Department for
Business, Energy
& Industrial Strategy

2022 Civil Nuclear Cyber Security Strategy

In partnership with civil nuclear industry:

May 2022

© Crown copyright 2022

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third-party copyright information you will need to obtain permission from the copyright holders concerned.

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

Contents

Ministerial Foreword

As the Minister for Energy, Clean Growth and Climate Change, I am delighted to present the *2022 Civil Nuclear Cyber Security Strategy*, which sets out an ambitious vision and five year roadmap of activities for the UK's civil nuclear sector. This vision cannot be achieved by any organisation in isolation, so I am delighted that the strategy has been developed and endorsed jointly with UK civil nuclear organisations, the Office for Nuclear Regulation and the National Cyber Security Centre. I look forward to working together with them to strengthen the cyber security of the UK's civil nuclear sector.

The United Kingdom was the world's first civil nuclear nation, and nuclear energy has powered homes and businesses in this country for over 60 years. As a source of low carbon power, nuclear energy will play a crucial role in reducing the UK's greenhouse gas emissions to net zero in 2050. It is also an important part of accelerating homegrown power for greater energy security. The sector supports 60,000 jobs across the whole nuclear fuel cycle – from enrichment to decommissioning and waste management – and at both a national and regional level. Its importance to the UK's national security, energy needs, and economy will only continue to grow, so it's never been more important to ensure that the sector is well-positioned and resilient against cyber threats.

The Government published the new *National Cyber Strategy* at the end of 2021, setting out our vision to maintain the UK's standing as a leading, responsible and democratic cyber power. Cyber represents a huge opportunity for UK businesses: transforming ways of working, promoting innovation, and increasing productivity and efficiency. However, it also creates opportunities for malicious actors to exploit, attack and disrupt networks in efforts to extort money or valuable intellectual property. We recognise that we have come a long way, but we still have more to do. The *2022 Civil Nuclear Cyber Security Strategy* sits beneath the national framework and outlines how we will deliver its objectives together within the UK's civil nuclear sector.

As both the cyber threat and digital technologies continue to evolve, it is crucial that we make a step change to stay ahead of the curve. Managing cyber risks requires a whole-of-organisation effort, underpinned by strong regulation, supported by sector-wide collaboration, and a positive security culture. The commitments set out in this strategy seek to collectively deliver that shared ambition, ensuring that the UK's civil nuclear sector will continue its legacy long into our net zero future.

Greg Hands MP

Minister of State for Energy, Clean Growth and Climate Change
Department for Business Energy and Industrial Strategy

Executive Summary

Electricity generated from nuclear power will play a vital role in supporting the UK's long term energy security, clean energy transition and achieving its net zero carbon emissions target by 2050. As the sector's strategic importance and size increases, it is more crucial than ever that civil nuclear organisations and their suppliers protect themselves against cyber security threats, and plan effectively for cyber incidents.

The *2021 National Cyber Strategy* sets the UK ambition to be a leading global cyber power, protecting and promoting the UK's interests in and through cyberspace. That vision is matched in the civil nuclear sector, with this strategy sitting underneath the national framework and supporting its delivery. Our goal is 'A UK civil nuclear sector which effectively manages and mitigates cyber risk in a collaborative and mature manner, is resilient in responding to and recovering from incidents, and ensures an inclusive culture for all'.

Cyber security in the sector is on a positive trajectory and cyber maturity has improved over the past five years with the support of this strategy's predecessor, the *2017 Civil Nuclear Cyber Security Strategy*. However, there is more work to do, and the evolving nature of both the threat and technology means we need to accelerate to keep pace with a changing external environment.

Building on a comprehensive understanding of current sector strengths and challenges, this strategy outlines four key objectives which the sector should achieve by 2026:

- The sector appropriately prioritises cyber security as part of a holistic risk management approach, underpinned by a common risk understanding, and outcome-focused regulation;
- The sector and its supply chain takes proactive action to mitigate cyber risks in the face of evolving threats, legacy challenges and adoption of new technologies;
- The sector enhances its resilience by preparing for, and responding collaboratively to cyber incidents, minimising impacts and recovery time; and
- The sector collaborates to increase cyber maturity, develop cyber skills and promote a positive security culture.

These objectives will be delivered by a range of priority and supporting activities and overseen by a programmatic approach to delivery. Key commitments include:

- Rolling out Cyber Adversary Simulation (CyAS) assessments and other threat-informed testing activities across the sector's critical Information Technology (IT) and Operational Technology (OT) systems;
- Setting baseline cyber security standards for the civil nuclear supply chain;

- Delivering a sector-wide live cyber incident response exercise with the National Cyber Security Centre, alongside an exercising programme targeted at senior decision-makers;
- Collaborating across the sector on third party and component assurance and management; and
- Working with developers of advanced nuclear technologies to support cyber security by design.

The nature of cyberspace and the challenges faced mean that this strategy cannot be delivered by any organisation alone, and has therefore been developed jointly with leaders from public and private sector civil nuclear organisations, the Office for Nuclear Regulation, and the National Cyber Security Centre. Its success hinges on joint delivery and continued co-operation across all partners. In recognition of this, the strategy has been endorsed by senior decision-makers across the sector through the Cyber Security Oversight Group, which will take responsibility for its implementation.

1. Strategic Context

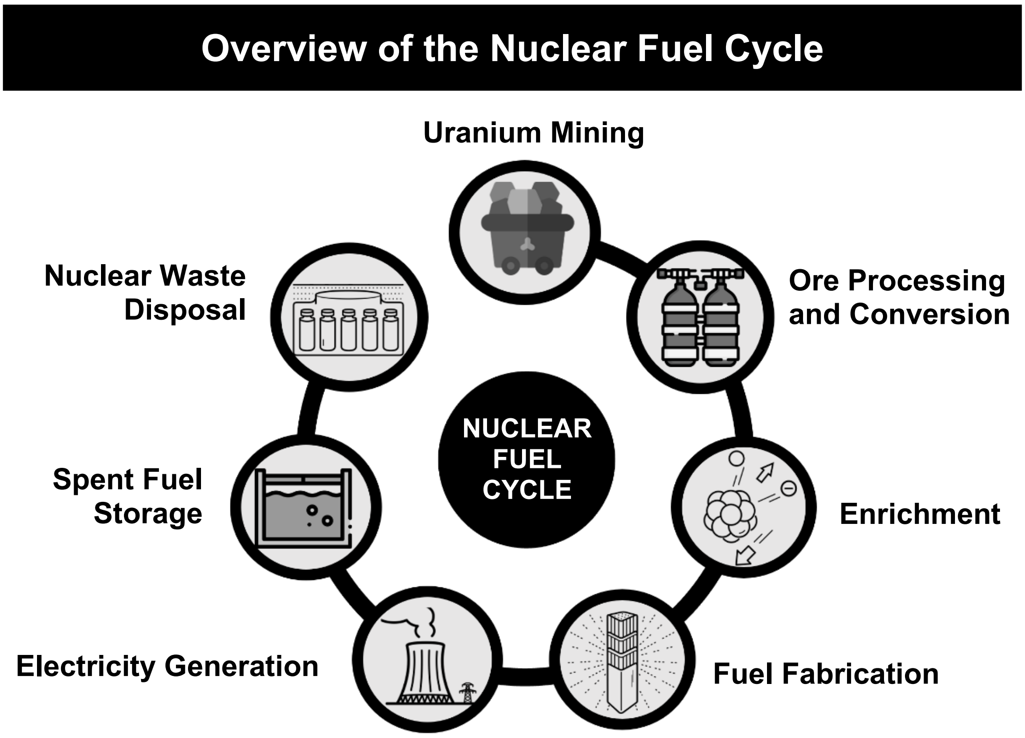
1.1 The Civil Nuclear Sector

Nuclear power will play a vital role in meeting the UK's electricity demands while supporting the clean energy transition, delivering our net zero carbon emissions target and increasing our energy security by 2050. Nuclear energy complements renewable sources in ensuring a low cost, stable and low carbon system, and offers additional resilience to the UK's energy security by providing a reliable baseload of power that is not fossil fuel, sun or wind dependent. The 2020 Energy White Paper[1], the Prime Minister's 10 Point Plan for a Green Revolution[2], the 2021 Net Zero Strategy[3] and the 2022 British Energy Security Strategy[4] all stated the Government's objective to advance nuclear as a secure and clean energy source through development of both large-scale nuclear and the next generation of small and advanced reactors. Crucial to its successful delivery will also be a well-planned decommissioning and waste management programme.

The UK civil nuclear sector is specialist, diverse and highly-skilled, supporting over 60,000 jobs nationwide. Our civil nuclear heritage originates from the 1950s, with Calder Hall in Cumbria being the first nuclear power station in the world to produce electricity for domestic use. Today the UK sector encompasses much of the nuclear fuel cycle process: from fuel enrichment and fabrication; to electricity production; to nuclear waste disposal. We host a world-leading nuclear transport capability; safely and securely transporting nuclear material around the world so it can be utilised and reprocessed effectively; and are home to Sellafield, Europe's largest nuclear site. The civil nuclear sector is also protected by a dedicated armed police force, the Civil Nuclear Constabulary, which is charged with the protection of civil nuclear sites and nuclear materials in England, Scotland and Wales.

[1] *Energy White Paper: Powering Our Net Zero*, December 2020
[2] *10 Point Plan for Green Industrial Revolution*, November 2020
[3] *Net Zero Strategy: Build Back Greener*, October 2021
[4] *British Energy Security Strategy*, April 2022

Figure 1 – A summary of the nuclear fuel cycle: the industrial processes for nuclear material from mining to disposal



Given the importance of the civil nuclear sector to the UK's energy system, population and environment, the UK remains committed to maintaining and strengthening its nuclear safety and security. In recognition of the UK's role in the global nuclear regime, we have a duty to continue to uphold ourselves as a responsible nuclear power. This means protecting the UK's nuclear material, facilities, information, and technology from the threats it faces, as well as facilitating the safe, timely and cost-effective management of our nuclear waste and decommissioning of nuclear facilities. Civil nuclear is recognised as one of the UK's Critical National Infrastructure sectors and it is robustly regulated to ensure that safety, security and safeguarding arrangements are effective. This substantive body of nuclear safety, security and safeguards laws and regulations[5] is enforced by the sector's independent regulator, the Office for Nuclear Regulation (ONR), working with the Environment Agency, Department for Transport, and the Information Commissioner's Office, amongst others.

1.2 Cyber Security in Civil Nuclear

As the civil nuclear sector's importance continues to grow, becoming more digitalised and interconnected, it cannot be complacent about keeping pace with the cyber security threats facing UK Critical National Infrastructure. The range of malicious cyber actors, from cyber criminals to hostile state actors, continues to expand, whilst the cyber threat is quickly evolving in terms of capability, new technology, and its global-to-local reach. Impacts can be targeted or indiscriminate, as demonstrated by notable cyber incidents occurring globally and in the UK. At

[5] Relevant legislation includes, but is not limited to: the Radiation (Emergency Preparedness and Public Information) Regulations (2019), Nuclear Safeguards Act (2018), Nuclear Industries Security Regulations 2003, The Civil Contingencies Act (2004) and the Nuclear Installations Act (1966)

the same time, increasing digital transformation provides significant opportunities for the UK, and its civil nuclear sector, to be world-leading in efficiency, safety, security, and innovation. Good security enables individual organisations and the sector as a whole maximise use of information and technology to achieve their wider goals.

