functions and services they deliver - are the cornerstone of our society. It is their significance, however, that makes them an attractive target for an ever-expanding army of adversaries, often with the kind of powerful cyber capabilities which, not so long ago, would have been the sole preserve of nation states. Whether in the pursuit of government data for strategic advantage or in seeking the disruption of public services for financial or political gain, the threat faced by government is very real and present.

Government organisations are routinely and relentlessly targeted: of the 777 incidents managed by the National Cyber Security Centre between September 2020 and August 2021, around 40% were aimed at the public sector. This upward trend shows no signs of abating.

Building and maintaining our cyber defences is therefore vital if we are to protect the functions and services on which we all depend. As government, we have made a great deal of progress in recent years, but there is much more to do. To meet the threats we will face in the coming decade we must build on our successes and transform how we approach cyber security in government.

The Government Cyber Security Strategy sets out how we will do this; by building greater cyber resilience across all government organisations, and working together to 'defend as one' - exerting a defensive force greater than the sum of our parts.

Every part of government has a role in achieving this. Government organisations are rightly empowered to manage their cyber risks - as well as harnessing local knowledge and understanding, this allows for tremendous innovation and agility. Such knowledge and expertise must however be shared across government to enhance our collective response, with more and advanced shared capabilities and services making the task increasingly straightforward, effective and efficient. This strategy provides the framework to drive this forward.

Government's resolve to achieve this is absolute. This commitment is reflected in the 2021 Comprehensive Spending Review, with £2.6 billion being invested in cyber and legacy IT, of which government cyber security is a critical component. £37.8 million of additional funding is also being invested to tackle cyber security challenges facing local councils to protect vital services and data, alongside targeted investment in our most critical departments.

This is an ambitious but necessary strategy that demands action across all of government. We must meet our responsibility to ensure that government's functions and services are resilient to the cyber threats they face - creating a stronger, better-defended government that is the foundation of our status as a cyber power.

Executive Summary

Context

1. The Integrated Review¹ and the National Cyber Strategy² set out the government’s ambition to firmly establish the UK as a democratic and responsible cyber power, able to protect and promote its interests as a sovereign nation in a world fundamentally shaped by technology. The UK’s legitimacy and authority as a cyber power is however dependent upon its domestic cyber resilience, the cornerstone of which is government and the public sector organisations that deliver the functions and services which maintain and promote the UK’s economy and society.
2. While government has made notable progress in recent years, there remains a significant gap between where government cyber resilience is now and where it needs to be. This gap is brought into sharp focus by the sheer volume of cyber attacks that the government sector experiences, and the evolving capabilities and techniques of the broad range of malicious actors conducting them. As well as the risk of disruption to government functions and public services, the targeting of essential services such as healthcare can pose a real risk to public safety.



Vision and Aim

3. This strategy’s vision is therefore to ensure **that core government functions - from the delivery of public services to the operation of National Security apparatus - are resilient to cyber attack, strengthening the UK as a sovereign nation and cementing its authority as a democratic and responsible cyber power.**
4. Core government functions are delivered by many diverse public sector organisations, including government departments, arms-length bodies, agencies and local authorities. This strategy therefore considers all such public sector organisations.
5. To achieve its vision the strategy pursues a central aim - **for government’s critical functions to be significantly hardened to cyber attack by 2025, with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030.**
6. This is a bold and ambitious aim. To achieve the level of organised and objective visibility of cyber security risk across the whole of government will require extensive processes, mechanisms and partnerships to be established; a task complicated by the varying levels of cyber maturity, capability and capacity. Key to this will be enabling lead government departments to assess and articulate the macro-cyber security posture of the arms-length bodies and other public sector organisations within their purview.

1 HMG; Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy; March 2021

2 HMG; ‘National Cyber Strategy’; December 2021

7. Achieving this aim will make government a significantly hardened target. As well as enabling government to protect its data and operate without undue disruption, it will ensure that government organisations are structured and organised to manage unknown and more sophisticated threats when they do arise.

Strategic pillars and transformational proposals

8. Government's approach to achieving this aim is centred around two complementary strategic pillars, each underpinned by a transformational proposal that will unlock and drive improvements across government.
9. The first is to **build a strong foundation of organisational cyber security resilience**; ensuring that government organisations have the right structures, mechanisms, tools and support in place to manage their cyber security risks.
10. This will be underpinned by the adoption of the National Cyber Security Centre's (NCSC) Cyber Assessment Framework (CAF) as the assurance framework for government, with government specific CAF profiles that articulate the outcomes required by government organisations in order to proportionately respond to the varying threats to their most important functions. Objective verification by independent auditors will be a requirement for central government departments, although it will be for lead government departments to adapt and apply such an approach in a way that is most appropriate for the public sector organisations within their scope. As well as improving visibility of cyber security risks, adopting the CAF provides a common framework for government to more effectively understand and manage them.
11. The second is to 'defend as one'. Recognising that the scale and pace of the threat demands a more comprehensive and joined up response, government will harness the value of sharing cyber security data, expertise and capabilities across its organisations to present a defensive force disproportionately more powerful than the sum of its parts.
12. This will be underpinned by the establishment of a Government Cyber Coordination Centre (GCCC). As a joint venture between the Government Security Group, the Central Digital and Data Office and the NCSC, the GCCC will work to better coordinate operational cyber security efforts, transforming how cyber security data and threat intelligence is shared, consumed and actioned across government.



Objectives

13. These pillars are supported by five objectives that set the dimensions of cyber resilience, providing a consistent framework and common language that can be applied across the whole of government.



Manage cyber security risk



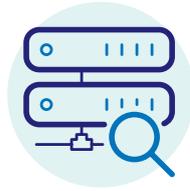
- 14. In order to manage cyber security risk, government organisations will be able to identify, assess and understand them. The foundation of this lies in the visibility and understanding of assets, their vulnerabilities, and the threat to them - whether internal to an organisation or emanating from its supply chain. Clear accountability and robust assurance will ensure that risk owners are aware of the risks they have the responsibility to manage, and that they are doing so appropriately.
- 15. Information about vulnerabilities will be shared across government to provide a central view of critical vulnerabilities that will enable cross-government risks to be identified and managed, facilitating rapid assessment, coordination and mitigation at scale.

Protect against cyber attack



- 16. The protective stance of individual government organisations will be inextricably linked to their assessment and management of risk. While it will never be possible to protect against all attacks, those accountable will be able to demonstrate that they have appropriately considered those risks and responded accordingly.
- 17. Proportionate cyber security measures will be embedded in the technology government uses, and technology and digital services will be correctly designed, configured and managed. Crucially, government will develop its shared capabilities, tools and services to address common cyber security issues at scale, improving cyber security across the whole of government as well as driving efficiency and value for money.
- 18. At the heart of this is government's responsibility to protect the data it handles. As well as appropriately classifying information, government will handle and share it in a way that is commensurate with the risks it presents, using the appropriate IT systems.

Detect cyber security events



19. Building on the foundation of risk management and commensurate protective measures, government will develop its capability to detect cyber security events across every part of its estate to ensure that risks can be mitigated before they critically impact government functions and services.
20. This means having the capability to monitor systems, networks and services to detect cyber security events before they become incidents. Enhanced coordination will enable government to have the agility to use these data inputs to detect at pace and scale, facilitating coherent responses as well as providing the capabilities to detect more sophisticated attacks.

Minimise the impact of cyber security incidents



21. While effective risk management, appropriate and proportionate protective measures and enhanced detection capability will make government a considerably hardened target, government organisations will still be impacted by cyber security incidents.
22. Government will therefore be fully prepared and able to respond to cyber incidents with the capability to restore affected systems and assets and resume the operation of its functions and services with minimal disruption. A critical component of this will be establishing the mechanisms to test and exercise incident response plans, both organisationally and across government, as well as the ability to learn lessons from incidents and 'near misses'.

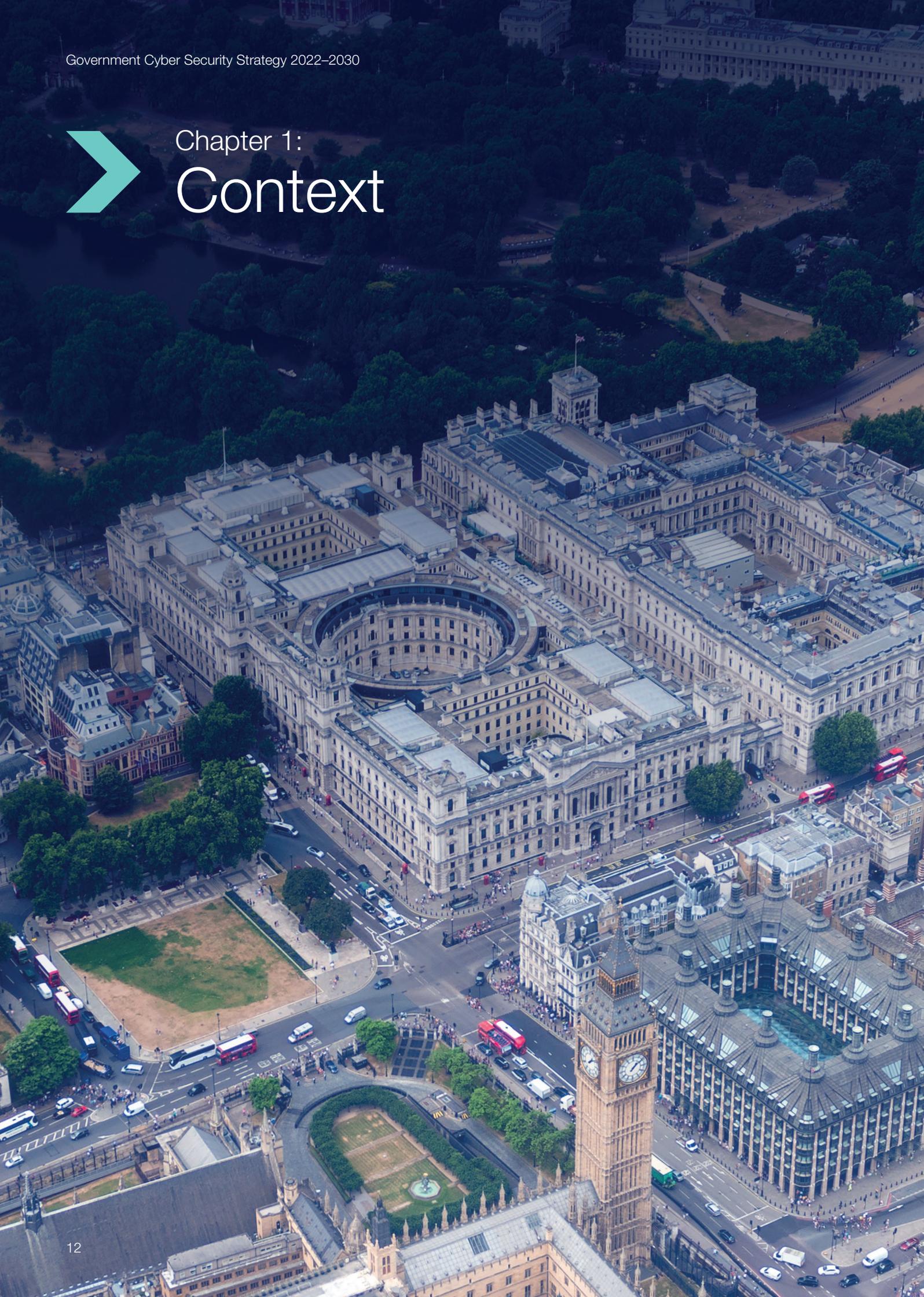
Develop the right cyber security skills, knowledge and culture



23. Achieving this strategy's vision and aim will not be possible without cultivating the required cyber security skills and knowledge, as well as fostering a cultural shift in cyber security across the whole of government.
24. Government will have a comprehensive understanding of its cyber security skills requirements and will incentivise and promote government cyber security careers. As well as formal career pathways that align with the UK Cyber Security Council, working towards the adoption of a single pay framework for the cyber profession will enable government to more effectively attract, develop and retain those skills, providing a sustainable government cyber security profession.
25. The need for sufficient cyber security skills and knowledge extends beyond technical cyber security roles to the breadth of professional functions that must give adequate consideration to cyber security. From the Digital, Data and Technology (DDaT) profession through to government's commercial and legal functions, sufficient cyber security knowledge and awareness will ensure that cyber security is actively considered wherever necessary.
26. Fundamentally, this strategy recognises the importance of cultivating a cyber security culture that empowers its people to learn, question and challenge to drive continuous improvement. This begins with improving cyber security awareness and knowledge across all public sector workers, building on these foundations to create a positive cyber security culture that promotes and empowers its people to proactively engage on organisational cyber security risks. Getting this right is the key to sustainable change.



Chapter 1: Context



The importance of government cyber security to national resilience

1. The Integrated Review of Security, Defence, Development and Foreign Policy³ (Integrated Review) brings national resilience to the fore of the UK's approach to its future security and prosperity. As global dependency on digital services and connectivity grows, the need for strong cyber resilience will become increasingly critical to this national effort.
2. The National Cyber Strategy⁴ pursues this objective, seeking to firmly establish the UK as a democratic and responsible cyber power, able to protect and promote its interests as a sovereign nation in a world fundamentally shaped by technology.
3. The UK's legitimacy and authority as a cyber power is however dependent upon its domestic cyber resilience; the cornerstone of which is its public sector. Government has a fundamental duty to deliver functions that maintain and promote the UK's economy and society, from the delivery of public services through to the operation of national security apparatus. These functions must be able to operate without undue disruption to maintain the trust and public confidence needed to enable the UK to prosper and, in turn, exercise influence beyond its borders.