In recognition of these evolving cyber threats and opportunities, the Government published the new *National Cyber Strategy* in December 2021, building on the successes of its predecessor national strategies in 2016 and 2011[6]. The National Cyber Strategy seeks to implement the ambition set out in the *2020 Integrated Review of Security, Defence, Development and Foreign Policy* for the UK to be a leading democratic cyber power[7], through its five key pillars:

- **Pillar 1: Strengthening the UK cyber ecosystem**, investing in our people and skills and deepening the partnership between government, academia and industry;
- **Pillar 2: Building a resilient and prosperous digital UK**, reducing cyber risks so businesses can maximise the economic benefits of digital technology and citizens are more secure online and confident that their data is protected;
- **Pillar 3: Taking the lead in the technologies vital to cyber power**, building in our industrial capability and developing frameworks to secure future technologies;
- **Pillar 4**: **Advancing UK global leadership and influence for a more secure, prosperous and open international order**, working with government and industry partners and sharing the expertise that underpins UK cyber power;
- **Pillar 5**: **Detecting, disrupting and deterring our adversaries to enhance UK security in and through cyberspace**, making more integrated creative and routine use of the UK's full spectrum of levers.

The *2022 Civil Nuclear Cyber Security Strategy* delivers a core element of Pillar 2, seeking to ensure that the civil nuclear sector is prepared for cyber risks and has the capabilities to prevent, respond to, and recover from, incidents when they occur. It also has an important role to play in supporting innovation and harnessing digital technologies, whilst the multinational nature of both the nuclear sector and the cyber threat means our goals can only be achieved by working internationally with bodies like the International Atomic Energy Agency (IAEA).

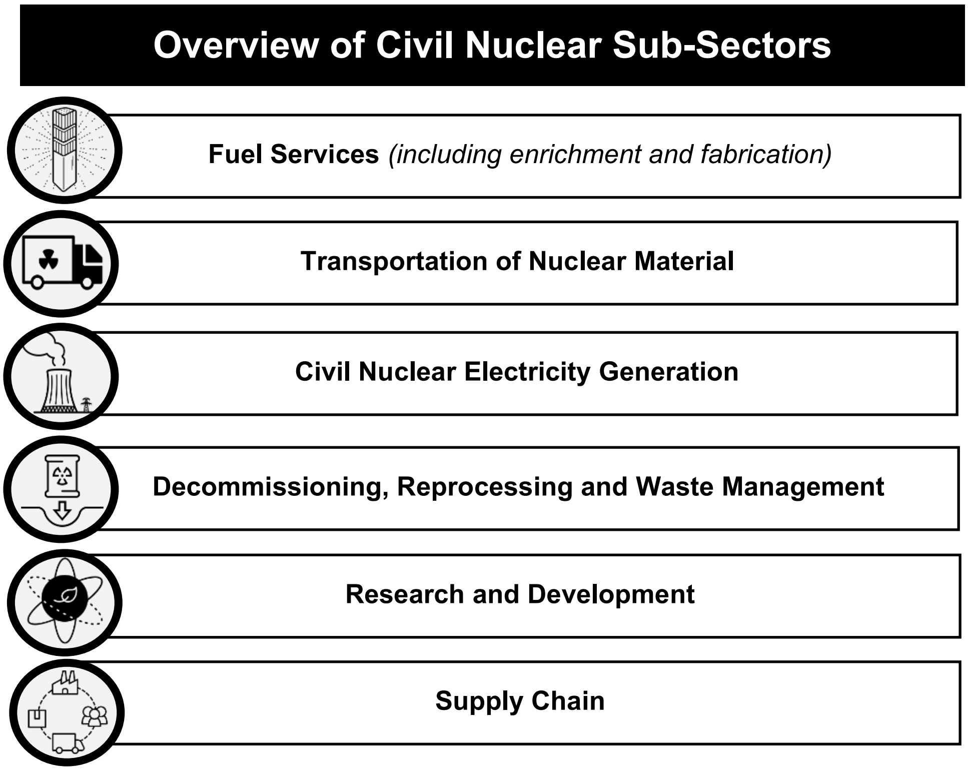
The UK's regulatory regime, enforced primarily by the ONR, is world-leading in its outcome-focused approach to managing cyber risk, building on the sector's strong risk management record. The sector has a mature safety and security culture across its varied organisations and personnel, and good progress has already been made on cyber security, facilitated by growing cross-sector cooperation and governance.

Nevertheless, increased prioritisation and collaboration is required to maintain this positive trajectory as cyber risks evolve. The 2020 Trojan attack on software company SolarWinds demonstrated how supply chains are being increasingly exploited to facilitate access to customer organisations. Meanwhile, the 2017 Triton malware attack, the 2020 attack on an

[6] UK National Cyber Strategy, December 2021
[7] *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*, March 2021

Israeli water facility and 2021 attack on Colonial Pipeline show the growing intent and capability to target Industrial Control System (ICS) environments. They are recognised as highly desirable assets, rich with valuable intellectual property and the potential to significantly disrupt operations. Closer to the nuclear sector, the 2020 ransomware attack on the Scottish Environmental Protection Agency (SEPA) illustrated the growing sophistication of cyber-attacks which can go undetected by even the most cyber mature organisations.

Figure 2 – A summary of the various sub-sectors within the Civil Nuclear Sector



Overview of Civil Nuclear Sub-Sectors

Fuel Services *(including enrichment and fabrication)*

Transportation of Nuclear Material

Civil Nuclear Electricity Generation

Decommissioning, Reprocessing and Waste Management

Research and Development

Supply Chain

The response to this multi-faceted risk environment must go beyond regulatory compliance towards a holistic risk management approach to cyber; recognising the role of cyber as a business enabler and an organisation-wide responsibility. The scope of this strategy thus looks across the entire civil nuclear sector, and across both regulated and unregulated domains within organisations. Building on the successes of the 2017 *Civil Nuclear Cyber Security Strategy*, it strengthens accountability for both regulated and unregulated cyber risks, promotes sector-wide collaboration and information-sharing, supports incident response planning, and delivers a step change in cyber security culture.

To embed this holistic risk management picture, each part of the sector must work in close partnership. Government, industry, regulators and the technical authority (the National Cyber Security Centre (NCSC)) have their own unique responsibilities and capabilities for civil nuclear cyber security. Taking action to manage and mitigate cyber vulnerabilities is primarily the task of the civil nuclear industry itself, who own the operation of the systems and have the expertise to take judgements on risk and appropriate cyber security controls on site. Industry is comprised of a mixture of private and public sector organisations, as well as the Civil Nuclear Constabulary and research and innovation bodies. The civil nuclear supply chain likewise holds responsibility for the security of the services, information and products they provide.

The industry and supply chain are supported by the ONR, which enforces and validates industry practice in line with security regulations, and the NCSC, which provides timely and accurate threat and vulnerability intelligence and advice. The Department for Business Energy and Industrial Strategy's (BEIS') role is to set strategic direction and risk appetite through the provision of threat planning assumptions and oversight of the overall regulatory framework, including the ONR's powers.

Figure 3 – A summary of the unique value-add of each civil nuclear partner to the sector's cyber security

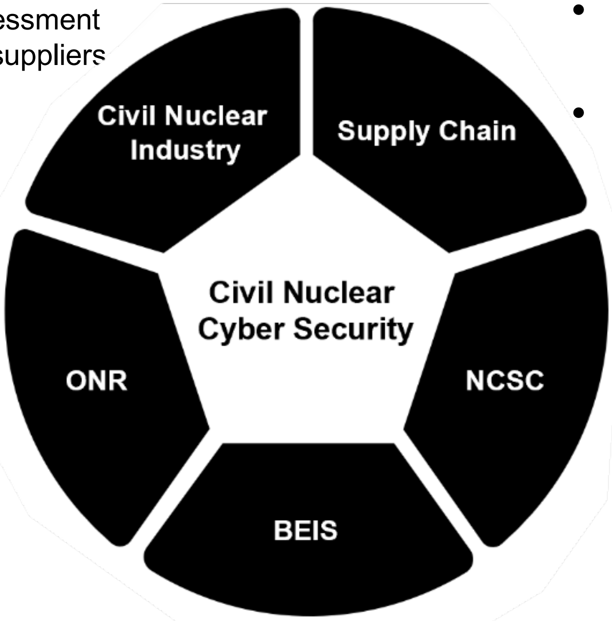
Overview of Unique Value-Add by Partner

CIVIL NUCLEAR INDUSTRY - ACTION

- Operation of civil nuclear sites and systems
- Implementation and maintenance of cyber security practices
- Risk ownership and assessment
- Contractual levers over suppliers

SUPPLY CHAIN - ACTION

- Production/provision of critical services and products
- Implementation and maintenance of cyber security practices
- Risk ownership and assessment



ONR - ENFORCEMENT

- Regulatory levers and incentives
- Expertise in nuclear cyber security
- Enforcement and direction powers

NCSC - ADVICE

- Threat intelligence and assessment
- Technical cyber expertise
- National cyber capabilities

BEIS - DIRECTION

- Threat planning assumptions
- Regulatory framework and the ONR powers

1.3 The 2017 Cyber Security Strategy

To proactively manage the cyber security challenges of the digital age in the civil nuclear sector, BEIS collaborated with the ONR, the NCSC and civil nuclear industry to develop the first, jointly-owned *Civil Nuclear Cyber Security Strategy (2017-21)* in 2017 – becoming the first UK Critical National Infrastructure sector to publicly launch a cyber security strategy.

This initial strategy described outcomes for the sector to strive towards and set expectations across the sector under four overarching activities for improving the understanding of cyber risks, mitigation of any cyber vulnerabilities identified, resources for cyber and cyber incident response.

Figure 4 – A high-level summary of the outcomes and overarching activities of the 2017 Civil Nuclear Cyber Security Strategy

Overview of Civil Nuclear Cyber Security Strategy (2017-21)

YEAR 1 OUTCOME (2016/17)	YEAR 2-4 OUTCOME (2017-19)	YEAR 5 OUTCOME (2020/21)
A continuing improvement in capability and capacity through training and exercising (supported by Government financing) with increasing senior executive understanding and ownership of cyber security risk facing their organisation. Successful delivery of the strategy will be demonstrated through regulator assessments and the NCSC assessment of industry exercising	An industry with reducing Government support, adapt to a tailored outcome-focussed approach using commercial cyber specialists as appropriate, as part of their holistic cyber (and overall) security stance.	An industry with a mature approach to understanding cyber threat and delivering outcome-focussed solutions which are approved by the regulator.

4 Overarching Activities to Support the Outcomes:

1. Delivering a **comprehensive understanding** of the cyber vulnerabilities across the civil nuclear sector
2. Continuously **mitigate** identified issues and vulnerabilities
3. Improve the sector's capability to **detect, respond and recover from cyber incidents**
4. Ensure **sufficient resources** are allocated to cyber security and resilience to transform capability in the sector.

The 2017 strategy put cyber security on the agenda alongside more traditional physical and personnel security, and safety and environmental risks. It set out the roles and responsibilities for cyber security for key entities across the sector – industry, the supply chain, regulators, and government – that individually and collectively play a role in strengthening the sector's cyber security posture. Feedback from across the sector conveyed that the strategy was foundational, facilitating a more joined up approach across the sector and ensuring that effective strategies were in place to identify cyber threats and mitigate vulnerabilities. Key achievements under this five-year strategy are set out in Figure 5.

As the 2017 strategy draws to a close, we recognise the significant progress made in improving the cyber security of the UK civil nuclear sector. However, the changing nature of the threat, greater focus on energy independence, and the evolution of civil nuclear technology and infrastructure mean there is still work to do. As the Government embarks on ambitious plans to bring at least one large-scale nuclear project to the point of Final Investment Decision by the end of this Parliament and develop the next generation of small and advanced reactors, cyber security needs to be embedded right from the design phase of our thinking. At the same time, as the UK's Advanced Gas-Cooled Reactor (AGR) fleet starts to move into decommissioning this decade, the challenges of our legacy infrastructure and our responsibility to maintain security throughout the entire infrastructure lifecycle remain paramount. Our 2022 strategy seeks to tackle these new challenges in a way that is future-proofed, measurable and flexible to the changing environment.

Figure 5: A summary of the key achievements of the 2017-21 Civil Nuclear Cyber Security Strategy

Key Achievements of the 2017-21 Civil Nuclear Cyber Security Strategy

A clearer understanding of the function, responsibilities and priorities of Government, the regulator, industry and the supply chain; helping strengthen ownership of mitigating cyber security risks.

The creation of the **Cyber Security Oversight Group (CSOG),** comprised of senior decision-makers with cyber security responsibilities, which brings industry, Government and regulator together to drive sector-wide collaboration and joint implementation of the strategy.

ONR's Security Assessment Principles (SyAPs), an integrated security regulatory framework, embedded across the sector. Replacing the previous prescriptive regulatory approach, SyAPs is outcome-focussed, empowering businesses to understand and own their security risks, with the flexibility to deploy security solutions that meet the outcome-based standard.

A mature, sector-wide technical cyber exercising programme with a focus on impacts to Operational Technology (OT) and the latest cyber trends. These exercises provide an opportunity to upskill the sector's cyber defenders on their technical skills, analytical and communication skills and raise wider awareness of safety colleagues on the cyber risks facing the OT environment.

The successful piloting of the NCSC's CyAS framework in the civil nuclear sector. An effective tool for testing and assuring the cyber security of an organisation's OT environment, this framework is specially designed to ensure testing of OT systems can be conducted safely.

A well-established, sector-wide civil nuclear cyber security graduate scheme which has grown a pool of suitably qualified cyber security professionals in the sector.

2. What Does Good Civil Nuclear Cyber Security Look Like?

To identify where challenges lie and monitor progress over time, we need to agree ‘what good looks like’ for civil nuclear cyber security. This helps us to target resources and priorities where they will have maximum impact.

Our goal for civil nuclear cyber security is that:

The UK civil nuclear sector effectively manages and mitigates cyber risk in a collaborative and mature manner. It is resilient in responding to and recovering from incidents, and promotes a positive security culture.

In determining what good looks like, we must take into account the following issues:

- Our desired outcomes must be **dynamic and adaptive**, allowing for rapid changes in priorities, threats and technologies, and recognising that action needs to be taken against both current risks and those that may emerge in the future. Future-proofed outcomes will also enable us to measure progress against these goals over time and in successive strategies.
- We must **embed cyber security in a wider risk and business growth context**, placing it as part of a ‘defence in depth’ approach to organisational security alongside physical and personnel protections. Our goals must recognise that cyber security should be prioritised amongst wider organisational safety, environmental and financial risks, as part of a holistic risk management approach. We must also recognise that cyber should be an enabler and an opportunity for business growth and innovation, rather than a hinderance.
- Our assessment must recognise that **good cybersecurity is a product of culture** rather than a set of isolated controls. Our interconnected services, suppliers and technology mean that cyber security cannot be achieved by security teams alone, or by only part of the sector – it must be organisation-wide and apply over the full nuclear life cycle. Success relies on embedding and sustaining **strong cyber security awareness**, practices and appropriate investment within and across all organisations (including partners and supply chain). **Promoting diversity of thought**, avoiding group-think, and promoting a positive culture is a crucial success factor in this process.
- It must apply equally to both **IT systems** (e.g. corporate networks, enterprise equipment, HR and finance systems, whether on premises or in the cloud) and **operational technology systems** (known as ‘OT’, which encompass the industrial systems, networks and plant equipment necessary to deliver the organisation’s product or service). Our decision to consider cyber and information security in the round reflects the fact that our entire digital footprint could be vulnerable to disruption or compromise by malicious actors. This can result in potentially

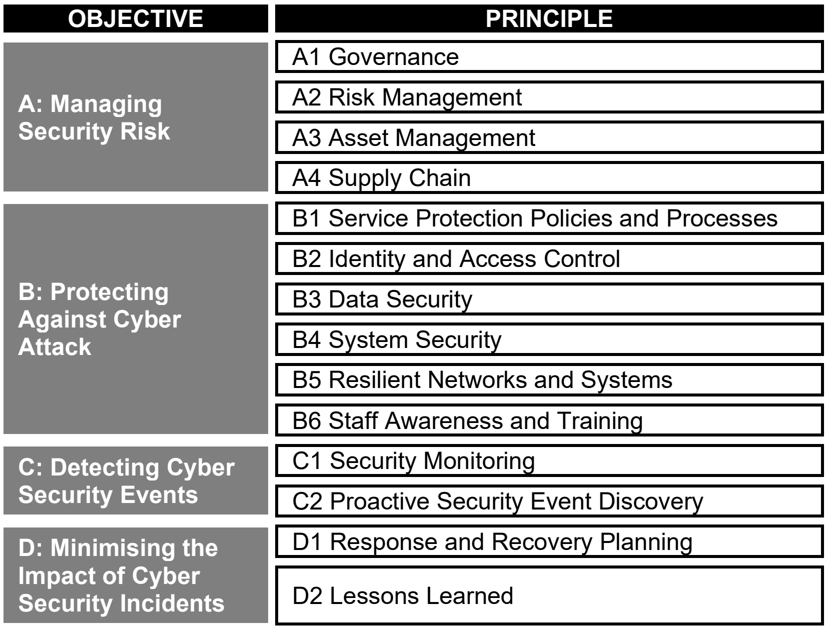
significant impacts – from reputational, financial and operational implications, all the way to severe safety and security outcomes. This is increasingly the case as IT and OT systems become more interconnected.

- And finally, increasing the sector's technical maturity alone will not deliver good cyber security: in considering what good looks like the importance of **strategic enablers** such as leadership, governance and competence must be recognised. As part of this, each partner – industry, ONR, supply chain, the NCSC and BEIS – should take responsibility for those issues where it is uniquely placed to take action.

Building on existing frameworks for cyber security maturity such as the ONR's Security Assessment Principles (SyAPs)[8] and the NCSC's Cyber Assessment Framework (CAF)[9], we have developed a high-level model of good civil nuclear cyber security. These outcomes outline what we want to achieve across all civil nuclear organisations, domains and systems (Figure 6).

In support of this model, a maturity framework was commissioned by BEIS, with the support of funding from the National Cyber Security Programme, to articulate some of these outcomes in more detail, in particular the indicators of good practice in cyber risk mitigation. The maturity framework was designed to be aligned with both the SyAPs and CAF, and outlined measurable goals against the indicators set out in Figure 7. Our intention is to use this framework as an objective assessor of cyber security maturity over time. Over the next five years this strategy will prioritise action and investment where there is a clear priority or gap. However, we recognise that new capabilities and challenges will arise over the life of the strategy. We will therefore regularly monitor and evaluate sector maturity against these indicators, enabling us to measure progress and redirect attention if priorities need to be adjusted.

Figure 6 – An overview of the CAF-aligned sector maturity framework used for the Benchmarking Project



OBJECTIVE	PRINCIPLE
A: Managing Security Risk	A1 Governance
	A2 Risk Management
	A3 Asset Management
	A4 Supply Chain
B: Protecting Against Cyber Attack	B1 Service Protection Policies and Processes
	B2 Identity and Access Control
	B3 Data Security
	B4 System Security
	B5 Resilient Networks and Systems
	B6 Staff Awareness and Training
C: Detecting Cyber Security Events	C1 Security Monitoring
	C2 Proactive Security Event Discovery
D: Minimising the Impact of Cyber Security Incidents	D1 Response and Recovery Planning
	D2 Lessons Learned

[8] Office for Nuclear Regulation's Security Assessment Principles (SyAPs) Framework
[9] UK National Cyber Security Centre (NCSC) Cyber Assessment Framework (CAF) Guidance

Figure 7 – A high-level model articulating good cyber security outcomes for civil nuclear cyber security

Across all domains and systems, the civil nuclear sector:

MANAGES	…sets and implements a **clear vision for cyber** security, supported by organisational strategies and objectives	…**appropriately prioritises cyber** as part of its holistic risk management strategy, based on a shared ambition and risk appetite	…**understands** the overall cyber **threat** and proactively anticipates and identifies changes in threat	…is supported with advice, guidance and enabling, **outcome-focused regulation**
MITIGATES	…proactively **mitigates its cyber risk** at all stages of the nuclear infrastructure and fuel lifecycles	…acts to ensure the cyber security of **new nuclear technologies** and infrastructure.	…proactively manages cyber security risks arising from its **supply chain**	
RESPONDS	…develops effective **cyber incident response plans and regularly test** these	…proactively **monitors its networks and detect incidents** and trends	…**responds promptly and effectively** to cyber incidents, minimising safety, security, operational and reputational impacts	**…recovers swiftly and learns lessons** from cyber incidents
COLLABORATES AND LEARNS	**…works effectively together** to manage common challenges and respond to incidents, and learns from best practice by others	….promotes a **positive culture** and **attracts and retains diverse, suitably qualified, and experienced personnel** into its cyber workforce	….embeds **cyber-secure behaviours** and **culture** throughout its workforce and partners	

3. Sector Maturity and Challenges

To assess the gap between current civil nuclear cyber security and our goal, we conducted a comprehensive gap analysis across the sector. This gathered both quantitative and qualitative data from businesses, the nuclear supply chain, the NCSC and the ONR to identify the major challenges and strengths facing the sector currently, and across the next five years.