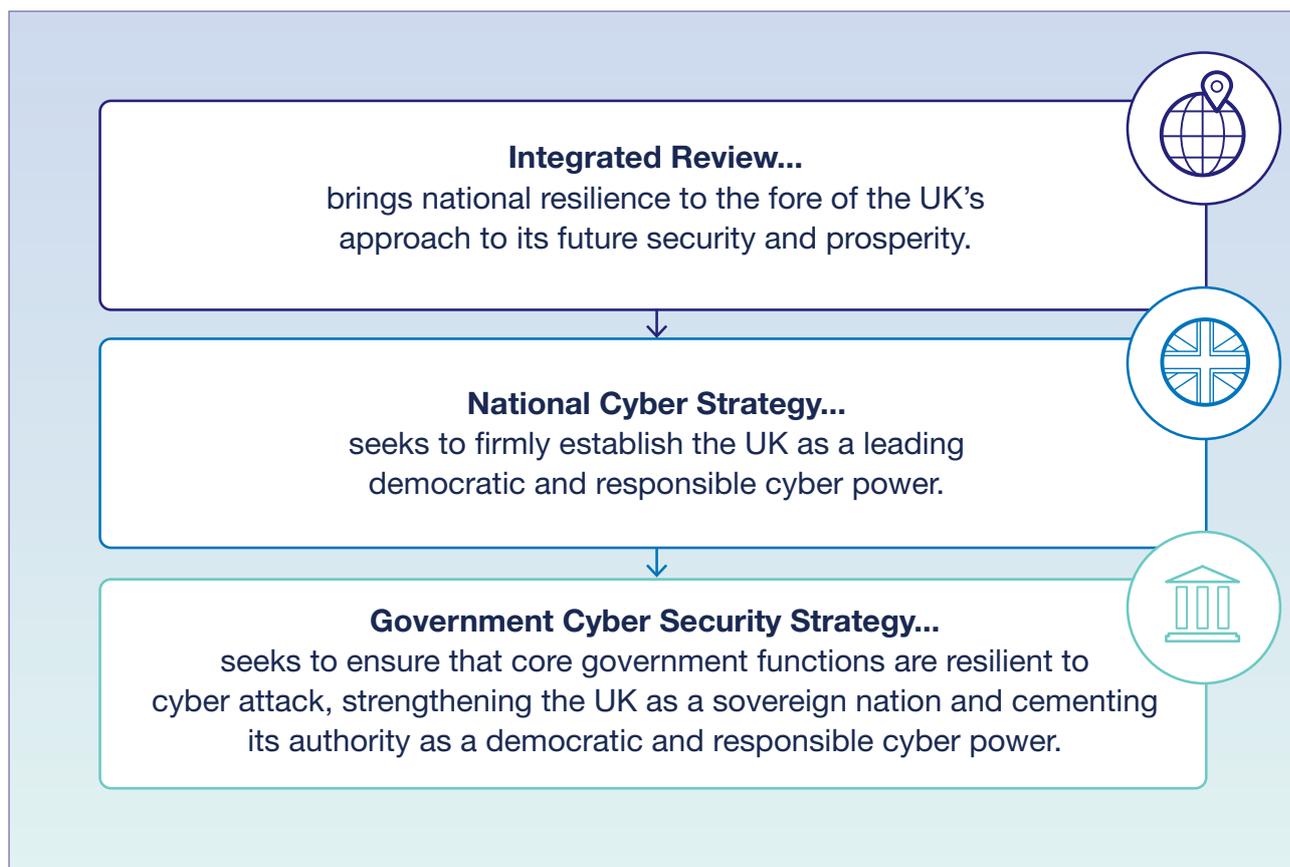


Figure 1: Strategic context

³ HMG; 'Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy'; March 2021

⁴ HMG; 'National Cyber Strategy'; December 2021

The challenges and opportunities for government

Progress

4. Government has made significant progress in the last five years. As well as the establishment of the National Cyber Security Centre (NCSC) as the UK’s national technical authority for cyber security, the creation of the Government Security Group and the Central Digital and Data Office in the Cabinet Office has provided central leadership of cyber security and digital transformation at the heart of government.
5. The introduction of the Minimum Cyber Security Standards for government in 2018,⁵ and the underpinning annual ‘Health Check’, signalled clear requirements for cyber security controls and behaviours, and improved government’s understanding of its cyber security posture. This understanding has been further enhanced by the introduction of the GBEST scheme for government which provides an advanced, intelligence-led simulated attack framework to assess an organisation’s cyber resilience.
6. The need for cyber security is being taken increasingly seriously at the highest levels, with more regular reporting to boards and government audit and risk committees consistently highlighting it as a critical risk. This recognition has been reflected through continued and significant investment in government cyber security through the National Cyber Security Programme and investment in addressing legacy IT across the government IT estate.
7. The NCSC continues to scale and develop its Active Cyber Defence programme to tackle cyber attacks in a relatively automated and scalable way, as well as growing the number of shared services and capabilities offered to improve government’s cyber resilience. The introduction and expansion of government’s SECRET IT platform has also transformed how government manages more sensitive information and enhanced collaboration across classifications.

FOCUS ON: A holistic approach to government security



Cyber security is a critical component of a broader suite of security disciplines and practices that are required to protect government’s assets and ensure that government’s functions can operate without undue disruption. These security practices intersect and must all be given appropriate consideration as part of an organisation’s holistic business risk management approach.

In recognition of this, in September 2021 the government published the Government Functional Standard GovS 007: Security⁶ (Security Standard). Government Functional Standards are a suite of management standards to guide people working in and with the UK government. The Security Standard represents an up-to-date view of the security arrangements government organisations should have in place to ensure government is able to function effectively, efficiently and securely.

The Security Standard brings together and clarifies what needs to be done, and why, with flexibility for organisations about how it is met in practice. It sets expectations for the governance, roles and accountabilities and practices needed, as well as providing a stable basis for assurance, risk management and capability building.

5 Cabinet Office; ‘Minimum Cyber Security Standard’; June 2018

6 Cabinet Office; ‘Government Functional Standards GovS 007: Security’, September 2021



8. Steps have been taken to address the cyber security skills challenge in government with the creation of the government security profession. The development of a cyber career framework - that sets out standard skills and knowledge requirements across government, directly linking to a cyber learning curriculum and a cyber pay offer - is attracting, developing and retaining cyber security talent. The government's early talent offer is also growing talent from within, through apprenticeships and fast stream schemes.
 9. The criticality of cyber security is also being recognised beyond the UK government. Public sector organisations are making strides, with the health sector being a notable example. The devolved governments also have well established cyber resilience strategies and action plans driving significant cyber security improvements in the sectors for which they have devolved responsibility.
- ## The challenge
10. Yet, while government's recognition and understanding of cyber security risk has evolved, it has also highlighted the gap between where government cyber resilience is now and where it needs to be. This gap is brought into sharp focus by the challenges departments have faced in achieving the Minimum Cyber Security Standards.
 11. The level of maturity, capability, investment, and security understanding across government organisations remains inconsistent and the size and complexity of government's digital estate, including the presence of legacy IT, makes the challenge significantly more complicated. The size and diversity of the government's supply chains makes it difficult to manage risks, with long-term contracts stifling innovation. Further to this, complex governance structures, insufficient accountability, levers and incentives, as well as underdeveloped mechanisms to effectively share information and capabilities significantly impacts government's visibility of cyber risk, as well as its ability to drive change at the scale and pace required. This is made more challenging by limited resources.
 12. Meeting the scale of the challenge is also dependent on people. However, in the context of a national cyber security skills shortage⁷, government struggles to compete with the private sector to attract and retain the required cadre of diverse and skilled cyber security professionals, despite its positive efforts to date. This extends beyond technical cyber security skills, including the broad range of professional functions that require cyber security knowledge and awareness. Moreover, internal competition over cyber professionals in government too often comes at the expense of knowledge retention and sustained change.

⁷ Ipsos MORI / DCMS; 'Cyber Security Skills in the UK Labour Market 2021'; March 2021

- 13. The need for improved cyber resilience is becoming more acute given the increasingly digital world. While ubiquitous digital connectivity and mass data generation create significant opportunities for government to improve its services and functions for the benefit of the UK and its citizens, it also introduces significant cyber security risks. As government's reliance on digital services grows - from the use of digital products and services to the migration of government data and services into the cloud - greater dependency is placed on those outside of government, often with footprints extending beyond the UK. The COVID-19 pandemic exacerbated these risks as well as fundamentally changing how government works, with hybrid working becoming the norm.
- 14. Such interconnectivity and dependency significantly increase the risk of malicious attack, with the potential to jeopardise trust and public confidence in government.

The threat

- 15. As cyber security risks evolve, so do the threats posed by malicious actors - from nation states to cyber criminals. While their capabilities and techniques continue to evolve and diversify, the commoditisation of offensive cyber tools and services increasingly lowers the capability threshold for anyone with the intent to disrupt or undermine the functioning of government.
- 16. At the same time government remains an attractive target for a broad range of malicious actors, with approximately 40% of the 777 incidents managed by NCSC between September 2020 and August 2021 affecting the public sector⁸. This is expected to continue to grow.

FOCUS ON: The impact of ransomware



In 2020, both Redcar & Cleveland and Hackney councils were hit by ransomware attacks. Despite the relatively small sizes of these organisations the impact on critical public services was disproportionate and acute. These attacks are not an anomaly but part of a significant upward trend.

Ransomware does not rely on the exploitation of new or novel vulnerabilities. Indeed, the barrier to such exploitation has been significantly lowered with the rise of ransomware as a service (RaaS), allowing 'customers' to purchase capabilities that were once the preserve of more capable actors.

While use of ransomware rises, the costs of remediating the impact of ransomware attacks remain significant. This only reinforces the need for strong cyber resilience and strengthens the case for appropriate cyber security prioritisation and investment, to mitigate the risks before they turn into serious incidents.

⁸ NCSC; 'NCSC Annual Review 2021'; November 2021

17. The threat from nation state actors is of considerable concern, with nearly half of nation state activity being targeted at governments across the world, with the UK being the third most targeted country behind the USA and Ukraine⁹. Equally the dramatic rise of ransomware attacks and recent high-impact incidents demonstrate both the scale of impact and the diversity of organisations affected, from government departments to wider public sector organisations. The targeting of healthcare, education and other essential services continues to demonstrate the severity of such cyber attacks, which not only cause significant disruption to the delivery of essential public services, but can also pose a real risk to public safety.

The opportunity

18. Although government faces significant challenges it also has many attributes and strengths. With such organisational diversity comes a wealth of capabilities, knowledge and data that must be developed and harnessed. Government must also take full advantage of the benefits that digital transformation brings, to drive innovation, analytical understanding and the scaling of capabilities.
19. Cyber resilience remains a cost effective and impactful lever against the cyber threat. Government organisations must therefore build from these foundations to improve their cyber resilience. Most crucially, government needs to harness its collective strength, bringing together and developing its capabilities to present a stronger defensive force which can match the ever-evolving cyber risk landscape.

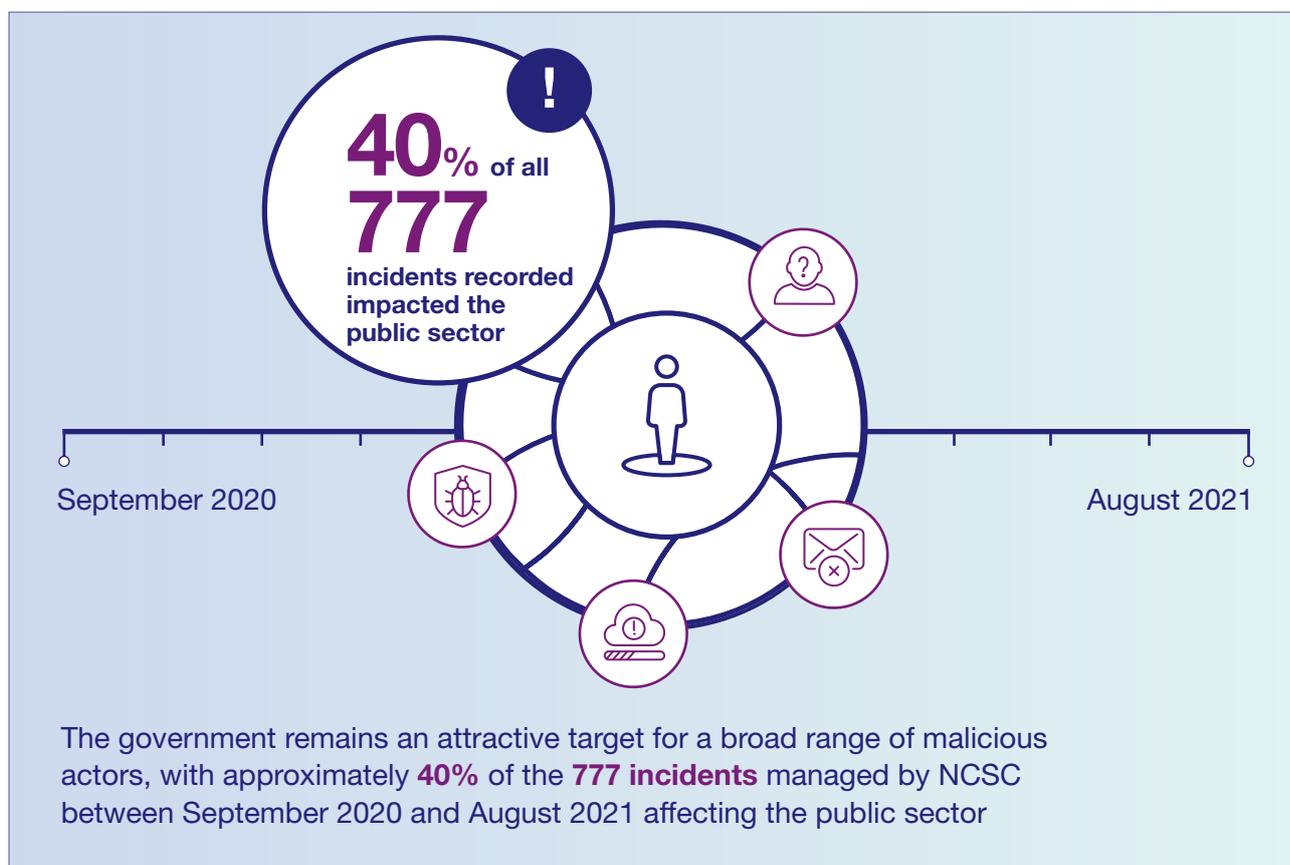


Figure 2: Cyber incidents affecting the public sector



Chapter 2: Approach



Vision and Aim

20. Government has a duty to deliver functions that maintain and promote the UK's economy and society. These functions must be able to operate without undue disruption to maintain the trust and public confidence needed to enable the UK to prosper. It is therefore imperative that these functions are sufficiently resilient to continuously evolving cyber threats.
21. To realise this vision, government will have the mechanisms in place to identify and manage known risks in order to maintain a proportionate and effective level of cyber security across all government organisations.
22. This will mean that government's OFFICIAL systems will be hardened against known vulnerabilities and improper security practices will no longer unduly expose government to easily preventable attack methods, with information above OFFICIAL being appropriately protected on higher-classification systems. Such a position, and the understanding that is derived from it, will mean that government is aware of attacks to its systems and can effectively maintain its cyber resilience.
23. Achieving this aim will make government a significantly hardened target - forcing adversaries to work harder while enabling government functions to operate without undue disruption, in turn cementing the UK's authority as a democratic and responsible cyber power.