3.1 Civil Nuclear Cyber Maturity Benchmarking Assessment

In 2020/21 BEIS used the maturity framework referred to in Figure 6 to conduct a *Cyber Maturity Benchmarking Assessment* across the civil nuclear sector. Chief Information Security Officers (CISOs) responsible for cyber security in nuclear sector organisations assessed themselves across the different criteria, and those results were overlaid by the regulator with their independent regulatory intelligence. This allowed us to look at areas of perceived strength or weakness and aggregate this data from individual organisations to build a sector-wide view. We were also able to compare organisational and regulatory assessments, and look at consistency across the range of scores for individual outcomes.

The assessment highlighted variation in maturity across domains, with regulated domains showing greater maturity than those which were unregulated and OT security being comparatively weaker than IT. The summary report outlined 13 recommendations as set out in Figure 8.

The *Cyber Maturity Benchmarking Assessment* provided both a quantitative assessment of sector maturity which can be used to assess strengths and weaknesses, and a baseline for sector maturity to measure progress against. This CAF-aligned framework will be used twice more during the lifetime of this strategy to assess progress, with the second of these iterations inputting into decision-making for future work.

Figure 8 – A summary of the recommendations from the Civil Nuclear Cyber Maturity Benchmarking Assessment

	RECOMMENDATIONS
1	Focus future cyber improvement initiatives on the areas identified for further development by the *Cyber Maturity Benchmarking Assessment*
2	Further strengthen the approach to information sharing on cyber (e.g. threat intelligence, good practices) and collaboration on cyber security within the sector
3	Continue to support the annual technical cyber exercise programme but also seek to develop a mature cyber incident response exercise programme
4	Support dutyholders to deliver regular, tailored cyber incident response exercises within their organisations in order to drive improvements and strengthen the maturity of their cyber incident response and recovery plans

5	Ensure the cyber security aspects of key sector assessments, documents and strategies that set out the civil nuclear sector's security posture accurately reflects the sector's risk profile and balances cyber security alongside physical and personnel security
6	Support the development of a more mature and holistic approach to supply chain cyber security. An approach where assurance activities are expanded, going beyond the regulated Sensitive Nuclear Information (SNI) supply chain and seeks to develop and adopt an effective baseline standard for the wider supply chain
7	Investigate and support the adoption of new, secure information sharing technologies suiting their organisation's needs to enable greater sharing of sensitive information securely and confidently across dutyholders and their supply chain organisations
8	Further develop the cloud security guidance on cloud adoption so it provides more actionable guidance for dutyholders on how to effectively secure both classified and unclassified information stored in the cloud
9	Learning lessons from the strong safety culture, understand how a strong cyber security culture can be well-embedded within the civil nuclear industry
10	Review whether the security regulations within the civil nuclear sector is still fit-for-purpose in counteracting current and future cyber risks
11	Develop specialist cyber security training to bridge the knowledge gap between safety and cyber security roles as well as raising awareness to the cyber risks facing Operational Technology (OT) systems
12	Encourage collaboration (e.g. sharing learning and good practice) with other sectors who are undoubtedly face similar challenges
13	Support dutyholders to adopt appropriate protective security monitoring and logging solutions for their IT and OT environments to strengthen their cyber security posture, without impacting upon functional safety.

3.2 Sector Engagement

As well as the benchmarking framework assessment, BEIS conducted a number of workshops and other engagements with industry, the ONR and the NCSC. The Civil Nuclear CISO Working Group (CISO WG) – an industry-led cyber collaboration forum for civil nuclear – provided invaluable input on the biggest upcoming challenges for the strategy to address.

Four key themes on challenges emerged as shown in Figure 9. These included challenges already identified by the *Cyber Maturity Benchmarking Assessment*, including supply chain risk management, the need to embed cyber security into new technologies, and the challenge of prioritising cyber security investment against other types of nuclear risk mitigation such as safety, physical security and environmental risk. However, the workshops also identified a number of additional areas for improvement, including the need for a stronger cyber security culture across the sector and the challenge of recruiting and retaining skilled and diverse cyber professionals in often remote locations. Participants in our workshops also repeatedly emphasised the value of support and engagement from their organisational Executive and Board in enabling organisations to achieve their cyber security objectives.

Figure 9 – A summary of the challenges identified through engagements across the sector

RISK MANAGEMENT

- Risks are not always managed holistically, risking security gaps and sub-optimal decisions, especially between the cyber, physical security and safety domains.
- Organisational cyber security strategies are not always clearly articulated, and are often focused on compliance, rather than risk management or cyber as an enabler.
- There is a lack of a common shared understanding of threats and risk appetites. This can lead to prescriptive regulatory interventions.

RISK MITIGATION

- Fast, agile implementation of improvements can be hampered by the significant scale and complexity of legacy operational systems.
- The sector is facing significant, novel cyber security challenges as the technology and cyber threat landscape rapidly evolves.
- Tackling the challenges of supplier assurance and new technology is difficult and requires cross-sector effort.

INCIDENT MANAGEMENT

- Cyber incident response within and across organisations requires more frequent exercising and executive-level support.
- Monitoring of networks and detection of cyber incidents is a key area for improvement.

CULTURE, COLLABORATION AND SKILLS

- The specialist nature of the civil nuclear sector and of cyber security can make recruitment and retention of diverse and suitably skilled personnel difficult. The culture can sometimes lack inclusively.
- Lack of cyber knowledge amongst key personnel and providers means cyber security is not mainstreamed across organisations

3.3 NCSC Threat Assessment

Finally, our gap analysis took into account the likely trends and emerging cyber threats over the lifetime of the strategy. Reflecting the wider UK national picture as set out in the *2021 National Cyber Strategy*, the key threats to civil nuclear are likely to be ransomware, Intellectual Property (IP) theft and an attack via the supply chain, as set out in Figure 10. This assessment of threat, along with the view from industry CISOs and the quantitative overview of sector maturity gives us a good picture of the context we should be writing the strategy within.

Figure 10 – Threat Assessment for the civil nuclear sector over the next five years

RANSOMWARE

Ransomware almost certainly represents the most likely disruptive threat to the UK Civil Nuclear Sector. It's a realistic possibility that current international efforts to combat ransomware will lead to an increase in worldwide attacks in the next 12 months, as ransomware actors seek to maximise their profits before anticipated changes make their operating environment more difficult.

Ransomware will almost certainly continue to be opportunistic based on whether threat actors can obtain access to victims' networks, but within that, favoured target sectors will be chosen based on perceived willingness to pay. Whilst data extortion has become a prominent tactic, the majority of ransomware attacks look

	highly likely to continue relying on encryption to incentivise victims into paying a ransom.
IP THEFT	IP theft will likely remain a persistent threat to industry as a new generation of nuclear technology is emerging. IP on small modular reactors (SMRs) will be attractive targets as foreign states seek to build their domestic capabilities in low-carbon energy systems.
SUPPLY CHAINS	Supply chains as an attack vector almost certainly represent a growing threat to the civil nuclear sector. Actors are developing a better understanding of the civil nuclear industry and its relationship with third parties including managed service providers (MSPs), software vendors and regulators. It is highly likely supply chains will continue to grow as a favoured cyber attack vector.

4. Strategy Themes and Priorities

The gap analysis undertaken against our model of good cyber security identified a number of key areas where the civil nuclear sector should prioritise action over the next five years, and BEIS, the ONR, the nuclear sector and the NCSC have worked closely together to articulate our priority objectives (Figure 11):

Figure 11 - A summary of the overarching goal and objectives of the 2021 Civil Nuclear Cyber Security Strategy

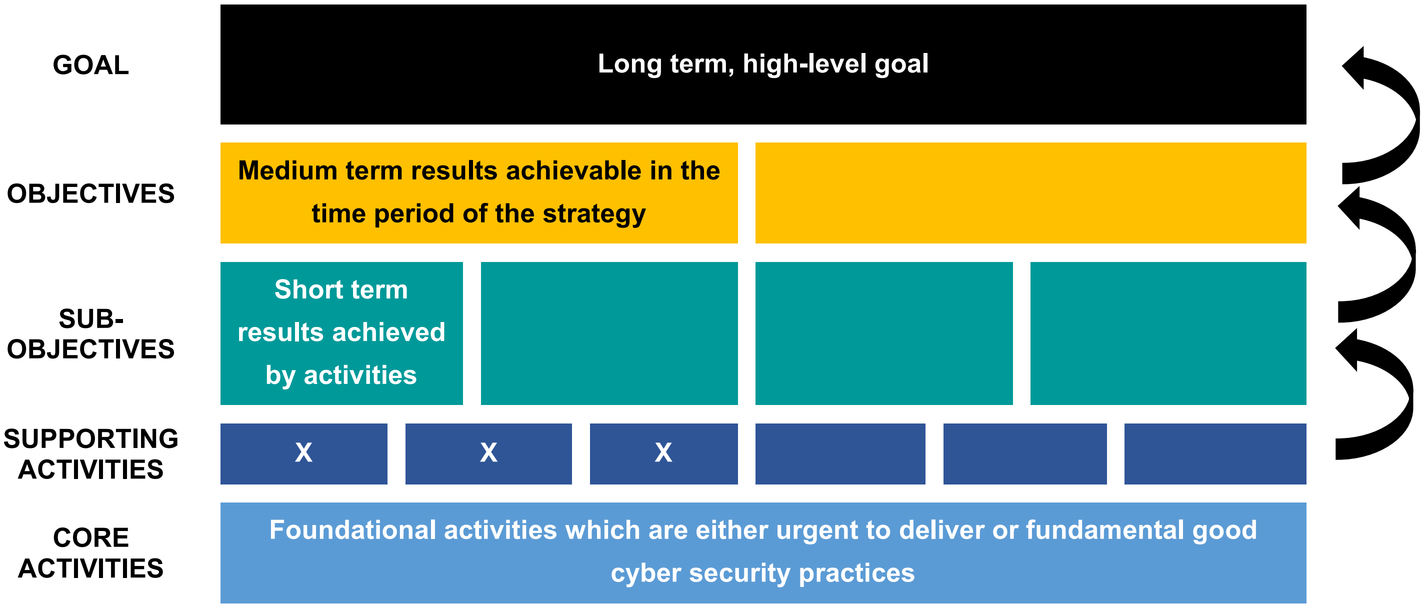
Goal	**The UK civil nuclear sector effectively manages and mitigates cyber risk in a collaborative and mature manner. It is resilient in responding to and recovering from incidents, and promotes a positive security culture.**			
	RISK MANAGEMENT	**RISK MITIGATION**	**INCIDENT MANAGEMENT**	**CULTURE, SKILLS & COLLABORATION**
Objectives	Sector appropriately prioritises cyber security as part of a holistic **risk management** approach underpinned by a common risk understanding and outcome-focused regulation.	The sector and its supply chain takes proactive action to **mitigate** cyber risks in the face of evolving threats, legacy challenges and adoption of new technologies.	The sector enhances its resilience by preparing for, and responding collaboratively to cyber **incidents**, minimising impacts and recovery time	The sector collaborates to increase cyber maturity, develop cyber skills and promote an inclusive and security-minded culture

Supporting the delivery of these five-year objectives are a prioritised set of activities and actions. These activities have been developed jointly by government, nuclear industry organisations, the NCSC and the ONR, and are designed to be owned and delivered across all partners.

This joint approach builds on the success of the *2017 Civil Nuclear Cyber Security Strategy* and recognises that the cyber maturity of the civil nuclear sector is a shared responsibility that cannot be delivered by government, or any organisation, alone. The activities identified draw on the powers and remit of each delivery partner to contribute to the overall achievement of the objectives, and each is assigned a clear owner to facilitate implementation and accountability.

The strategy is structured so that activities are explicitly linked with and contribute towards the outline objectives and overall goal (Figure 12). As the objectives are themselves based upon the sectors areas of relative weakness, this approach ensures we target those actions that will most impact our overall progress.

Figure 12 – Structure of the Civil Nuclear Cyber Security Strategy 2022


GOAL
Long term, high-level goal
OBJECTIVES
Medium term results achievable in the time period of the strategy
SUB-OBJECTIVES
Short term results achieved by activities
SUPPORTING ACTIVITIES
X
X
X
CORE ACTIVITIES
Foundational activities which are either urgent to deliver or fundamental good cyber security practices

4.1 Risk Management

Our objective: The sector appropriately prioritises cyber security as part of a holistic risk management approach underpinned by a common risk understanding, and outcome-focused regulation (Figure 13)**.**

This objective focuses on how cyber risks are considered, prioritised and managed across the sector, including the policies and risk decisions taken within organisations, and the requirements and risk appetite set by Government and the regulator. Recognising the need for a dynamic cyber risk posture, it considers how cyber security is funded compared to other nuclear security risks and seeks to ensure that decision-makers at all levels are informed by an appropriate understanding of organisational threats and vulnerabilities.

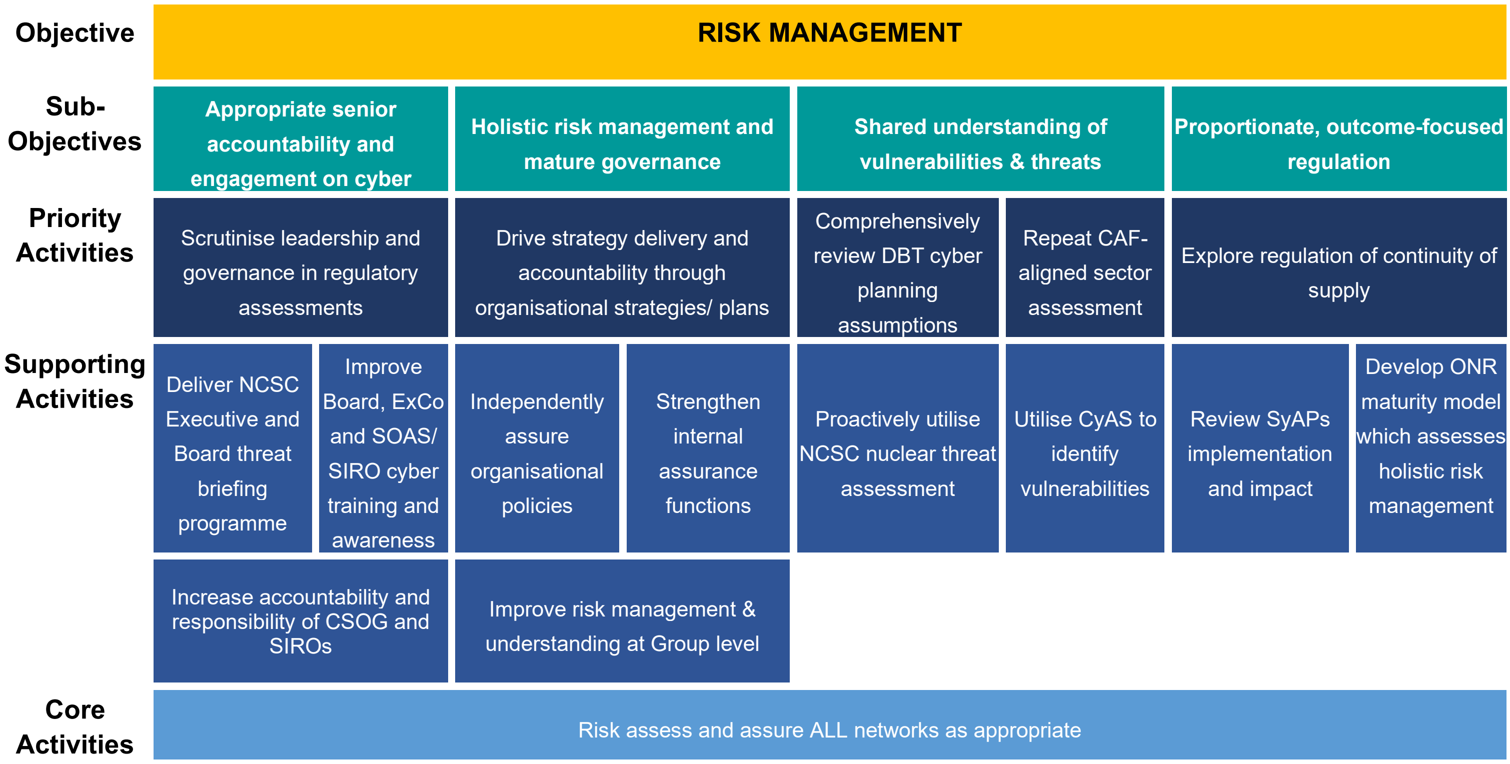
Over the five years of the strategy, we will deliver the following priority and supporting activities on risks management:

- Ensure appropriate **engagement and accountability at a senior level** within organisations across the sector by: explicitly assessing leadership and governance criteria in the ONR regulatory assessments of civil nuclear dutyholders; providing organisational Boards with cyber threat briefings improving Board and Executive Committee cyber awareness and training; and holding senior decision-makers more strongly to account through cross-sector governance.
- Support a **holistic risk management approach** to cyber security and deliver **mature governance** structures by: driving strategy delivery and accountability through organisational implementation plans; improving risk management and understanding at corporate group level; risk assessing and assuring all networks as appropriate; and strengthening assurance – both through the creation of internal assurance

functions within organisation, and the increased utilisation of external, independent assurance of policies and plans.

- Maintain a **shared understanding of cyber threats and vulnerabilities** by: repeating the CAF-aligned dutyholder self-assessment to identify strategic vulnerabilities and weaknesses as they arise; proactively utilising NCSC's annual sector threat assessment; and deploying threat-informed assurance such as the CyAS framework to identify system-level vulnerabilities. BEIS will also review the Design Basis Threat (DBT) – the threat planning assumptions for the civil nuclear sector – to ensure the cyber threat described is kept current and drives appropriate investment decisions.
- Ensure a continued **proportionate and outcome-focused regulatory approach** by: reviewing the implementation of the SyAPs; develop a holistic risk assessment maturity model for regulatory assessments; and explore whether the civil nuclear generating fleet should be regulated to maintain a level of electricity provision to the National Grid, in line with other UK electricity generators.

Figure 13 – A summary of the Risk Management objective and its priorities and supporting activities



Objective: RISK MANAGEMENT

Sub-Objectives:
- Appropriate senior accountability and engagement on cyber
- Holistic risk management and mature governance
- Shared understanding of vulnerabilities & threats
- Proportionate, outcome-focused regulation

Priority Activities:
- Scrutinise leadership and governance in regulatory assessments
- Drive strategy delivery and accountability through organisational strategies/ plans
- Comprehensively review DBT cyber planning assumptions
- Repeat CAF-aligned sector assessment
- Explore regulation of continuity of supply

Supporting Activities:
- Deliver NCSC Executive and Board threat briefing programme
- Improve Board, ExCo and SOAS/ SIRO cyber training and awareness
- Independently assure organisational policies
- Strengthen internal assurance functions
- Proactively utilise NCSC nuclear threat assessment
- Utilise CyAS to identify vulnerabilities
- Review SyAPs implementation and impact
- Develop ONR maturity model which assesses holistic risk management
- Increase accountability and responsibility of CSOG and SIROs
- Improve risk management & understanding at Group level

Core Activities: Risk assess and assure ALL networks as appropriate

4.2 Risk Mitigation

Our objective: The sector and its supply chain takes proactive action to mitigate cyber risks in the face of evolving threats, legacy challenges and adoption of new technologies (Figure 14)**.**

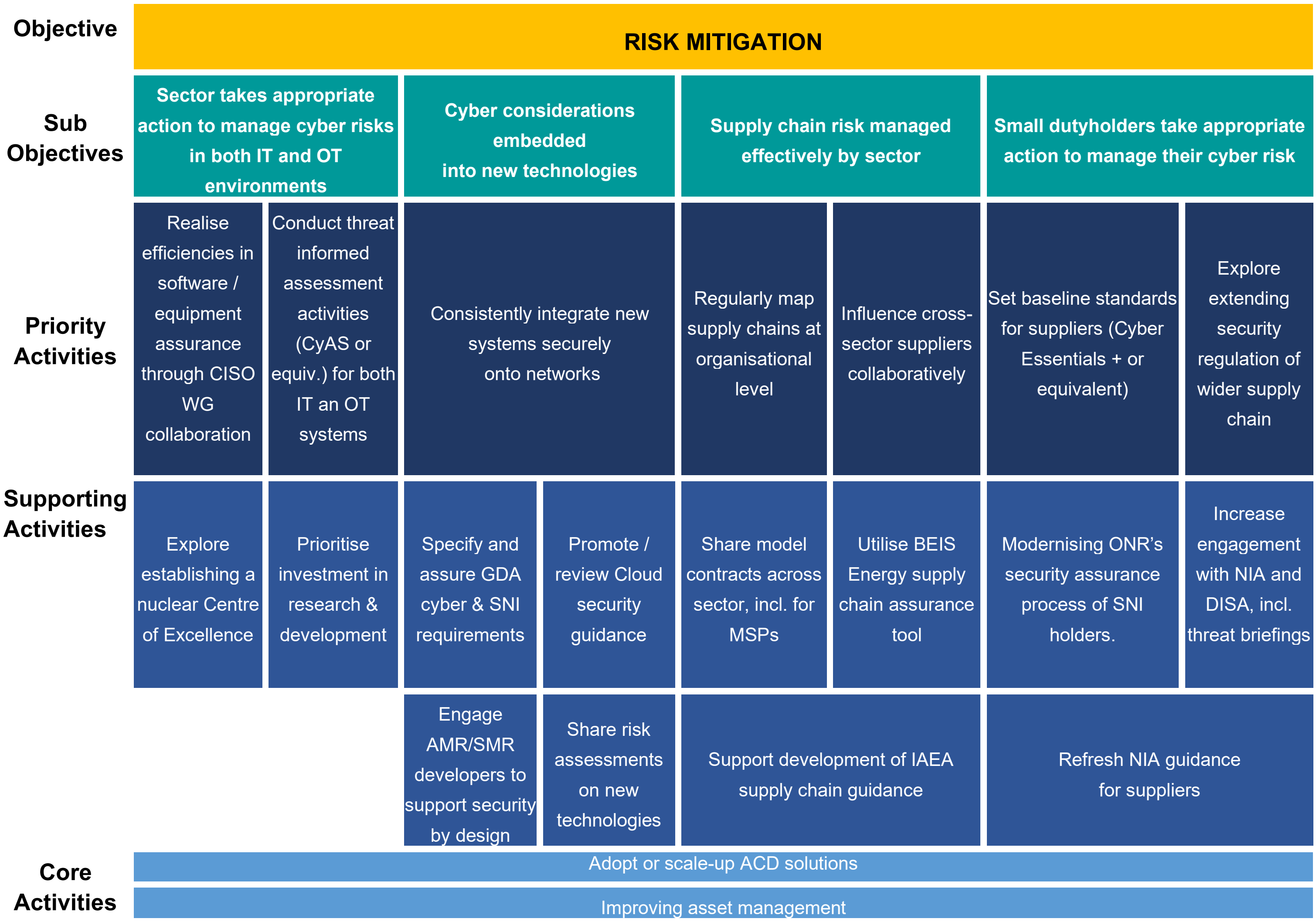
Under this objective we outline how the sector can mitigate the specific risks posed to the IT and OT environments, including by new technologies and the supply chain.