VISION:



This strategy seeks to ensure that core government functions - from the delivery of public services to the operation of National Security apparatus - are resilient to cyber attack, strengthening the UK as a sovereign nation and cementing its authority as a democratic and responsible cyber power.

AIM:



Government's critical functions to be significantly hardened to cyber attack by 2025, with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030.

Unpacking the Aim:

The aim of the strategy sets out a clear ambition for government. Progress towards it will be driven by an understanding of risk. This means identifying areas of particular risk and prioritising the most impactful interventions to ensure that government can rapidly improve its cyber resilience.

The strategy's aim focuses on the management of 'known vulnerabilities and attack methods'. This focus refers to more than publicly disclosed security flaws, also accounting for the improper security practices and behaviours that unduly expose an organisation to cyber attack.

Good cyber security practices are well established and their adoption will mitigate the vast majority of cyber attacks. As well as dramatically improving an organisation's cyber resilience, adopting well-established cyber security practices will ensure that an organisation is structured and organised to manage unknown and more sophisticated threats when they do arise.

FOCUS ON: Cyber Resilience



Cyber resilience refers to the ability of an organisation to maintain the delivery of its key functions and services and ensure the protection of its data, despite adverse cyber security events. Given government's fundamental duty to deliver functions and services that maintain and promote the UK's economy and society, cyber resilience lies at the very heart of this strategy.

The scope of this strategy

Core government functions are delivered by many diverse public sector organisations, including government departments, arms-length bodies, agencies, local authorities, and other wider public sector organisations. This strategy therefore considers all such public sector organisations. In doing so it recognises the breadth, complexity and varying degrees of autonomy of these organisations, particularly those beyond central government.

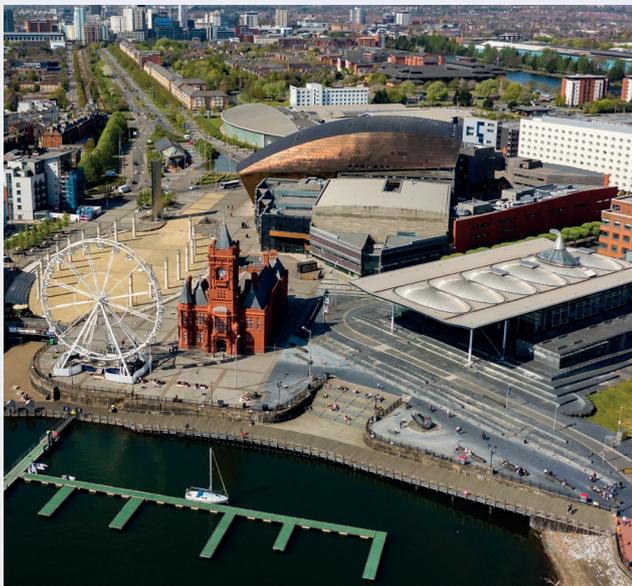
Lead government departments are best placed to understand the unique characteristics of the organisations within their purview, including their arms-length bodies and agencies, as well as other government bodies and wider public sector organisations. The focus is therefore placed on enabling lead government departments to assess and articulate the macro cyber security posture of those organisations, driving improvements as necessary.



The devolved governments

While cyber security - within the wider remit of national security - is a reserved matter, responsibility for public services within Scotland, Wales and Northern Ireland is devolved to the respective devolved governments. This includes the devolution of health and social care, education and transport, amongst others. Devolved governments therefore have the responsibility to ensure that those services are resilient to cyber risks.

While these matters are devolved, the UK as a whole shares the vision set out in this strategy. The UK government will therefore continue to work collaboratively with the devolved governments to ensure that collective issues are addressed in partnership, with appropriate information and support being shared to maintain the resilience of the UK.



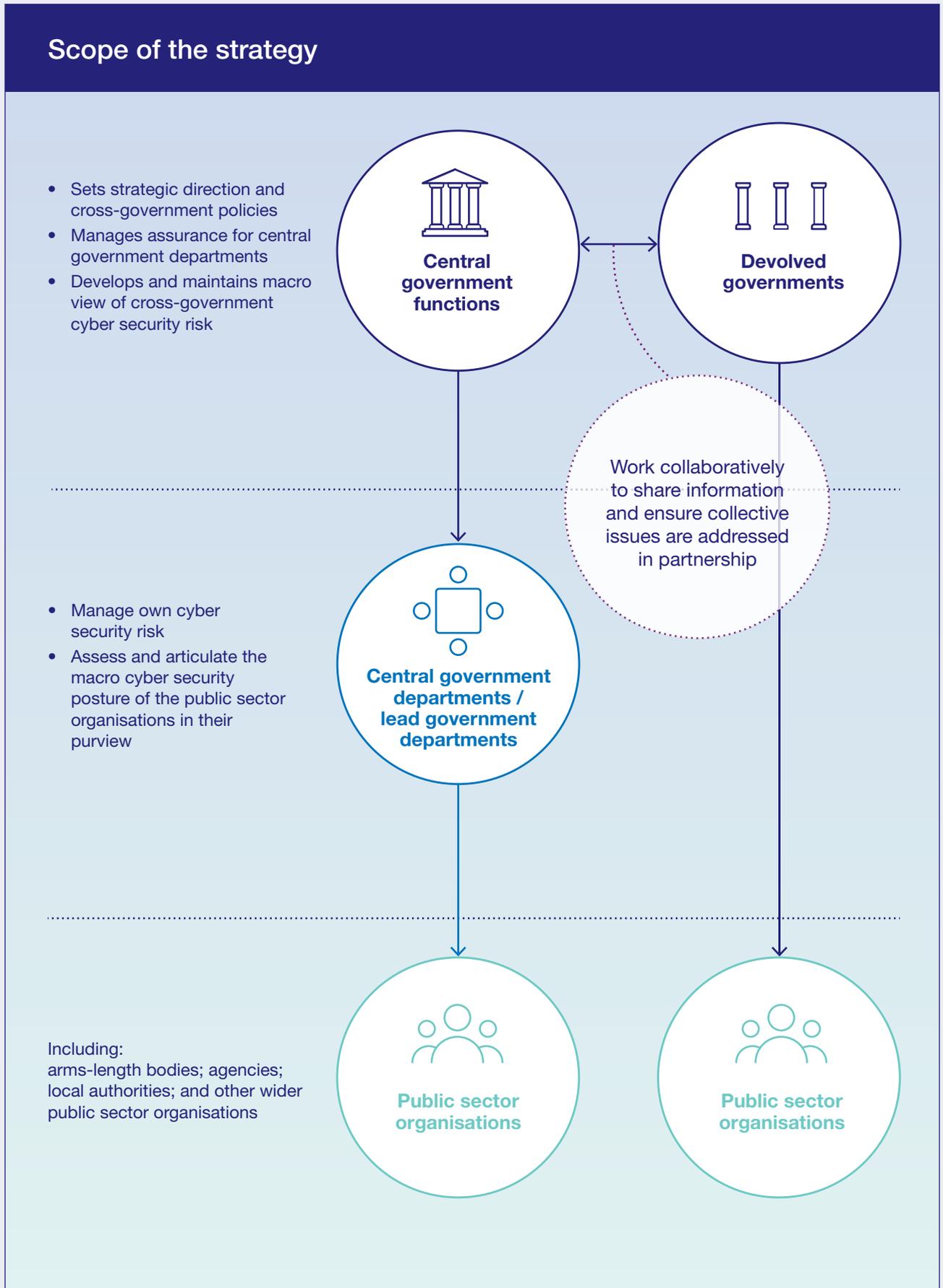


Figure 3: Scope of the strategy

Pillars

24. Achieving this vision and aim will require a step-change in how government approaches cyber security. As well as continuing to strengthen organisational cyber resilience, government will 'defend as one' to ensure

that it can meet the scale of the challenges it faces. This strategy therefore centres around two core and complementary strategic pillars which define and drive the government's approach to cyber resilience.

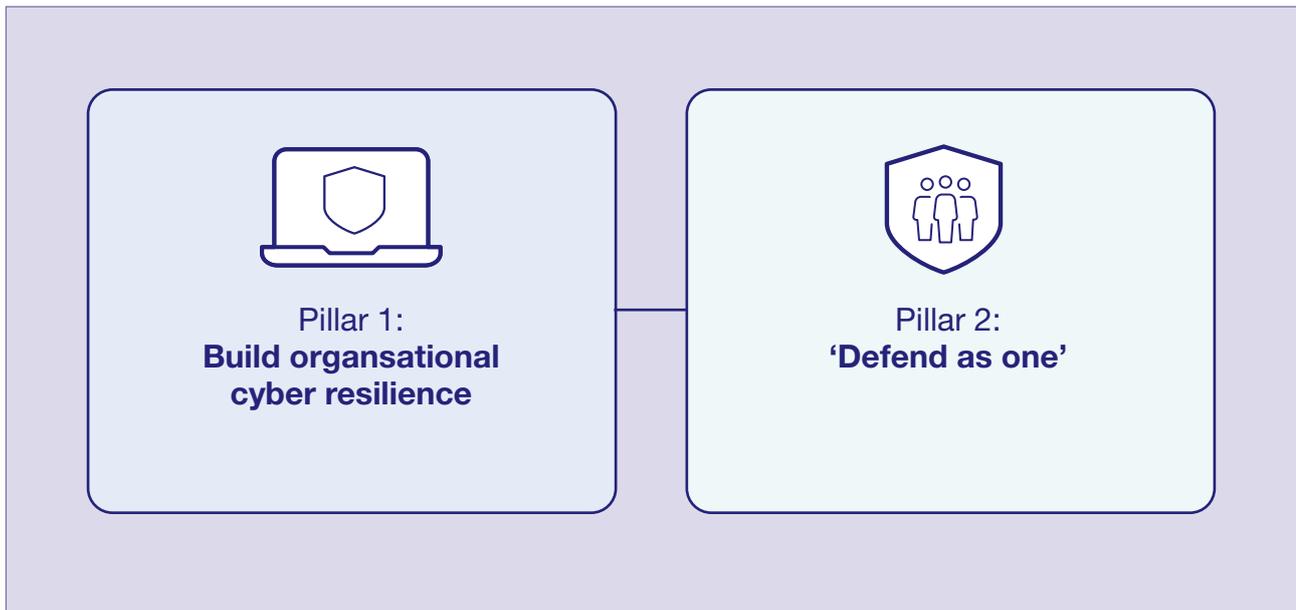


Figure 4: Strategic pillars



Pillar 1: Build a strong foundation of organisational cyber security resilience

25. As well as being responsible and accountable for managing their own cyber security risks, government organisations must increasingly recognise their collective responsibility for the cyber resilience of the whole of government. Given that failings of one organisation can have significant implications for many others, it is imperative that all individual organisations build and enhance their cyber security posture, accounting for the risks they face and the criticality of the function they have responsibility for.

26. Government organisations will therefore have the right structures, mechanisms, tools and support in place to ensure that they can manage their cyber security risks. This will be underpinned by genuine accountability, so government has confidence in its cyber resilience, both at an organisational and cross-government level.

TRANSFORMATIONAL PROPOSAL - Enhanced cyber security assurance



Government will adopt the Cyber Assessment Framework (CAF) as the assurance framework for government. The CAF has been developed by the NCSC - the UK's technical authority on cyber security - and represents an industry standard that is used by operators of essential services under the Network and Information Systems regulations¹⁰ as well as more widely across the private sector, including critical national infrastructure (CNI) sectors. Adopting the CAF ensures that government is assessing its cyber resilience in a consistent and comparable way to other organisations that operate the UK's essential services.

Tiered government CAF profiles, underpinned by government-specific cyber threat profiles, will articulate the outcomes required by government organisations in order to proportionately respond to varying threats to their most important functions. Government organisations' assessment of cyber resilience against the relevant CAF profile will be verified by independent auditors. As well as providing an objective assessment of government cyber resilience, independent auditing will highlight critical areas for improvement.

This assurance process will be a requirement for government departments, however it will be for lead government departments to adapt and apply such an approach in a way that is most appropriate for the public sector organisations in their purview. Devolved governments will take a similar leadership role across their areas of responsibility. Crucially, however, lead government departments and devolved governments will be able to articulate the macro cyber security posture of the organisations within their purview with reference to the CAF's objectives to ensure that government cyber resilience is assessed and understood in a consistent and comparable way.

While the CAF will be used as the framework to provide consistent cyber security assurance of government departments, individual departments may continue to use whatever framework they feel is most appropriate to best enable them to manage their cyber security risks. Prominent cyber security frameworks, such as the National Institute of Standards and Technology (NIST) cyber security framework and ISO 27001, are consistent with the CAF, ensuring that assurance reporting requirements do not disturb mature internal cyber security risk management structures and processes.



**Pillar 2:
'Defend as one'**

- 27. While developing a strong foundation of organisational cyber security is critical, the scale and pace of the threat demands a more comprehensive and joined up response. Government will therefore 'defend as one'; harnessing the value of sharing cyber security data, expertise and capabilities across government to present a defensive force disproportionately more powerful than the sum of its parts.
- 28. This means ensuring that all government organisations have timely access to relevant and actionable cyber security data that enhances their ability to manage cyber risks, as well as working collaboratively to better coordinate and target shared government capabilities and services that address common cyber security issues at scale.
- 29. Doing so will have a disproportionate benefit to the cyber security of government. It will also facilitate innovation by coordinating the identification of common cyber security risks affecting government organisations and harnessing government expertise and resources to address those problems at scale.

**TRANSFORMATIONAL PROPOSAL -
The Government Cyber Coordination Centre (GCCC)**



Government will establish a cyber coordination centre to better coordinate operational cyber security efforts across government organisations and truly enhance government's ability to 'defend as one'. Building on successful private sector models such as the Financial Sector Cyber Collaboration Centre (FSCCC), the GCCC will foster partnerships to rapidly identify, investigate and coordinate the response to incidents alongside threat and vulnerability reporting. Key to this will be transforming how cyber security data and threat intelligence is used across government.