The activities which will help us achieve this objective of the next five years are:

- **Mitigating cyber risks within and across IT and OT domains**, by: sharing and improving approaches to software and equipment assurance across the sector, building on the NCSC's assurance principles and using appropriate tools (including Active Cyber Defence) as they become available; conducting threat-informed assessment activities through frameworks like CyAs; improving asset management; investigating the development of a sector Centre of Excellence to share knowledge and expertise; and continuing to prioritise investment in Research & Development (R&D).

- Ensuring **cyber security is embedded into the deployment of new nuclear and digital technologies** by: integrating new systems securely onto networks systems; reviewing and better promoting existing Cloud Security guidance; and sharing risk assessments on new technologies. As advanced nuclear technologies continue to develop, we will engage closely with developers of Small Modular Reactors (SMRs) and Advanced Modular Reactors (AMRs) on cyber security considerations, and ensure that the ONR's Generic Design Assessment (GDA) process, by which the ONR approves new reactor designs, has cyber and information security requirements (including for Sensitive Nuclear Information (SNI)) built in.
- Effective management of **supply chain cyber risk** by the nuclear sector by: regular mapping of supply chains; sharing of model third party contracts; working jointly with suppliers and trade associations (including the Defence Industry Security Association, DISA and the Nuclear Industry Association, NIA) to support and encourage their cyber security, promoting international guidance on supply chain security being developed by the IAEA, and utilising existing best practice toolkits such as the supply chain assurance tool developed by BEIS.
- Support the **nuclear supply chain to take appropriate action to manage their own cyber risk**, by: increasing engagement with supply chain industry groups, including provision of cyber threat briefings; and working with trade associations to refresh and promote its guidance for suppliers. Additionally, nuclear organisations will set baseline cyber and information security standards for suppliers; the ONR will benchmark the existing cyber security maturity of holders of SNI; and BEIS will consider the case for regulation of cyber security in the supply chain.

Figure 14 – A summary of the Risk Mitigation objective and its priority and supporting activities



Objective	**RISK MITIGATION**							
Sub Objectives	**Sector takes appropriate action to manage cyber risks in both IT and OT environments**		**Cyber considerations embedded into new technologies**		**Supply chain risk managed effectively by sector**		**Small dutyholders take appropriate action to manage their cyber risk**	
Priority Activities	Realise efficiencies in software / equipment assurance through CISO WG collaboration	Conduct threat informed assessment activities (CyAS or equiv.) for both IT an OT systems	Consistently integrate new systems securely onto networks		Regularly map supply chains at organisational level	Influence cross-sector suppliers collaboratively	Set baseline standards for suppliers (Cyber Essentials + or equivalent)	Explore extending security regulation of wider supply chain
Supporting Activities	Explore establishing a nuclear Centre of Excellence	Prioritise investment in research & development	Specify and assure GDA cyber & SNI requirements	Promote / review Cloud security guidance	Share model contracts across sector, incl. for MSPs	Utilise BEIS Energy supply chain assurance tool	Modernising ONR's security assurance process of SNI holders.	Increase engagement with NIA and DISA, incl. threat briefings
			Engage AMR/SMR developers to support security by design	Share risk assessments on new technologies	Support development of IAEA supply chain guidance		Refresh NIA guidance for suppliers	
Core Activities	Adopt or scale-up ACD solutions							
	Improving asset management							

4.3 Incident Management

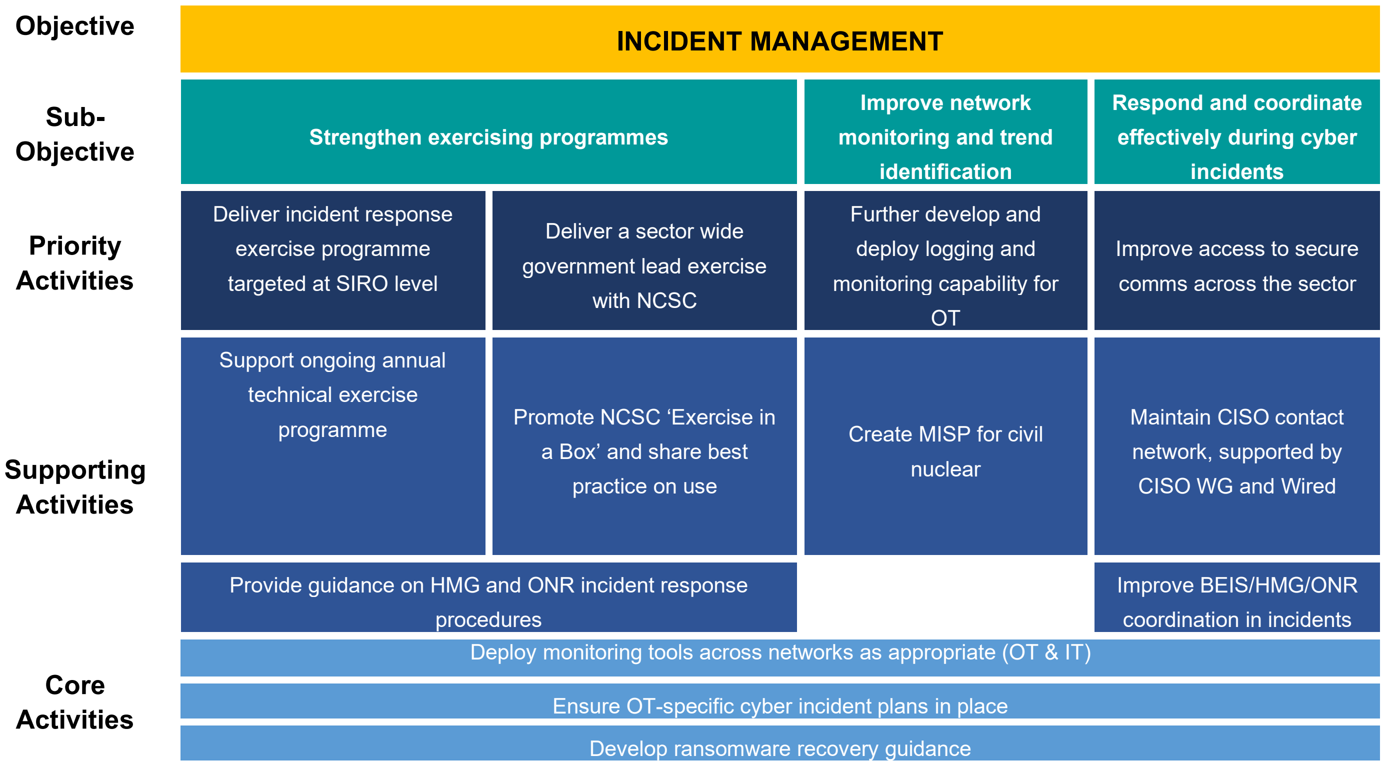
Our objective: The sector enhances its resilience by preparing for, and responding collaboratively to cyber incidents, minimising impacts and recovery time (Figure 15)**.**

Incident management is an area which we saw a particular increase in maturity during the period of the last strategy, with government response planning and an annual programme of sector-wide technical exercising beginning. This progress should be continued and maintained. However, an area of relative weakness as identified through the *Cyber Security Maturity Assessment* was active logging and monitoring of systems to ensure abnormal activity and trends are identified and mitigated, and network monitoring is therefore a key objective of this strategy.

In the coming strategy period we will:

- **Strengthen exercising programmes** by: delivering exercising targeted at senior decision-makers and undertaking an ambitious live exercise in addition to maintaining the sector-wider annual technical exercising programme. Response guidance for the sector will also be reviewed, monitoring tools deployed where appropriate and the NCSC exercising tools promoted.
- Improve **network monitoring, logging and identification of trends** by: further integrating ACD and other tools, and creating a Civil Nuclear Malware Information Sharing Platform (MISP): a machine-to-machine information sharing platform for threat intelligence.
- **Respond and coordinate effectively during cyber incidents** by: improving access to secure communications capabilities; ensuring OT specific plans are in place for managing cyber incidents; improving CISO cross-sector engagement and coordination; developing ransomware recovery guidance; and continuing to improve incident coordination between government and the regulator.

Figure 15 – A summary of the Incident Management objective and its priority and supporting activities



Objective	**INCIDENT MANAGEMENT**			
Sub-Objective	**Strengthen exercising programmes**		**Improve network monitoring and trend identification**	**Respond and coordinate effectively during cyber incidents**
Priority Activities	Deliver incident response exercise programme targeted at SIRO level	Deliver a sector wide government lead exercise with NCSC	Further develop and deploy logging and monitoring capability for OT	Improve access to secure comms across the sector
Supporting Activities	Support ongoing annual technical exercise programme	Promote NCSC 'Exercise in a Box' and share best practice on use	Create MISP for civil nuclear	Maintain CISO contact network, supported by CISO WG and Wired
	Provide guidance on HMG and ONR incident response procedures			Improve BEIS/HMG/ONR coordination in incidents
Core Activities	Deploy monitoring tools across networks as appropriate (OT & IT)			
	Ensure OT-specific cyber incident plans in place			
	Develop ransomware recovery guidance			

4.4 Culture, Collaboration and Skills

Our objective: The sector collaborates to increase cyber maturity, develop cyber skills and promote an inclusive and security-minded culture.