Ensuring that such data can be rapidly shared, consumed and actioned will dramatically improve government's ability to 'defend as one' when managing incidents, vulnerabilities and threats at scale.

As a joint venture between the Government Security Group, the Central Digital and Data Office and the NCSC, the GCCC will form strong partnerships with government departments and the devolved governments.

FOCUS ON: Data-driven cyber security



This strategy puts data at the heart of cyber security. The secure use of data - automated and machine readable wherever possible - will inform decision making and drive improvements where required.

Objectives

30. The strategy's pillars are underpinned by five objectives. These set the dimensions of what needs to be considered with regard to cyber resilience, providing a consistent framework and common language that can be applied to the whole of government.

1) Manage cyber security risk:

Effective cyber security risk management processes, governance and accountability enable the identification, assessment and management of cyber security risks - at both the organisational and cross-government level.

2) Protect against cyber attack:

Understanding of cyber security risk informs the adoption of proportionate security measures with centrally developed capabilities enabling protection at scale.

3) Detect cyber security events:

Comprehensive monitoring of systems, networks and services enable cyber security events to be managed before they become incidents.

4) Minimise the impact of cyber security incidents:

Cyber security incidents are swiftly contained and assessed, enabling rapid response at scale.

5) Develop the right cyber security skills, knowledge and culture:

Sufficient, skilled and knowledgeable professionals fulfil all required cyber security needs - extending beyond technical cyber security experts to the breadth of professional functions that must incorporate cyber security into the services they provide - all underpinned by a cyber security culture that promotes sustainable change.



FOCUS ON: A perpetually reinforcing ecosystem



The strategy’s objectives set out the core components of cyber resilience that will guide cyber security efforts across government. These objectives are perpetually reinforced - through the governance and oversight of the strategy, the development and implementation of central and shared interventions, and through government cyber security assurance.

As well as providing a consistent framework and common language for cyber security across government, establishing such a reinforcing ecosystem will provide a coherent and comprehensive picture of government cyber resilience that will continually refine and drive improvements where they are most needed.

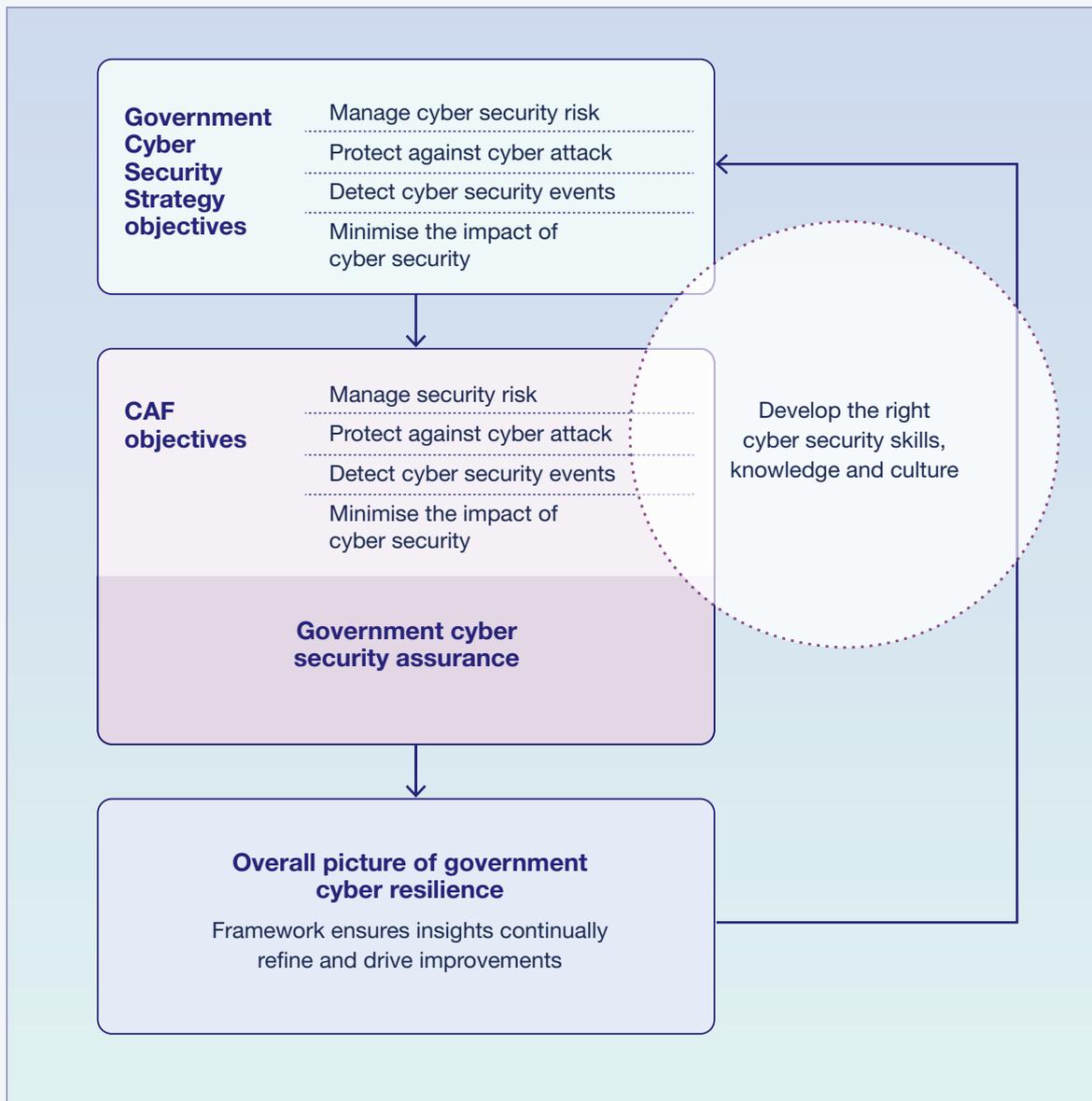


Figure 5: A reinforcing ecosystem

The Government Cyber Security Strategy

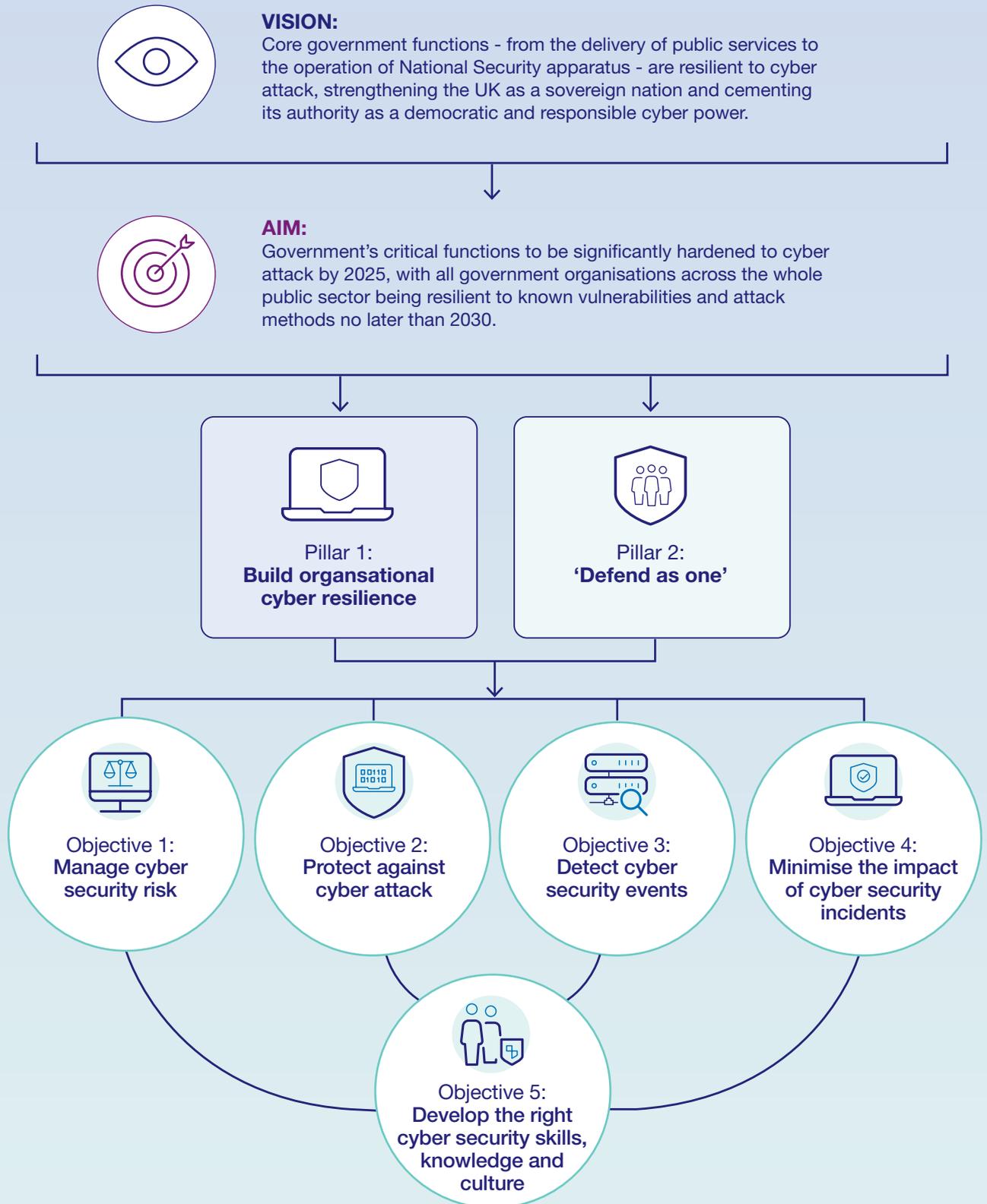


Figure 6: The Government Cyber Security Strategy



Chapter 3:

Managing cyber security risk



31. Management of risk lies at the heart of this strategy. It is only when risk is understood that mitigations can be applied and investment prioritised. Accurate risk information is therefore critical to enabling accountable individuals to make effective risk-based decisions. It also provides the system-wide view needed to address systemic risks and to drive scaled interventions.

Objective 1:
**Government will manage
cyber security risk**



Government organisations will have risk management processes, governance and accountability in place to enable the effective identification, assessment and management of their cyber security risks, with sufficient overarching visibility to effectively manage systemic risk.

32. In order to manage cyber security risks, government organisations will be able to identify, assess and understand them. The foundation of this lies in the visibility and understanding of assets held and operated - whether that be infrastructure, digital services and applications, or data - and the threat to them. This visibility is the foundation from which an accurate assessment of risk can be derived. Clear accountability and robust assurance will ensure that risk owners are aware of the risks they have the responsibility to manage, and that they are doing so appropriately.

Governance and accountability

Outcome 1:

Government has established governance arrangements with clear accountability enabling effective management of cyber risks at all levels of government

33. To drive government risk management to the appropriate level requires changes and enhancements to governance and accountability across government. Cyber risk will be seen as an integral component of business risk and resilience management, with effective organisational cyber security management structures that enable government organisations to fully understand and account for the risks they own. This includes having established roles and responsibilities for their systems and services and clear channels for communicating and escalating risks to ensure that decision makers have the visibility required to make effective decisions. Most crucially, it requires clear and transparent accountability up to Accounting Officers and the executive board, to ensure that decision makers are informed and empowered to express their organisation’s risk position, as well as be held accountable for their risk decisions.

34. Lead government departments are best placed to understand the unique characteristics of the organisations within their purview and will construct the mechanisms to assess and articulate the macro cyber posture of those organisations, putting in place the appropriate governance arrangements to drive required improvements.



35. While Accounting Officers are responsible for their organisation’s risk, transparent central governance structures will maintain oversight and responsibility for cross-government cyber security risk, ensuring that systemic risks are identified and managed.

Assets and vulnerabilities

Outcome 2:

Government has comprehensive visibility and understanding of its digital assets enabling it to identify and manage vulnerabilities and the cyber security risks they present

36. Without comprehensive visibility of government's IT, digital and data assets, as well as users, cyber security risks go unrecognised and unmanaged. Not only does this limited visibility restrict an organisation's ability to protect its estate, it reduces government's ability to identify and act on aggregated and systemic risks that could have a devastating impact on the functioning of government.
37. All government organisations will therefore have an active and automated asset discovery and management method in place to continuously determine what systems, hardware and software they own and operate - including those provided by suppliers - so that the potential risks to them can be managed. As government organisations migrate to cloud services they should take advantage of the available asset management tools which make it significantly easier for an organisation to know what it owns and operates, how they are configured, and where they are vulnerable.
38. Vulnerabilities in technology and digital services are introduced or discovered almost constantly. Government's approach to managing these will, therefore, reflect this evolving landscape. Government will have the mechanisms in place to enable vulnerabilities to be rapidly identified, assessed and managed. This involves providing a clear path for anyone - whether a public sector employee, a commercial entity or a private individual - to highlight potential vulnerabilities, and robust vulnerability management programmes to be in place across all government organisations to ensure identified vulnerabilities are effectively managed across their IT estate.
39. Information about critical vulnerabilities will be securely shared across government, to ensure that all government organisations can take appropriate action. Effective information sharing will also provide a central view of critical vulnerabilities which will develop government's visibility of dependencies across its systems and services, enabling the identification and management of more systemic issues, as well as facilitating rapid assessment, coordination and mitigation at scale.

FOCUS ON: Cross-government vulnerability reporting service



Government will develop a coherent and joined up cross-government vulnerability reporting service. This will enable the mature handling of, and response to, vulnerabilities which have the potential to impact government.

Security researchers and members of the public will be able to easily and securely report vulnerabilities they identify on the government digital estate. Reports will be triaged and the appropriate government organisation will be notified of valid vulnerabilities received. Through this service government organisations will be able to accelerate their ability to find and fix vulnerabilities before adversaries can exploit them.

By providing this capability centrally, government will, for the first time, be able to holistically tackle cyber security vulnerabilities at scale and pace across the public sector.

Data assets

Outcome 3:

Government has comprehensive visibility of the data it handles and shares so that it can appropriately assess and respond to the risks it presents

40. As well as IT assets, government organisations will have comprehensive visibility over their data assets. From personal data to classified information, data underpins all government IT and services and will be protected proportionate to the risk and in compliance with data protection legislation. Government organisations will therefore have a mature understanding of what data assets they handle, how they are stored or hosted, and where they are shared, so they can adequately assess the risks they present and ensure that sufficient protections are put in place to manage them.

Supply chain risk

Outcome 4:

Government understands and manages risks emanating from commercial suppliers

41. Commercially provided products and services play an integral part in delivering government's functions and services. As government supply chains become increasingly expansive and interconnected, vulnerabilities in suppliers' systems, and in the products and services they deliver, present increasingly attractive opportunities to adversaries seeking to gain access to government networks. Recognising this growing risk, government will take steps to better understand its dependencies on suppliers and ensure that their products and services are integrated into government systems in a way that takes full account of their impacts on security and resilience. In doing so, government will be an exemplar in the procurement and deployment of commercial products and services, becoming a stimulus to improve the broader ecosystem of such suppliers across the UK.
42. Central mapping of government's critical and common suppliers will enable the identification and coordinated management of systemic and aggregate supply chain risks to government. Supply chain cyber security principles will establish clear requirements for these suppliers, with the expectation that they provide transparent statements of adherence. Government will also make full use of its established commercial relationships and aggregate spending power to ensure that its key suppliers deliver on these principles. As well as reinforcing appropriate and proportionate cyber security controls and behaviours, such central oversight will promote standard requirements and provide shared assurances that will reduce duplication and drive efficiencies for both government organisations and their suppliers.

43. While such action will significantly raise the expectations placed on critical and cross-government suppliers, requirements should also be proportionate and robust for smaller and more bespoke suppliers, building from Cyber Essentials as a foundational tool to gain confidence that relevant suppliers have appropriate protections in place. Alignment between commercial and security functions will ensure that cyber security is part of every procurement process, enabling commercial teams to clearly articulate the cyber security requirements based on an understanding of risk. Cyber security requirements in government procurement frameworks and contracts will be strengthened, ensuring that commercial arrangements are risk based and consistent with robust clauses relating to the identification and management of subcontractors. This will make it easier to procure tools and services with appropriate security by default.
44. Improved understanding of suppliers and their dependencies will also enable government to better respond to cyber security incidents that emanate from the supply chain. Such understanding will provide oversight of cross-government impacts and enable more focused and efficient engagements with the suppliers, ensuring that any incident is managed swiftly and efficiently. The GCCC will play a critical role in facilitating this.

FOCUS ON: Cyber security in government contracts



Government is developing security schedules that can be easily applied to a variety of common procurement scenarios - from bespoke builds deployed on third party infrastructure to generic consultancy agreements. These schedules will support government organisations in requesting proportionate cyber security measures in government contracts, as well as conducting regular assurance against them.

These security schedules will be made available across government so that government organisations have access to relevant and manageable security clauses. This will ensure that appropriate security measures - proportional to the risk - are included in all government contracts.

Threat information

Outcome 5:

Government understands the threat it faces relative to its functions in order to plan appropriate mitigations, at both an organisational and cross-government level

45. As well as government's ability to understand what it has and how it is vulnerable, it will also understand the threat to it in order to arrive at an accurate assessment of risk. The seamless collation and dissemination of threat information is crucial as it provides those responsible for defending systems and networks with the strategic, tactical, technical and operational detail needed to predict and defend against attacks.
46. Government organisations will therefore have the ability to receive and utilise such threat information, as well as the capability to generate it from the monitoring of their system in a systematised manner - automated wherever possible. Threat information generated locally will be enhanced by the coherent use of government and private sector threat information.
47. Central mechanisms will be in place to facilitate more comprehensive, targeted and, where possible, automated, threat information sharing across government. This will enable government organisations to make effective prioritisation decisions based on up-to-date information.

FOCUS ON: Countering Threats



The National Cyber Strategy sets out the UK's objective to detect, investigate and share information on state, criminal and other malicious cyber actors and activities in order to protect the UK, its interests and its citizens.

This will involve:

- maintaining a comprehensive understanding of the cyber capabilities of state, criminal and other malicious cyber actors and their strategic intent towards the UK;
- ensuring that the most serious state, criminal and other threats are routinely and comprehensively investigated, drawing on all sources of information and bringing together expertise across government, law enforcement and the private sector; and
- enabling information and data on the threat to be routinely shared at scale and pace.

Government organisations will be both a customer and contributor to these efforts, taking full advantage of the knowledge that exists across the UK to provide a deeper understanding of the threat.

Cyber security data

Outcome 6:

Government organisations have timely access to relevant and actionable cyber security data that enhances their ability to make effective risk management decisions

48. Cyber security data is an invaluable commodity, including essential information about the threats and vulnerabilities that government needs to understand in order to effectively manage the risks it faces. The need for all government organisations to have access to relevant and actionable cyber security data is paramount, but while some parts of government are incredibly data rich, others do not have access to the cyber security data that they need to make effective risk-based decisions.
49. As well as making better use of existing cyber security data - from sources such as cross-government services, organisational systems and endpoint logging and monitoring - greater value will be extracted from analysis of aggregate data, with enhanced dissemination of critical insights to those who need to respond to them. The newly established GCCC will play a fundamental role in facilitating this, by ensuring that targeted cyber security data is shared across government - in a way that is appropriate to its classification and legal status - and supporting organisations to effectively consume it.



Government cyber security assurance

Outcome 7:

Government cyber security assurance provides government with the visibility it needs to make effective decisions and the confidence that it has appropriate cyber security measures in place to manage the risks to its functions

50. Cyber security assurance is needed to provide visibility of cyber security risk across government organisations as well as the confidence that those risks are being appropriately and proportionately managed. To achieve this, a government cyber security assurance process will provide consistent and independently verified assurance against government CAF profiles.¹¹ Focusing on an organisation’s most important functions, including critical national infrastructure, it will provide an objective way of assessing whether an organisation’s cyber security assessment and management of cyber security risk is proportionate and within accepted risk tolerances. This assurance process will be further verified and augmented through real world testing and exercising, such as penetration testing and red teaming. Outcomes of assurance activities will be machine readable wherever possible, facilitating automated analysis of the impact on cyber security.



51. While these assurance processes will be mandated for central government departments, it will provide a model that lead government departments and devolved governments may adapt and apply across the public sector organisations in their purview.



52. The visibility over government’s cyber security posture provided by this assurance will give government the overarching confidence that cyber security risks to its functions are being managed sufficiently. It will also highlight common issues and challenges at scale, enabling cost effective and targeted intervention.

¹¹ See ‘Transformational proposal: Enhanced cyber security assurance’ for more detail

Private sector and international partnerships

Outcome 8:

Strategic partnerships with the private sector and international partners are further embedded to enhance proactive defence at a global scale

53. Government relies on partnerships with the private sector and international allies to strengthen its cyber resilience. This influence spans from the third-party products and services that government procures and deploys through to the development of new technologies and the future governance of cyberspace.
54. Given the fundamental role that private sector partners have in the development, operation and delivery of government functions, it is crucial that critical cyber security challenges are tackled collaboratively. Government will therefore continue to develop its partnerships with private sector organisations and academia to enhance its resilience across all aspects of security; building trusted relationships and shared outcomes.
55. As highlighted in the National Cyber Strategy, the cyber domain transcends international boundaries. Sharing knowledge and expertise with international allies will increase collective ability to understand and defend against common adversaries, in turn strengthening collective and global cyber resilience. Government will continue to build partnerships with its allies to achieve shared objectives.





Chapter 4:

Protecting against cyber attack



56. Protecting government effectively from cyber attack is dependent on its understanding of risk. Directly responding to risks faced will ensure that government is an increasingly hardened target for any adversary.

Objective 2:
Government will protect against cyber attack



Government's understanding of cyber security risk will inform the adoption of proportionate security measures across government organisations, with centrally developed capabilities enabling protection at scale.

57. The protective stance of individual government organisations will be inextricably linked to its assessment and management of risk. While it will never be possible to protect against all attacks, those accountable will be able to demonstrate that they have appropriately considered those risks and responded accordingly.

Secure technology and digital services

Outcome 9:

Government adopts a common approach to ‘secure by design’ to ensure that appropriate and proportionate cyber security measures are embedded within the technology government uses, and that the security of digital services is continually assured throughout their lifecycle

- 58. Government relies on a range of technologies to operate its functions and deliver digital services. These include both commodity and bespoke components that present cyber security risks, which need to be managed through their lifecycle. To do this, government will adopt a ‘secure by design’ framework that will ensure all technology and digital services are planned, procured, designed, built, operated, modified and decommissioned securely, enabling them to be consistently and continuously assured against best practice and robust standards.
- 59. This ‘secure by design’ framework will further enable government to take advantage of industry innovation by enhancing its ability to test, pilot, and deploy commercial tools, services and capabilities that make a marked improvement of government’s security and efficiency.
- 60. The ability to protect against evolving vulnerabilities and threats is constrained by the presence of legacy and vulnerable IT across the government’s IT estate. Government will therefore continue its efforts to manage, upgrade or remove such IT and put the necessary safeguards and ongoing investment in place to ensure government IT is sufficiently secure throughout its entire lifecycle.



FOCUS ON: A 'secure by design' framework for government

The government's 'secure by design' framework will cement 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.

The framework will provide a continuous and iterative process for security, ensuring that there is a consistent, comprehensive and proportionate process to manage cyber security risk through the entire lifecycle, while providing a consistent framework for continuous security assurance. It will ensure that developers of digital services have security experts embedded within their teams to provide continuous security advice, rather than relying on ad-hoc security advice at the end of a project.

This process will be incorporated within the Service Standard¹² and Infrastructure and Projects Authority gated process¹³ to ensure cyber security is an integral part of creating public services. Secure by design blueprints, patterns, design principles and best practices will also be published to ensure that wider public sector organisations have a clear understanding of what is expected for securing the services they design, deliver and operate.

A critical component of government's 'secure by design' approach is ensuring that any technology procured by government has an appropriate level of cyber security. These 'secure by design' principles will therefore be baked into the Technology Code of Practice¹⁴ which, through the government spend controls processes¹⁵, will ensure that all technology used by government is appropriately securable.

12 HMG; 'Service Standard'

13 HMG; 'Infrastructure and Projects Authority: assurance review toolkit'

14 Central Digital and Data Office; 'The Technology Code of Practice'

15 Central Digital and Data Office; 'Digital and technology spend controls'

Cyber security controls

Outcome 10: Government organisations deploy cyber security controls commensurate with their risk profile to ensure that risks to their functions are managed proportionately

- 61. While secure technology provides the foundations of effective cyber security, appropriate and proportionate security controls will also be put in place. While many security controls will be common across all government organisations, such as appropriate access controls, the broader set of requirements will respond to threats faced. outcomes will depend on the application of particular controls which will be clearly signposted to government organisations, alongside appropriate policies and guidance. While lead government departments will be able to apply such an approach in a way that is most appropriate, they will be able to draw from such processes, guidance and support.
- 62. The threats faced by an organisation’s important functions will therefore determine the appropriate CAF profile as part of the government’s assurance process. That CAF profile will define the outcomes required to appropriately manage the risk posed by the threat. Achieving those proportionate
- 63. Higher classification systems provide the additional cyber security controls required to handle information classified above OFFICIAL. These systems are centrally managed and assured to maintain the appropriate level of cyber security.



Figure 7: Appropriate and proportionate access controls



Secure configuration

Outcome 11:

Government technology is appropriately configured, with standard profiles for common technology and architectures being developed and continuously updated

- 64. Technology and digital services are only as secure as their architecture and configuration allow. While adopting a comprehensive ‘secure by design’ approach will address some of this risk, a designer, administrator or user always has a responsibility to appropriately configure a system or service to meet security requirements. Doing so incorrectly can leave systems and data unprotected or easily open to compromise. This risk will become increasingly acute as government continues its digital transformation.
- 65. To reduce this risk, secure by design configuration patterns and capabilities for prominent products and services will be developed in partnership with suppliers and promoted across government to ensure that common products and services are configured correctly. These configurations will be easily auditable, enabling cross-government visibility to identify aggregate risks and respond to identified threats at pace and scale.

FOCUS ON: Secure configuration of government’s productivity suites



Government will work with its primary providers of productivity suites to further develop baseline security configurations for government organisations to follow and adapt. Doing so will ensure that all government organisations understand how to configure their productivity suites to provide a baseline level of cyber security, which will dramatically reduce common risks caused by misconfiguration.

Shared capabilities

Outcome 12:

Shared capabilities, tools and services tackle ‘common’ cyber security issues at scale

- 66. A core component of this strategy’s ‘defend as one’ pillar is the necessity of harnessing shared capabilities, tools and services to disproportionately improve government cyber security as well as provide value for money. Whether that be centralised work to protect *gov.uk* domains for the whole public sector, or the development and increased availability of Active Cyber Defence tools and services, such efforts either reduce the risk faced by government organisations or support them in managing it efficiently and effectively.
- 67. Government will therefore continue to develop and scale-up such capabilities. Coordination and collaboration are key to this, both to ensure that solutions are targeted where they are most needed and to enable government to foster innovation to drive improved cyber security at scale.

FOCUS ON: Active Cyber Defence



Active Cyber Defence is an NCSC programme that seeks to 'protect the majority of people in the UK from the majority of the harm caused by the majority of the cyber attacks the majority of the time'. There is a specific intent to tackle, in a relatively automated way, a significant proportion of the cyber attacks that impact government systems.

Active Cyber Defence is complementary to, and does not replace, system owners' investment in good cyber security. It is made up of a growing number of capabilities, including:

- **Capabilities to detect and disrupt threats** – by identifying malicious activity at scale and/or instigating an automated response to disrupt it. These include:
 - **Takedown Service** – finds malicious sites and notifies owners to get them removed
 - **Protective DNS** – blocks inadvertent access to domains or IPs that are known to contain malicious content, and malware already on a network attempting to call home
 - **Host Based Capability** – analyses technical metadata on hosts, such as laptops and servers, across government departments for malicious activity to make OFFICIAL systems a harder target [see '*FOCUS ON: Host Based Capability*' for more detail]
 - **Cyber Threat Intelligence Adaptor** – enables authorised organisations to receive a high-quality, contextually rich, cyber threat intelligence feed from the NCSC
- **Capabilities to provide self-service checks and alerts** – making it simpler for organisations to check and improve their security posture. These include:
 - **Early Warning** – helps organisations investigate cyber attacks on their network by notifying them of malicious activity detected in information feeds
 - **Mail Check** – helps organisations assess their email security compliance and adopt secure email standards
 - **Web Check** – helps owners of public sector websites to identify and fix common security issues, making sites a less attractive target to attackers
 - **Exercise in a Box** – provides a toolkit of realistic scenarios that helps organisations practise and refine their response to cyber security incidents in a safe environment

This list is by no means exhaustive and the number of capabilities continues to evolve.¹⁶

Focused investment in selected Active Cyber Defence capabilities will be a key part of the success of this strategy. This includes targeted development and extended coverage for wider public sector organisation, and new capabilities responding to emerging developments in technology and adversary tradecraft.