With budgetary and personnel resource constraints, this objective is increasingly important for the Civil Nuclear sector's cyber security maturity. During the five year life of this strategy we aim to:

- **Collaborate across the sector to tackle common challenges** by: increasing information sharing and resources across common platforms; building upon the success of the cross-nuclear CISO WG to develop solutions to common challenges; providing support and resources to new CISOs; creating a lessons learned group on the NCSC's Cyber Security Information Sharing Partnership (CISP); and collaborating internationally to develop guidance and best practice.
- **Improve the skills and experience of nuclear cyber security professionals by:** articulating cyber skills required for non-cyber expert roles; promoting and establish mentoring and reverse mentoring programmes; and supporting inter-sector and intra-sector secondments, apprenticeships and graduate schemes as well as the i100 scheme. **Promote a positive security culture by**: building on the Chilcott Report and other research to track progress towards avoiding group-think and improving diversity of thought; and setting organisational objectives on promoting a diverse and inclusive workforce.
- **Embedding cyber security training and accountability across organisations** by: adopting basic cyber training across all personnel and supporting training in the supply chain; developing a cyber Community of Interest (COI) for engineers and operational technology personnel through a cross-sector training programme; continuing to review cyber security culture in the ONR's regulatory assessments; and promoting the use of the security culture self-assessment tool[10] developed by the Centre for the Protection of National Infrastructure (CPNI), the UK's national technical authority for physical, personnel and protective security.

[10] https://www.cpni.gov.uk/secure-4-assessing-security-culture

Figure 16 – A summary of the Culture, Collaboration and Skills objective and its priorities and supporting activities

Objective	**CULTURE, COLLABORATION AND SKILLS**					
Sub-Objectives	**Collaboration across sector to tackle shared challenges**		**Improve skills and experience of nuclear cyber professionals and promote a positive security culture**		**Embed cyber security training and accountability across organisations**	
Priority Activities	Increase information sharing across common platforms		Articulate cyber skills required for non-cyber expert roles			
Supporting Activities	Create CISO resource pack to facilitate information- and best practice-sharing	Maximise use of CISO WG network to tackle common challenges and develop cross-sector solutions	Build on Chilcott Report and other research to track progress towards avoiding group-think and promoting a positive security culture	Continue and extend cyber apprentice graduates and i100 scheme	Develop cyber COI for engineering personnel through cross-sector training programme	Scrutinise organisational cyber security culture through regulatory activities
	Collaborate internationally to develop guidance and share practice	Create a lessons learned CISP Group	Promote / establish mentoring and reserve mentoring programmes	Support secondments (cross-sector and beyond nuclear)	Adopt basic cyber training across all sector personnel	Promote use of CPNI security culture assessment tool
			Set organisational objectives to promote a diverse and inclusive workforce		Drive adoption of cyber security training within supply chain	

5. Implementation and Monitoring

To achieve the stated objectives and deliver the activities set out in this strategy, a sector-wide effort and prioritisation is required. Investment, resource and commitment from senior leadership is necessary to drive the required business change: we estimate that nuclear sector organisations would need to dedicate 5-10% of their annual organisational change capacity to cyber to successfully deliver the strategic outcomes. This change capacity is critical as the outcomes cannot be achieved by security teams alone but need active support from all areas of each business. Change capacity will be measured and managed in different ways by different organisations but may include resourcing and staffing, 'airtime' from leadership and communications campaigns, and the proportion and prioritisation of technical change requests and new projects on cyber security improvements as opposed to new business functionality, as well as other measures.

5.1 Priority and Core Activities

To achieve the ambition we have set out, implementation of the strategy and delivery of the priority and supporting activities will be monitored and evaluated on an annual basis. 18 priority activities (outlined in Figure 17) have been identified based on their transformative potential and high impact, and/or because they require collective and coordinated action across the sector. These priority actions will be implemented to collectively agreed timelines.

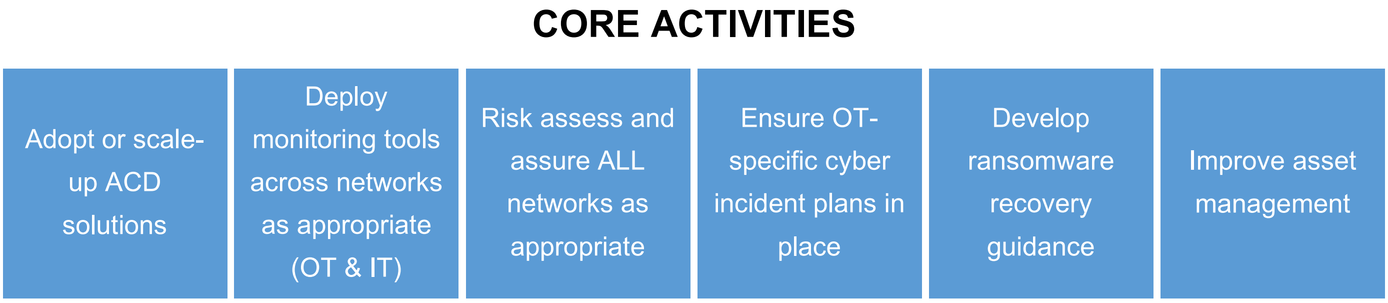
Figure 17 – A summary of the priority activities that will be centrally coordinated and implemented

Risk Management	Scrutinise leadership and governance in regulatory assessments	Drive strategy delivery and accountability through organisational strategies / plans	Comprehensively review DBT cyber planning assumptions	Repeat CAF-aligned sector assessment	Explore regulation of continuity of supply		
Risk Mitigation	Realise efficiencies in software/equipment assurance through CISO WG collaboration	Conduct threat informed assessment activities (CyAS or equiv) for both IT and OT systems	Integrate new systems securely onto networks	Regularly map supply chains at organisational level	Influence cross-sector suppliers collaboratively	Set baseline standards for suppliers (Cyber Essentials + or equiv	Explore extending security regulation of wider supply chain
Incident Management	Deliver incident response exercise programme targeted at SIRO level	Deliver a sector wide government lead exercise with NCSC	Further develop and deploy logging and monitoring capability for OT	Improve access to secure comms across the sector			
Culture, Collaboration and Skills	Share information across common platforms	Articulate cyber skills required for non-cyber expert roles					

The supporting activities will be implemented by each delivery partner in line with its own internal planning and prioritisation. All delivery partners have committed to producing an individual implementation plan or strategy which demonstrates how they will deliver the activities which they own or support. Although in some cases supporting activities may not be relevant to all delivery partners, the following 'core activities' are considered either urgent to deliver, or fundamental good cyber security practice which all nuclear sector organisations should prioritise for early implementation if not already in place:

- Adopt available Active Cyber Defence (ACD) tools.
- Deploy monitoring tools across all relevant operational technology and information systems to identify abnormal activity and trends.
- Undertake continuous risk assessment and assurance of all relevant networks.
- Ensure incident response plans are in place for cyber-security attacks on operational technology and networks, as well as IT networks.
- Develop ransomware recovery guidance and plans to support organisational business recovery following an incident.
- Ensure all critical cyber and information assets are identified and managed appropriately.

Figure 18 – A summary of the core activities ('getting the basics right') to implement during the first 3 years of the 2021 strategy



CORE ACTIVITIES

Adopt or scale-up ACD solutions

Deploy monitoring tools across networks as appropriate (OT & IT)

Risk assess and assure ALL networks as appropriate

Ensure OT-specific cyber incident plans in place

Develop ransomware recovery guidance

Improve asset management

5.2 Implementation and Monitoring

Learning from the 2017 strategy showed that a more directive and demonstratable strategy methodology was required and so this strategy will take a programmatic approach to its delivery. This includes a high-level roadmap for the priority and core activities as set out in Figure 20, which will be supplemented by a range of supporting activities continuing throughout the strategy's timeline. All activities will be monitored and evaluated against a series of indicators and milestones.

Delivery of the strategy will be overseen and monitored by the CSOG, the senior cross-sector forum looking at strategic issues pertaining to the strategy. CSOG will be supported by a dedicated Delivery Oversight Board (DOB), alongside annual reporting requirements which will assess strategy activity delivery.

In addition, the CAF aligned sector *Cyber Security Maturity Assessment* will be carried out at the mid-point and end-point of the strategy to objectively monitor cyber security improvements, and evaluate whether our programmed activities are having the required impact towards achieving our overall goal. The strategy activities and priorities will be reassessed and baselined at the mid-strategy point if required. This may result from changing threat and context, lessons or vulnerabilities identified from incidents, and/or evaluation of the value the activities are delivering.

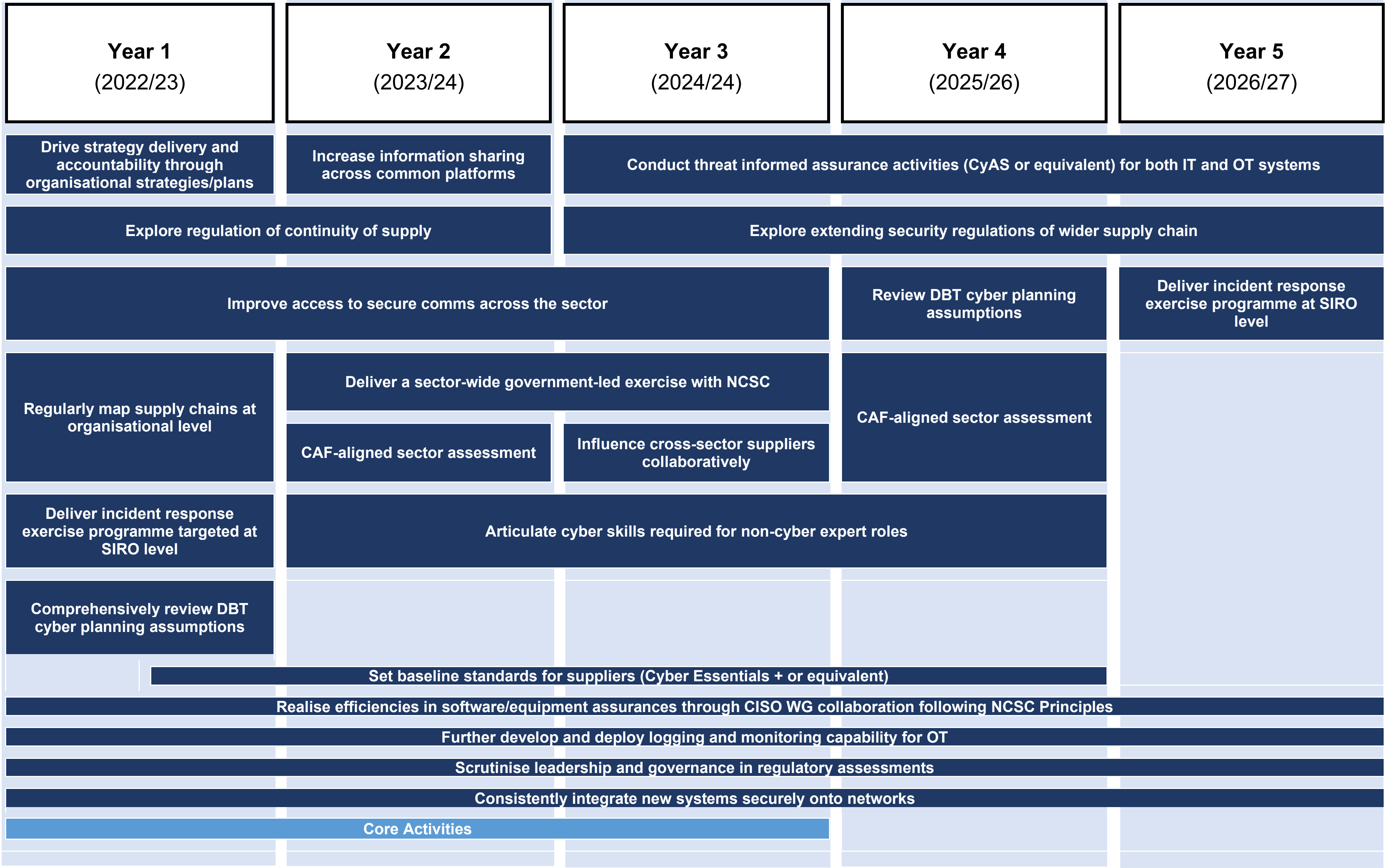
5.3 Roles and Responsibilities for Strategy Delivery

A clear and shared understanding of the roles and responsibilities for implementing the *2022 Civil Nuclear Cyber Security Strategy* is crucial for meaningful and timely delivery. Each activity is owned by a designated delivery partner, as set out in Annex A. Figure 19 articulates the summary of the roles and responsibilities for each delivery partner.