Information and data security

Outcome 13:

Government data is classified appropriately and handled and shared in a way commensurate to the risk it presents

- 68. Government has a responsibility to protect data, whether classified information or the personal data that it handles and shares to deliver its functions and services. Government will therefore handle, share, and store or host its data assets in a way that is proportionate to the risks they present.
- 69. At the heart of this is the effective classification of information based on agreed threat models and a comprehensive assessment of risks associated with the information being handled. Central classifications policy sets out the criteria and the required handling instructions for information classified at different tiers.

FOCUS ON: Classifications policy



Government will update the Security Classifications Policy to improve the handling of information at the OFFICIAL tier and ensure that the most sensitive information held at this tier is adequately and consistently protected. It will also provide departments and individual users with clearer guidance, especially on new capabilities and changes to ways of working, so they can better protect classified information.

FOCUS ON: Security in data sharing



The National Data Strategy¹⁷ sets out the government's mission to transform its use of data to drive efficiency and improve public services. To achieve this, the government is undertaking an ambitious and radical transformation of its own approach, driving major improvements in the way information is efficiently managed, used and shared across government. As well as demanding robust data standards that drive consistency and interoperability, government will ensure that data protection and security is at the heart of its approach.

¹⁷ HMG; 'National Data Strategy'; December 2020



70. The majority of government information is classified as OFFICIAL and is dependent upon the technology and controls outlined above. However, there will be occasions where the threat model requires certain information to be protected at a higher classification, for which the commodity technology available for OFFICIAL information is not suitable. To account for this need, government will continue to develop a 'full-stack' solution that enables a suitably secure, collaborative and user-friendly way of working across government at the appropriate classification.
71. Where sensitive data has to be processed on OFFICIAL systems in order to perform a business function, protections will be put in place that are commensurate to the risks presented.

FOCUS ON: Rosa



Rosa is the cross-government SECRET IT service. Since its launch it has been adopted by an increasing number of users for an increasing number of use cases, reaching over 12,000 users and 74 departments in 2021. Government will build on this success by continuing to invest in Rosa to ensure that it continues to meet the growing needs of its users.

As well as making it significantly easier to handle government information at the appropriate classification, the increasing provision of Rosa will mean it is less likely that information is under-classified, making it much more difficult for adversaries to access and exploit.

FOCUS ON: Harnessing emerging technologies



The pace of technological change presents both challenges and opportunities for government cyber security. Government must be able to apply such technologies to enhance its cyber security capabilities across the government, while ensuring that its application is as secure as it needs to be.

Artificial Intelligence (AI)

AI is a form of software that can learn to solve problems at a scale and speed impossible for humans and is becoming an integral part of modern systems. In cybersecurity, AI has three distinct aspects:

- Use of AI to secure systems. Many AI algorithms are complex and opaque, with the potential to introduce new classes of vulnerability. Understanding and mitigating these emerging threats is a priority.
- Use of AI to improve cybersecurity threat detection and, in some cases, to enable automated response to threats.
- Recognising and mitigating AI-based attacks from adversaries.

The Office for Artificial Intelligence is a joint BEIS-DCMS unit responsible for overseeing implementation of the wider National AI Strategy.¹⁸ In addition, the Alan Turing Institute and similar bodies are researching how we might build and use AI in a more ethical, responsible manner. Government is committed to creating and using AI in a way that supports security, fairness, empowerment, transparency and accountability.

Quantum

Quantum computers use properties of quantum mechanics to compute in a fundamentally different way from today's 'classical' computers. They are, theoretically, capable of performing certain computations that would not be feasible for classical computers.

'Quantum-safe cryptography' replaces the quantum-vulnerable mathematical problems with those believed to be intractable for both classical and quantum computers. 'Quantum-safe cryptography' using standards-compliant products will therefore provide the most effective mitigation for the serious threat that quantum computers pose to long-term cryptographic security, and will be deployed across government when required.

¹⁸ HMG; 'National AI Strategy'; September 2021

FOCUS ON: Advanced protections

The thrust of this strategy is about ensuring government reaches and maintains a level of resilience that is proportional to its risk. However, it is recognised that the most sophisticated actors may be able to overcome robust cyber security measures given enough investment and determination.

Government will deploy its full spectrum of capabilities to respond to the most sophisticated threats. Such capabilities will include advanced protection and detection techniques, as well as targeted use of government's offensive cyber capability and broader international and diplomatic efforts to disrupt and deter such threats.



Chapter 5:

Detecting cyber events



72. Despite robust protections being put in place, evolving adversary techniques and the discovery of unknown vulnerabilities means that cyber attacks will still occur. To respond to the changing threat landscape, government requires comprehensive detection capabilities to identify emerging risks so that they can be managed.

Objective 3: Government will detect cyber security events



Government has the capability to monitor its systems, networks and services to detect cyber security events before they become incidents. Enhanced coordination will enable government to have the agility to use these data inputs to detect at pace and scale, facilitating coherent responses as well as providing the capabilities to detect more sophisticated attacks.

73. Building on the foundation of risk management and commensurate protective measures, government will develop its capability to detect cyber security events across every part of its estate to ensure that the risks can be mitigated before they critically impact government functions.

Detection within government organisations

Outcome 14:

Government networks, systems, applications and end points are monitored to provide proportionate internal detection capability

74. To adequately fulfil their responsibilities to manage their risks, every government organisation will have proportionate monitoring capabilities as well as the ability to retain and interrogate logs to facilitate the detection of cyber threats. Monitoring should be as holistic as possible - from the monitoring of underpinning infrastructure, such as domains, through to host-based monitoring of end points and cloud-based services, and the monitoring of privileged accounts on an organisation's network and in its supply chain. To achieve this, smaller organisations may form part of a larger conglomerate, particularly within sectors orchestrated by lead government departments.
75. Government will establish a common process and language for organisations to record and share information about cyber security incidents and 'near misses' - in a machine-readable format. This will ensure that there is consistency and comparability across government organisations as well as allowing for enhanced visibility that will improve government's ability to learn, adapt and mitigate at scale.
76. The detection capabilities of government organisations will continue to evolve, particularly for those departments who have lower risk tolerances. In such circumstances, more advanced detection methods, such as behavioural monitoring, will be deployed to detect more sophisticated attacks.

FOCUS ON: Host Based Capability (HBC)



HBC is a service run by NCSC, designed to make OFFICIAL systems a harder target. Technical metadata on hosts, such as laptops and servers, across government departments is analysed using specialised knowledge and tradecraft at NCSC.

HBC is provided as a three-part service:

- **Detect:** HBC takes a sector-focused view of the threats departments face. It uses NCSC's knowledge of indicators, adversary tactics, techniques and procedures to detect malicious activity.
- **Threat Surface:** Reporting provides metrics to help departments understand and improve their IT cyber hygiene.
- **Forewarn:** HBC seeks to warn departments about their exposure to major vulnerabilities.

HBC's use across government will continue to scale, with future developments including cloud-based capability, and responses to shifts in technology and attacker tradecraft.

Detection at scale

Outcome 15:

Shared detection capability provides detection at scale across government

77. Effective detection capability requires the timely sharing of information across the whole of government, so that events identified in one organisation can be mitigated across all others. The mechanisms will be established to ensure that this information can be easily and securely shared, in an automated way, with an expectation placed on organisations to escalate alerts swiftly with clear and defined paths for doing so. Getting this right is critical to identifying, managing and mitigating emerging threats at the scale and pace required.
78. To enhance the detection and identification of more sophisticated actors on government networks and systems, a programme of strategic threat hunting will be established which will include the exploration of more advanced capabilities such as deception tactics and honeypots.





Chapter 6:

Minimising the impact of cyber security incidents



79. Even with robust protection and detection measures in place, government will be impacted by cyber security incidents. It is therefore essential that government is able to rapidly respond to cyber incidents when they do happen and minimise their impact as far as possible.

Objective 4:
**Government will minimise
the impact of cyber
security incidents**



Cyber security incidents will be swiftly contained, assessed and managed, enabling rapid mitigation response across government.

80. Effective risk management, appropriate and proportionate protective measures, and enhanced detection capability will make government a considerably hardened target. However, government will also improve its ability to respond and recover from incidents when they do happen to ensure the continuity of essential functions and services.

Response preparation

Outcome 16: Government is fully prepared to respond to cyber incidents

- 81. Organisational and cross-government cyber security incident response plans will clearly set out how government will respond to an incident to minimise its impact. Organisational plans will be routinely exercised through table-top scenario planning and red, blue and purple term activities, being updated as required to ensure that they are fit for purpose and continue to reflect the current threat environment.
- 82. Cross-government exercising will also be routinely carried out to ensure that senior leadership teams across government - including wider public sector organisations that deliver critical services - are practised and prepared to lead the response to cyber incidents that may impact multiple organisations across the public sector.

Incident response

Outcome 17: Government rapidly responds to cyber incidents, both organisationally and across government

- 83. Government organisations - either directly or through support of another government organisation - will have the structures and capabilities in place to triage cyber security incidents and rapidly assess their impact. Having clear escalation pathways is a crucial part of this, to ensure that the right people are made aware - both within the organisation and beyond - and the right expertise and resource is made available.
- 84. Central incident response functions will have the capacity and capability to manage serious and cross-government cyber security incidents with defined processes and mechanisms in place to ensure that all impacted parties are working collaboratively to minimise the impact. The GCCC will play a critical role.

Incident recovery

Outcome 18:

Government restores systems and assets affected by cyber security incidents and resumes the operation of its functions with minimal disruption

- 85. As well as being prepared and able to respond to cyber security incidents, government will be able to recover from them as quickly as necessary so that any disruptions to its functions are minimised.
- 87. Following the completion of incident response processes, central oversight of recovery from the most severe incidents will ensure that systemic risks are identified and mitigated.
- 86. Enacted response plans will ensure that an organisation can assess the risk from an incident using appropriate expertise and taking the necessary steps to resume its functions to an acceptable level within tolerable periods of disruption.

Lessons learned

Outcome 19:

Lessons learned from cyber incidents drive improvements in government's cyber security

- 88. To continue to drive improvements in cyber security, government will learn lessons from every cyber security incident and event - from serious incidents to 'near misses'.
- 90. Just as importantly, government will learn lessons from less serious events and 'near misses'. At the heart of this is the creation of a culture where cyber security colleagues feel confident sharing such information across government, without fear of embarrassment or blame. Doing so will ensure that government understands the root causes of incidents and can diagnose and communicate solutions to the whole of government to enhance its collective cyber resilience.
- 89. Government will be able to objectively learn from serious and cross-government cyber security incidents, with the most significant incidents being subject to an independent review to provide sufficient scrutiny.



Chapter 7:

Developing the right cyber security skills, knowledge and culture



91. Achieving this strategy's vision and aim will not be possible without appropriately skilled people, including those working in technical, policy and strategy, risk management, and leadership roles. In line with the objectives set out in the National Cyber Strategy, government will lead by example in boosting the scale, diversity and quality of cyber security professionals across government organisations, while fostering a cyber security cultural shift that will facilitate sustainable change.

Objective 5:

Government will develop the right cyber security skills, knowledge and culture



Government has sufficient, skilled and knowledgeable professionals to fulfil all required cyber security needs. This extends beyond technical cyber security experts to the breadth of professional functions that must incorporate cyber security into the services they provide - underpinned by a cyber security culture that promotes sustainable change.

92. There is diversity in the breadth and depth of cyber security skills required across government. These include deep technical skills and the non-technical cyber security skills that are needed across other specialisms and professions, such as digital, policy, commercial and assurance. Guided by the standards and pathways established by the UK Cyber Security Council, government will develop its understanding of the range of cyber security skills and knowledge required across government and will respond accordingly, ensuring that its workforce is inclusive and diverse.
93. This aspiration is, however, set within the context of a national cyber security skills gap¹⁹. The focus is therefore placed on investing in and building those skills from a multitude of entry points with a consistent career offer across government to aid recruitment and retention while reducing reliance on contractors. The continued creation of leading learning opportunities will further develop the profession, strengthening government's employment offer and its ability to compete.
94. While the government security profession is focused on improving the cyber security profession across government departments, it mutually supports cyber security skills initiatives across the public sector, as well as providing a framework for wider public sector organisations to understand and manage their cyber security skills requirements.

19 Ipsos MORI / DCMS; 'Cyber Security Skills in the UK Labour Market 2021'; March 2021

FOCUS ON: Cyber security skills as part of the UK ‘cyber ecosystem’



Strengthening the UK cyber ecosystem by investing in people and skills and deepening the partnership between government, academia and industry is one of the central pillars of the National Cyber Strategy.

Cyber security skills are a fundamental component of that ecosystem and the National Cyber Strategy sets out the clear objective to enhance and expand the nation’s cyber skills at every level. This includes:

- A significant increase in the number of people who have the skills they need to enter the cyber workforce;
- A higher quality and more established, recognised and structured cyber security profession;
- A more diverse cyber workforce; and
- A steady and diverse flow of highly skilled people coming through our education system.

Government is a key part of this ecosystem and its efforts to develop the right cyber security skills and knowledge will align with broader national efforts to enhance the UK’s cyber ecosystem.

95. Achieving sustainable change also demands a shift in cyber security culture, to one that encourages and empowers people to challenge, question, learn and drive continuous improvement. Central to this is

the creation of inclusive environments and the attraction and development of a diverse security workforce that reflects the wider UK population.

Skills requirements

Outcome 20:

All government cyber security skills requirements are understood

96. Government will have a comprehensive understanding of the volume and range of cyber security skills and knowledge - both technical and non-technical - required to enable it to function with the required resilience. As well as informing the development of government workforce and

resourcing strategies, this understanding will support and align with the work of the UK Cyber Security Council to ensure that consistent taxonomies, standards and pathways are developed and adopted for the cyber security profession across the UK.

Attracting and retaining talent

Outcome 21:

Government attracts and retains the diverse cyber security workforce it needs to be resilient

97. As well as the gap in cyber security skills in the UK²⁰, the cyber security workforce continues to lack the diversity it needs.²¹ Attracting and retaining a government workforce that truly represents different genders and ages, social, cultural and ethnic backgrounds, as well neurodiversity, is essential to providing the spectrum of perspectives and the creativity needed to tackle the increasing diversity of threats faced.
98. Government will use its developing understanding of its workforce, in the context of the wider UK cyber security workforce, to develop its approach to attracting and retaining talent. The development of apprenticeship and graduate programmes, combined with an extensive outreach programme to target underrepresented groups, will continue to attract cyber security talent into entry level roles. However, the majority of skills shortages across in the UK, including government, are found among more senior positions.²² The adoption of a single cyber capability pay framework across government, linked to accreditation, will ensure that pay is directly linked to skill level. This will enable government to better compete with the private sector and attract talent into all required positions, as well as providing commonality across government departments. Cyber security careers will be further incentivised through a range of initiatives, with a drive towards strengthening a culture of inclusion and improving representation.
99. Government also recognises that cyber security talent can be found in every corner of the UK, with particular hotspots of cyber security firms found in the South East, the North West, the South West and Scotland.²³ To boost regional growth in the sector, the Department for Digital, Culture, Media and Sport (DCMS) is working closely with regional cyber security clusters, supporting their development and improving reach and insight into local and regional cyber security sector ecosystems. There are now over twenty established and emerging cyber security cluster organisations in the UK that are promoting and investing in cyber security. To support these efforts, and to tap into these regional talent pools, government has already begun to establish its own centres of cyber security expertise across different regions of the UK and will continue to invest in more regional security centres.

FOCUS ON: Cyber workforce and resourcing hub service



Government will move to an in-house cyber workforce and resourcing hub service to improve recruitment outcomes and reduce the use of contractors. This includes working closely with external partners to build a strong brand as well as targeted recruitment and marketing of opportunities to improve diversity outcomes. Central oversight of the cyber workforce will enable a more flexible model and greater movement across government.

20 Ipsos MORI / DCMS; 'Cyber Security Skills in the UK Labour Market 2021'; March 2021

21 NCSC / KPMG; 'Decrypting Diversity: Diversity and inclusion in cyber security'; 2020

22 IPSOS MORI/DCMS; 'Cyber Security Skills in the UK Labour Market 2021'; March 2021

23 IPSOS MORI/DCMS; 'UK Cyber Security Sectoral Analysis 2021'; February 2021

Develop talent

Outcome 22:

Government continuously develops its cyber security workforce to ensure that it has and retains the skills it needs

- 100. Working with the UK Cyber Security Council, government will continue to develop comprehensive career pathways for its cyber security professionals. These pathways will provide diverse and fulfilling cyber security careers with a full development and learning offer.
- 101. Key to this will be the introduction of a skills assessment tool that will allow government to map the cyber security skills gap against

key roles with a view to developing centrally funded learning programmes. Through the creation of such comprehensive learning curricula, government will drive the professionalisation of cyber security roles. This will be supported by partnerships with recognised learning academies and security institutions, ensuring that learning is consistent and accessible to those public sector organisations with less resources to invest in training.

FOCUS ON: Establishing a government security learning academy



Government will establish a learning academy aimed at upskilling government security professionals and the wider civil service. Among other security disciplines, it will develop both technical and non-technical skills, providing masterclasses and access to qualifications, linking up with professional bodies and academia to assure in-house skills through skills assessment and accreditation.

- 102. A strong focus will be placed on developing an approach to accreditation that is linked to recruitment and promotion. This will ensure the status of the profession is recognised both inside and outside of the public sector, and that skills are developed in-line with national standards as defined by the UK Cyber Security Council.
- 103. As well as more formal career pathways, a focus will be placed on strengthening government's leadership community to

ensure they have the skills required. This will be part of our approach to build the cyber security community across government, to facilitate and encourage the sharing of ideas and approaches, as well as lessons learned when things go wrong. Creating the right communities will break down barriers and enable cyber security colleagues from across government to develop individual talent as well as collective expertise.

Cyber security knowledge across other government functions

Outcome 23:

Sufficient cyber security knowledge and awareness across government's professional functions ensures that cyber security is actively taken into consideration

104. The need for cyber security applies to all domains and needs to be given appropriate consideration across all professional functions, from the Digital, Data and Technology (DDaT) profession through to government's commercial and legal functions. While the degree of expertise required will vary depending on the function in question, having an appropriate knowledge of cyber security is essential.

105. Government will develop its understanding of these requirements and will work across other professions to improve cyber security knowledge and awareness, with a particular focus on senior leaders.

Cyber security culture

Outcome 24:

Government has a cyber security culture that empowers its people to learn, question and challenge, enabling continuous improvements in behaviours and resulting in sustainable change

106. People and organisational culture are at the heart of reducing risk. To truly make a difference, it is essential to focus on people as well as technology. This effort begins with improving cyber security awareness and knowledge across all public sector workers, reinforcing the expectations of public servants and embedding cyber security awareness into public service values. Government will provide tailored advice and implement a broad range of awareness-raising initiatives to ensure that all public sector workers can better protect themselves and the government organisations they work for.

107. Government will build on these foundations to create a positive cyber security culture that promotes and empowers its people to proactively engage on the organisational cyber security risk. Leadership, communication and consistency are key to this, both departmentally and across government. Transparent reporting structures will make it easy to report and all reporting will be handled confidentially and sensitively. Mistakes will not be stigmatised and incidents will be objectively understood with findings used as development and learning opportunities. People will be kept informed of progress and benefits to the organisation will be highlighted and celebrated.



Chapter 8: Measuring success



Achieving the aim

108. This strategy sets out how government will build and maintain its resilience in the face of continuously evolving cyber risks. At its heart is the aim for government's critical functions to be significantly hardened to cyber attack by 2025, with all government organisations across the whole public sector being resilient to known vulnerabilities and attack methods no later than 2030. Achieving this aim will mean that government as a whole will present a hardened target, enabling government functions to operate without undue disruption and cementing the UK's authority as a leading democratic and responsible cyber power.
109. This is an ambitious aim. To achieve the level of organised and objective visibility of cyber security risk across the whole of government will require extensive processes, mechanisms and partnerships to be established. The task is complicated by the varying levels of maturity, capability and capacity that exist across government organisations. This is particularly pertinent for lead government departments, who, as well as considering their own cyber security posture, must also consider the cyber security posture of the public sector organisations in their purview.
110. Given the dynamic and complex nature of cyber security vulnerabilities and the continuous evolution of cyber attack tactics, techniques and procedures, accounting for known vulnerabilities is challenging. Further to this, 'known' vulnerabilities cannot simply refer to publicly disclosed security flaws, but must also account for improper security practices that unduly expose an organisation to cyber attack. While measuring cyber security is challenging, establishing a coherent government cyber security assurance framework, with tiered government CAF profiles underpinned by government-specific cyber threat profiles, will provide a robust and consistent means of assessing cyber resilience in a way that is proportional to threats faced.
111. The strategy's aim will therefore be achieved when all government organisations meet the outcomes set out in the appropriate CAF profile under the government's cyber security assurance framework in the following timeframes:
- Government organisations that are determined to be responsible for critical functions will meet the outcomes set out in an 'Enhanced' CAF profile by 2025.
 - All central government departments will meet outcomes set out in their designated CAF profiles by 2026.
 - All other government organisations will meet outcomes set out in a 'Basic' CAF profile by 2030.
112. Progress towards this aim will be clearly monitored, both to demonstrate the successful impact of the strategy and to highlight areas where particular focus is required. The following indicators will be used to measure progress towards the aim:
- The proportion of government organisations in scope that have identified their critical functions.
 - The proportion of government organisations in scope whose critical functions have been assessed against the government assurance framework.
 - The proportion of government organisations in scope whose assurance outcomes are assessed as achieved.

Maintaining an appropriate measure of resilience

113. As the cyber threat and risk environment continues to evolve, it is essential to ensure that the outcomes demanded of government organisations remain appropriate. All CAF profiles, and the government specific threat profiles that underpin them, will therefore be periodically reviewed to ensure the required

outcomes are sufficient to maintain cyber resilience in face of evolving risks. Doing so will maintain the integrity of the aim of this strategy and make sure that achievement of required outcomes remains a strong indicator of government resilience.

Underpinning key performance indicators (KPIs)

114. It is recognised, however, that these measures and indicators alone are not sufficient to provide a complete picture of government resilience. These broad measures will therefore be underpinned by a number of more granular KPIs that draw from the strategy’s objectives and will guide the delivery of this strategy.

115. A number of key principles will be applied to guide the use of KPIs, ensuring that they are consistent, appropriate, and provide the oversight and transparency needed to demonstrate genuine success, as well as hold government to account.

116. The required outcomes will also be underpinned by cross-government policies. The impact of such policies will be monitored and measured, with regular and robust evaluation. Taken together, these measures will provide a comprehensive picture of government’s cyber resilience.

FOCUS ON: Principles of performance measurement



- KPIs will place a minimum burden on government organisations.
- Data generation will be automated or based on preplanned and agreed timelines wherever possible.
- KPIs will be achievable.
- KPIs will not be pursued at the expense of genuine cyber security outcomes.
- KPIs will demonstrate genuine impacts and benefits (recognising the limited quantifiable data that directly demonstrates cyber security outcomes).





Chapter 9:
Implementing
the strategy



Implementation

117. Initiatives set out in this strategy can be grouped as follows:

- Transformational initiatives that will be undertaken immediately to unlock disproportionate benefits across the strategy's outcomes.
- Short to medium term initiatives that will be established during the first spending review period.
- Medium to longer term initiatives that are currently unfunded and will be delivered during the next spending review period.

118. Longer term unfunded initiatives are at varying stages of development. These will be regularly reviewed to ensure alignment with policy priorities, value for money and deliverability. A critical review will be tied to the next spending review to ensure that funding is directed appropriately towards achieving the aim of this strategy.

FOCUS ON: The Government Security Centre for Cyber (Cyber GSeC)



The Cyber GSeC delivers a broad range of capabilities and services that support government organisations to improve their cyber security posture and achieve an appropriate level of cyber resilience. It therefore plays a critical role in delivering the outcomes of this strategy.

In its pilot year, the GSeC worked with departments to assist in rolling out Active Cyber Defence products produced by the National Cyber Security Centre (NCSC) and provided trusted, specialist services, such as the Cyber Gap Analysis assessments and reports, as well as access to expert cyber consultancy. Building from its success, the Cyber GSeC will be scaled up to play an increasingly critical role in supporting government to address weaknesses in cyber security. As well as providing bespoke support to individual organisations, it acts as a critical delivery capability for the roll out of centrally driven initiatives, reaching across all government organisations with a particular focus on those that carry the greatest risk.

The Cyber GSeC is part of a broader suite of Government Security Centres which look at the range of government security disciplines, from cyber security to physical and personnel security. All Government Security Centres work closely together on cross-cutting issues, ensuring that government continues to improve its security posture across all security disciplines.

Transformational proposals

119. Government will prioritise implementation of its two transformational proposals, which will provide the mechanisms required to facilitate a significant and disproportionate improvement in cyber resilience across government.

<p>1</p> <p>Adopt the CAF as the assurance framework for government, with tiered CAF profiles - underpinned by government-specific threat profiles - to respond to the varying threats to government functions, validated by independent and objective verification where applicable.</p>	<p>Pilots to be conducted by the end of 2022, followed by incremental rollout</p>
<p>2</p> <p>Establish the GCCC to unlock and transform how cyber security data is used across government.</p>	<p>Initial operational capability in 2022</p>



Implementation plan

<p>2022-25</p>	<p>2025-30</p> <p>While initiatives may not be fully implemented until this time, planning and development will begin as soon as practicable</p>
<div style="display: flex; align-items: center;">  <h2>Manage cyber security risk</h2> </div>	
<p>Enhanced governance and accountability across government</p> <p>Enhanced asset discovery and management discovery measures across government</p> <p>Investment in vulnerability management, including a vulnerability reporting service for the whole of government</p> <p>Map systemic risks in government’s supply chain and implement government procurement strategy</p> <p>Further embed strategic partnerships with the private sector, academia and international partners</p>	<p>Enhanced automated, live threat information shared at scale across government and wider public sector</p>
<div style="display: flex; align-items: center;">  <h2>Protect against cyber attack</h2> </div>	
<p>Implementation of ‘secure by design’ framework across government</p> <p>Manage, upgrade or remove legacy technology across the government estate</p> <p>Common configuration for common digital products and services developed and shared</p> <p>Trial and development of new shared capabilities to protect against attack alongside prioritised Active Cyber Defence roll out for the public sector</p> <p>New government classifications policy published and implemented</p>	<p>Harnessing of emerging technologies to enhance government cyber security</p>

2022-25	2025-30 While initiatives may not be fully implemented until this time, planning and development with begin as soon as practicable
 Detect cyber security events	
<p>Comprehensive and proportionate detection capability developed across government</p> <p>Enhanced mechanisms to share incident and cyber security event information</p> <p>Establish common language for organisations to record information about cyber security incidents and ‘near misses’</p>	<p>Every government digital system to have 24/7 security monitoring</p> <p>Harnessing future technology to grow and accelerate detection of cyber security events</p> <p>Establish a strategic threat hunting programme for government, including the use of shared capability and deception tactics</p>
 Minimise the impact of cyber incidents	
<p>Routine cyber security exercising of government critical functions</p> <p>Independent review (lessons learnt) process for all serious and or cross government cyber security incidents and vulnerabilities</p>	<p>Provision of expert exercising capability available across the public sector</p>
 Develop the right cyber security skills, knowledge and culture	
<p>Establish the Government Security Learning Academy</p> <p>Developed career pathways for government cyber professions</p> <p>Establish multiple entry points into the cyber profession</p> <p>Deliver a programme of cyber security culture improvement</p>	<p>Expand the cyber apprentice and training programme</p> <p>Invest further in regional security centres for government</p> <p>Adopt a single pay framework for cyber profession across government</p>

Objectives and Outcomes Summary

<p>OBJECTIVE</p> <p>Manage cyber security risk</p> <p>SUMMARY Effective cyber security risk management processes, governance and accountability enable the identification, assessment and management of cyber security risks - at both the organisational and cross-government level.</p>	<p>OUTCOMES</p> <ol style="list-style-type: none"> 1. Government has established governance arrangements with clear accountability enabling effective management of cyber risks at all levels of government 2. Government has comprehensive visibility and understanding of its digital assets enabling it to identify and manage vulnerabilities and the cyber security risks they present 3. Government has comprehensive visibility of the data it handles and shares so that it can appropriately assess and respond to the risks it presents 4. Government understands and manages risks emanating from commercial suppliers 5. Government understands the threat it faces relative to its functions in order to plan appropriate mitigations, at both an organisational and cross-government level 6. Government organisations have timely access to relevant and actionable cyber security data that enhances their ability to make effective risk management decisions 7. Government cyber security assurance provides government with the visibility it needs to make effective decisions and the confidence that it has appropriate cyber security measures in place to manage the risks to its functions 8. Strategic partnerships with the private sector and international partners are further embedded to enhance proactive defence at a global scale
<p>OBJECTIVE</p> <p>Protect against cyber attack</p> <p>SUMMARY Understanding of cyber security risk informs the adoption of proportionate security measures with centrally developed capabilities enabling protection at scale.</p>	<p>OUTCOMES</p> <ol style="list-style-type: none"> 9. Government adopts a common approach to ‘secure by design’ to ensure that appropriate and proportionate cyber security measures are embedded within the technology government uses, and that the security of digital services is continually assured throughout their lifecycle 10. Government organisations deploy cyber security controls commensurate with their risk profile to ensure that risks to their functions are managed proportionately 11. Government technology is appropriately configured, with standard profiles for common technology and architectures being developed and continuously updated 12. Shared capabilities, tools and services tackle ‘common’ cyber security issues at scale 13. Government data is classified appropriately and handled and shared in a way commensurate to the risk it presents

<p>OBJECTIVE</p> <p>Detect cyber security events</p> <p>SUMMARY</p> <p>Comprehensive monitoring of systems, networks and services enable cyber security events to be managed before they become incidents.</p>	<p>OUTCOMES</p> <p>14. Government networks, systems, applications and end points are monitored to provide proportionate internal detection capability</p> <p>15. Shared detection capability provides detection at scale across government</p>
<p>OBJECTIVE</p> <p>Minimise the impact of cybersecurity incidents</p> <p>SUMMARY</p> <p>Cyber security incidents are swiftly contained and assessed, enabling rapid response at scale.</p>	<p>OUTCOMES</p> <p>16. Government is fully prepared to respond to cyber incidents</p> <p>17. Government rapidly responds to cyber incidents, both organisationally and across government</p> <p>18. Government restores systems and assets affected by cyber security incidents and resumes the operation of its functions with minimal disruption</p> <p>19. Lessons learned from cyber incidents drive improvements in government's cyber security</p>
<p>OBJECTIVE</p> <p>Develop the right cyber security skills, knowledge and culture</p> <p>SUMMARY</p> <p>Sufficient, skilled and knowledgeable professionals fulfil all required cyber security needs - extending beyond technical cyber security experts to the breadth of professional functions that must incorporate cyber security into the services they provide - all underpinned by a cyber security culture that promotes sustainable change.</p>	<p>OUTCOMES</p> <p>20. All Government cyber security skills requirements are understood</p> <p>21. Government attracts and retains the diverse cyber security workforce it needs to be resilient</p> <p>22. Government continuously develops its cyber security workforce to ensure that it has and retains the skills it needs</p> <p>23. Sufficient cyber security knowledge and awareness across government's professional functions ensures that cyber security is actively taken into consideration</p> <p>24. Government has a cyber security culture that empowers its people to learn, question and challenge, enabling continuous improvements in behaviours and resulting in sustainable change</p>

Annex: Cyber Assessment Framework

The Cyber Assessment Framework (CAF) was developed by the NCSC - in its role as national technical authority for cyber security - to provide a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible.

The CAF is comprised of four objectives: managing security risk; protecting against cyber attack; detecting cyber security events; and minimising the impact of cyber security incidents.

These objectives are underpinned by 14 principles that are supported by 39 contributing outcomes, which specify what needs to be achieved - rather than a checklist of what needs to be done. Each contributing outcome is associated with a set of indicators of good practice (IGPs). IGPs are used to develop sector-specific CAF profiles, which provide a view of appropriate and proportionate cyber security for those organisations.

Cyber Assessment Framework’s objectives, principles and contributing outcomes²⁴

Objective	Principle	Contributing outcome
Managing security risk	Governance	Board direction
		Roles and responsibilities
		Decision making
	Risk management	Risk management process
		Assurance
	Asset management	Asset management
Supply chain	Supply chain	
Protecting against cyber attack	Service protection policies	Policy and process development
		Policy and process implementation
	Identity and access control	Identity verification, authentication and authorisation
		Device management
		Privileged user management
		Identity and access management (IdAM)

²⁴ NCSC, 'Cyber Assessment Framework version 3.0'; September 2019

Protecting against cyber attack	Data security	Understanding data
		Data in transit
		Stored data
		Mobile data
		Media / equipment sanitisation
	System security	Secure by design
		Secure configuration
		Secure management
		Vulnerability management
	Resilient networks and systems	Resilience preparation
		Design for resilience
		Backups
	Staff awareness and training	Cyber security culture
Cyber security training		
Detecting cyber security events	Security monitoring	Monitoring coverage
		Securing logs
		Generating alerts
		Identifying security incidents
		Monitoring tools and skills
	Protective security event discovery	System abnormalities for attack detection
		Proactive attack discovery
Minimising the impact of cyber security incidents	Response and recovery planning	Response plan
		Response and recovery capability
		Testing and exercising
	Lessons learned	Incident root cause analysis
		Using incidents to drive improvements

Glossary

A

Active Cyber Defence (ACD):

An NCSC programme which seeks to reduce the harm from commodity cyber attacks, consisting of a number of interventions or services that help an organisation to find and fix vulnerabilities, manage incidents or automate the disruption of cyber attacks. Some services are designed primarily for the public sector, whereas others are made available more broadly to private sector or citizens, depending on their applicability and viability.

Arm's-length bodies:

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.

Artificial Intelligence (AI):

A technology in which a computing system is coded to 'think for itself', adapting and operating autonomously. AI is increasingly used in more complex tasks, such as medical diagnosis, drug discovery, and predictive maintenance.

B

Blue teaming:

A team responsible for defending an organisation's information systems by maintaining its security posture against mock attackers (the Red Team).

C

CAF profile:

The articulation of required outcomes corresponding to the Cyber Assessment Framework that reflect an organisation's 'threat profile'.

Central Digital and Data Office:

Part of the Cabinet Office - leads the digital, data and technology function for government, aiming to achieve transformation at scale by working with departments, and other government functions like commercial, project delivery and security professionals.

Central government:

Central government comprises all the organisations that are controlled directly or indirectly by government ministers.

Central government functions:

Central government units that have cross-government responsibilities and provide cross-government services and capabilities.

Critical National Infrastructure (CNI):

Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers that operate and facilitate them), the loss or compromise of which could result in:

- major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or
- significant impact on national security, national defence, or the functioning of the state.

Cryptography:

The science or study of analysing and deciphering codes and ciphers; cryptanalysis.

Cyber attack:

Deliberate exploitation of computer systems, digitally-dependent enterprises and networks to cause harm.

Cyber Assessment Framework (CAF):

An assessment framework developed by the NCSC that provides a systematic and comprehensive approach to assessing the extent to which cyber risks to essential functions are being managed by the organisation responsible.

Cyber Essentials:

A Government-backed, industry-supported scheme to help organisations protect themselves against common online threats.

Cyber incident:

An occurrence that actually or potentially poses a threat to a computer, internet-connected device, or network – or data processed, stored, or transmitted on those systems – which may require a response action to mitigate the consequences.

Cyber power:

Cyber power is the ability to protect and promote national interests in and through cyberspace.

Cyber resilience:

The ability of an organisation to maintain the delivery of its key 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.

Cyber security assurance:

The verification that systems and processes meet the specified security requirements and that processes to verify ongoing compliance are in place.

Cyber security controls:

The processes and tools an organisation have in place to detect, prevent, reduce or counteract security risks.

Cyber security data:

Any data that is relevant to cyber security, including data on cyber threats and vulnerabilities.

Cyber risk:

The potential that a given cyber threat will exploit the vulnerabilities of an information system and cause harm.

Cyber threat:

Anything capable of compromising the security of, or causing harm to, information systems and internet connected devices (to include hardware, software and associated infrastructure), the data on them and the services they provide, primarily by cyber means.

D**Devolved government:**

The separate legislatures and executives in Scotland, Wales and Northern Ireland following devolution, responsible for many domestic policy issues with the power to make laws for these areas.

Digital, Data and Technology (DDaT):

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

Domains:

A domain name locates an organisation or other entity on the Internet and corresponds to an Internet Protocol (IP) address.

F**Financial Sector Cyber Collaboration Centre (FSCCC):**

NCSC supported initiative that partners the Financial Authorities, industry, the National Crime Agency to improve the cyber resilience of the UK's financial sector.

G

GBEST:

GBEST is an intelligence-led simulated attack framework developed and managed by the Cabinet Office. It is derived from the Bank of England’s CBEST framework but is focused on building the overall cyber resilience of government.

Government:

The organisations that operate and deliver the functions that run the UK, including central government departments, arms-length bodies, agencies, local authorities and other wider public sector organisations.

Government Cyber Adversary Simulation Exercise (GCASE):

GCASE is similar to GBEST provides although provides a less in-depth level of assurance, while being faster to deploy.

Government Cyber Coordination Centre (GCCC):

Proposed joint venture between the Government Security Group, the Central Digital and Data Office and the NCSC, bringing together their respective functions and areas of expertise to better coordinate operational cyber security efforts across government, transform how cyber security data and threat intelligence is used across government and truly enhance government’s ability to ‘defend as one’.

Government Security Centre for Cyber (Cyber GSeC):

Function that delivers a broad range of capabilities and services that support government organisations to improve their cyber security posture and achieve an appropriate level of cyber resilience.

Government Security Group:

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

H

Host Based Capability (HBC):

HBC is a software agent available to government departments for the OFFICIAL devices they use. This includes laptops, desktops and servers. The agent is installed on the devices and works in the background to collect technical metadata.

I

Incident management:

The management and coordination of activities to investigate, and remediate, an actual or potential occurrence of an adverse cyber event that may compromise or cause harm to a system or network.

Incident response:

The activities that address the short-term, direct effects of an incident, and may also support short-term recovery.

Integrated Review:

Global Britain in a Competitive Age, the Integrated Review of Security, Defence, Development and Foreign Policy, describes the government’s vision for the UK’s role in the world over the next decade and the action government will take to 2025.

ISO 27001:

International Standards Organisation standard which covers requirements for an information security management system.

L

Lead government department:

A government department that has other public sector organisations within its purview.

Legacy:

Systems, services or any components that are ineffectively maintained or supported by internal teams, contractors, suppliers or vendors.

M

Macro cyber posture:

An assessment of the overall cyber security resilience of the organisations under the purview of a lead government department.

Minimum Cyber Security Standards:

Minimum set of cyber security standards introduced in 2018 that government expects departments to adhere to and exceed wherever possible.

N

National Cyber Security Centre (NCSC):

The UK's technical authority for cyber threats, providing a unified national response to cyber incidents to minimise harm, helping with recovery and learning lessons for the future.

National Cyber Security Programme:

The programme of work set up to implement the National Cyber Security Strategy, and deliver against its strategic outcomes.

Network:

A collection of host computers, together with the sub-network or inter-network, through which they can exchange data.

Network and Information Systems regulations (NIS):

UK regulations that provide legal measures to boost the level of security (both cyber & physical resilience) of network and information systems for the provision of essential services and digital services.

National Institute of Standards and Technology (NIST) Cyber Security Framework:

A set of guidelines published by the US National Institute of Standards and Technology for organisations to better manage and reduce cybersecurity risk, as well as foster risk and cybersecurity management communications.

O

Offensive cyber:

Adding, deleting or manipulating data on systems or networks to deliver a physical, virtual or cognitive effect. Offensive cyber operations often exploit technical vulnerabilities, use systems or networks in ways that their owners and operators would not intend or condone, and may rely on deception or misrepresentation.

OFFICIAL:

The lowest level in the Government Security Classifications system, which defines the level of confidentiality needed to protect an asset, covering the majority of government work.

Operators of essential services:

Organisations within vital sectors which rely heavily on information networks, for example utilities, healthcare, transport, and digital infrastructure sectors as identified by the criteria in the Network and Information Systems (NIS) Regulations 2018.

P

Penetration testing:

Activities designed to test the resilience of a network or facility against hacking, which are authorised or sponsored by the organisation being tested.

Public sector:

The portion of the economy composed of all levels of government and government-controlled enterprises.

Purple teaming:

A cyber security testing exercise in which a team takes on the role of both red and blue team.

Q

Quantum:

Quantum technology relies on the principles of quantum physics. The advancing understanding and control of what are known as ‘quantum effects’ such as superposition and entanglement will lead to a new wave of advances that will underpin our economy and society: sensing, data transmission and encryption, timing and computing.

R

Ransomware:

Malicious software that denies the user access to their files, computer or device until a ransom is paid.

Red teaming:

A penetration testing team which takes on an offensive role, attacking computer systems to explore the ways in which a genuine aggressor would carry out an attack.

Rosa:

A government IT capability and service that enables collaborative working up to SECRET with the very latest technologies.

S

SECRET:

Government security classification covering very sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors.

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.

Secure configuration:

Security measures that are implemented when building and installing computers and network devices in order to reduce unnecessary cyber vulnerabilities.

T

Threat hunting:

Cyber threat hunting is the process of proactively searching across networks and endpoints to identify threats that evade security controls.

Threat model:

An engineering technique to identify threats, attacks, vulnerabilities, and countermeasures that could affect an IT system.

Threat profile:

An articulation of the threat to an organisation and its assets, which informs the designated CAF profile under government’s proposed assurance process.

U

User:

A person, organisation entity, or automated process, that accesses a system, whether authorised or not.

V

Vulnerability:

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

Vulnerability reporting service:

A mechanism through which an organisation can be alerted to security flaws before they are exploited by attackers.



HM Government

Cabinet Office
70 Whitehall
London
SW1A 2AS