Figure 19 – A table outlining the roles and responsibilities for the implementation of the strategy

DELIVERY PARTNER		ROLE AND RESPONSIBILITIES
Industry	Nuclear Organisations	As owners and operators, industry bear the primary responsibility for managing and continuously improving their organisation’s cyber and information security arrangements. In addition, they are responsible for assuring the security of their supply chain and proactively encouraging them to strengthen their security arrangements.
	Supply Chain	The civil nuclear supply chain is responsible for managing and continuously improving their organisation’s cyber and information security arrangements.
ONR		As the civil nuclear sector regulator for nuclear safety, security and safeguards, ONR is responsible for monitoring and enforcing regulations to drive individual and sector-wide improvements on cyber and information security. In alignment with ONR’s regulatory priorities, ONR will actively contribute to and support industry in fulfilling the relevant activities set out in this strategy. It will also continue to provide assurances to the government on the overall security of the sector.
BEIS		As the lead government department for civil nuclear, BEIS will take an enabling role and will set the strategic direction to ensure that the UK’s regulatory framework is proportionate and fit-for-purpose. BEIS will coordinate the monitoring the implementation of the strategy through the DOB and the CSOG governance mechanisms.
NCSC		As the UK’s technical authority for cyber security, the NCSC will provide specialist advice and support to the sector on cyber security, including timely cyber threat and vulnerability intelligence.

Figure 20 – A high-level roadmap of the priority and core activities to deliver from the 2021 strategy



Year 1 (2022/23)

Year 2 (2023/24)

Year 3 (2024/24)

Year 4 (2025/26)

Year 5 (2026/27)

Drive strategy delivery and accountability through organisational strategies/plans

Increase information sharing across common platforms

Conduct threat informed assurance activities (CyAS or equivalent) for both IT and OT systems

Explore regulation of continuity of supply

Explore extending security regulations of wider supply chain

Improve access to secure comms across the sector

Review DBT cyber planning assumptions

Deliver incident response exercise programme at SIRO level

Regularly map supply chains at organisational level

Deliver a sector-wide government-led exercise with NCSC

CAF-aligned sector assessment

Influence cross-sector suppliers collaboratively

CAF-aligned sector assessment

Deliver incident response exercise programme targeted at SIRO level

Articulate cyber skills required for non-cyber expert roles

Comprehensively review DBT cyber planning assumptions

Set baseline standards for suppliers (Cyber Essentials + or equivalent)

Realise efficiencies in software/equipment assurances through CISO WG collaboration following NCSC Principles

Further develop and deploy logging and monitoring capability for OT

Scrutinise leadership and governance in regulatory assessments

Consistently integrate new systems securely onto networks

Core Activities

Annex A – A Full List of Strategy Activities

A table outlining a full list of activities from the 2022 Civil Nuclear Cyber Security Strategy and their owners. (Priority activities in bold, core activities in italics)

FULL LIST OF STRATEGY ACTIVITIES				
Sub-Objective	**ID**	**Activity**	**Description of Activity**	**Owner**
RISK MANAGEMENT				
Appropriate senior accountability and engagement on cyber	**1**	**Scrutinise leadership and governance in regulatory assessments**	**ONR will explicitly assess cyber leadership and governance in its regulatory assessments of civil nuclear dutyholders, recognising its importance as a strategic enabler of cyber security.**	**ONR**
	2	Deliver NCSC Executive and Board threat briefing programme	Delivery of NCSC’s cyber threat briefings at the Executive and Board-level across the civil nuclear sector, to support senior awareness of the cyber threat, and inform appropriate decision-making.	NCSC
	3	Improve Board, Executive Committee and Senior Information Risk Owner (SIRO) cyber training and awareness	Improvements to cyber awareness and training at the senior level (i.e. Board, ExCo and SIROs) across the civil nuclear sector to strengthening capabilities and confidence on managing cyber security risks.	Industry
	4	Increase accountability and responsibility of the Cyber	Ensure appropriate engagement, accountability and responsibilities at a senior-level (e.g. Executives, SIROs)	ONR BEIS

		Security Oversight Group (CSOG) and SIROs	across the civil nuclear sector. Senior executives in the civil nuclear sector often deal with a multitude of risks, of which cyber forms only a part. However, cyber security cannot be achieved without significant senior support and increased accountability.	
Holistic risk management and mature governance	**5**	**Drive strategy delivery and accountability through organisational strategies/plans**	**Civil nuclear organisations will develop implementation plans to demonstrate how they will implement their commitments under the *2022 Civil Nuclear Cyber Security Strategy.***	**Industry**
	6	Independently assure organisational policies	Increase use of external, independent assurance of organisational cyber policies and plans to support quality risk judgements and mitigate the risk of group-think.	Industry
	7	Strengthen internal assurance functions	Establish and maintain internal assurance functions within organisations to support quality risk judgements and mitigate the risk of group-think.	Industry
	8	Improve risk management and understanding at Group level	Improve cyber risk management and understanding at the corporate group level whilst ensuring clarity in respect to risk ownership and regulatory responsibility.	Industry
	9	*Risk assess and assure all networks as appropriate*	*Both OT and IT systems should be appropriately risk assessed on a regular basis to support informed and proportionate risk judgements.*	*Industry*
Shared understanding of	**10**	**Comprehensively review the cyber planning assumptions in the DBT**	**The DBT will undergo a comprehensive review to ensure that the cyber threat planning assumptions accurately reflect the civil nuclear sector's current threat profile and drive appropriate investment decisions**	**BEIS**

vulnerabilities and threats	**11**	**Repeat CAF-aligned sector assessment**	**Repeat the sector-wide assessment against the CAF and SyAPs aligned framework on a biennial basis, to provide a sector-wide view on cyber security and identify strategic vulnerabilities and weaknesses as they arise. This will be a self-assessment overlaid with regulatory intelligence.**	**ONR**
	12	Proactively utilise NCSC nuclear threat assessment	Proactively utilise the NCSC's annual civil nuclear cyber threat assessments to inform risk management decisions.	Industry
	13	Utilise the Cyber Adversary Simulation framework to identify vulnerabilities	Deploy threat-informed assurance activities to identify system-level vulnerabilities.	Industry
Proportionate, outcome-focused regulation	**14**	**Explore regulation of continuity of supply**	**Investigate regulating the cyber security of civil nuclear generation for continuity of electricity supply, alongside existing nuclear safety, security and safeguarding requirements.**	**BEIS**
	15	Review SyAPs' implementation and impact	Review the implementation and impact of the ONR's regulatory security framework, the Security Assessment Principles (SyAPs), to identify learning and any remaining gaps.	ONR
	16	Develop ONR maturity model which assesses holistic risk management	Refine the ONR's maturity model which supports regulatory assessments of civil nuclear dutyholders, in order to holistically assess safety and security risk management.	ONR
RISK MITIGATION				
Sector takes appropriate action to	**17**	**Realise efficiencies in software and equipment assurance through CISO**	**Maximise efficiencies in assuring software and equipment by sharing approaches, processes and**	**Industry**

manage cyber risks in both IT and OT environments		**Working Group collaboration**	**judgements across the sector, based on the NCSC assurance principles.**	
	18	**Conduct threat informed assessment activities (CyAS or equivalent) for both IT and OT systems**	**Conducting threat-informed assessment activities (e.g. CyAS or equivalent) for live-testing and assuring both IT and OT systems.**	**Industry**
	19	Explore establishing a nuclear Centre of Excellence	Investigate the development of a sector-wide Centre of Excellence to identify and maximise opportunities for sharing knowledge and resources across the sector.	Industry (NDA)
	20	Prioritise investment in Research and Development	Prioritise existing, and develop new, collaborative research and development opportunities to mitigate IT & OT risks in existing and new nuclear technology.	Industry
	21	*Improving asset management*	*Strong asset management is essential for making appropriate risk assessments and judgements. It needs to be improved in line with relevant standards and organisational procedures, where not already done so.*	*Industry*
	22	*Adopt or scale-up Active Cyber Defence (ACD) solutions*	*ACD solutions are highly successful in combatting common cyber threats and attacks before they even reach the end user of a system. ACD is already used widely in the sector but remains an important tool and should be scaled up or adopted where not already done so.*	*Industry*
Cyber considerations embedded into new technologies	**23**	**Integrate new systems securely onto networks**	**Consistently integrate new systems securely onto networks by recognising and effectively managing the inherent cyber risk in all change activities.**	**Industry**
	24	Specify and secure Generic Design Assessment (GDA)	Ensure that the ONR's GDA process has effective cyber security and information security standards embedded	ONR

		requirements for cyber and Sensitive Nuclear Information	alongside safety, wider security, environmental protection and waste management standards from the outset of the design process.	
	25	Promote/review Cloud security guidance	Review and promote existing Cloud security guidance to ensure it remains relevant, up-to-date and widely known across the sector, facilitating best practice.	Industry
	26	Engage developers of Small and Advanced Modular Reactors to support security by design	Engage closely with developers of Small Modular Reactors and Advanced Modular Reactors to embed effective cyber security standards in the design stage of new reactor development.	ONR
	27	Share risk assessments on new technologies	Share risk assessments on new technologies across the sector to increase efficiency and share best practice and judgements.	Industry
Supply chain risk managed effectively by sector	28	**Regularly map supply chains at organisational level**	**Organisations to regularly map their supply chains to identify those providing critical services and products.**	**Industry**
	29	**Influence cross-sector suppliers collaboratively**	**Utilise existing forums for coordinating assurance activities for and influencing sector-wide suppliers more collaboratively.**	**Industry**
	30	Utilise BEIS Energy supply chain assurance tool	Utilise existing best practice on supply chain management through the sector-agnostic supply chain assurance tool developed by BEIS.	Industry
	31	Support development of IAEA supply chain guidance	Contribute to and promote international guidance on supply chain security being developed by the IAEA.	ONR

	32	Share model contracts across sector, incl. for MSPs	Share examples or templates for third party contracts across the sector in order to promote best practice and simplify compliance for suppliers supporting multiple nuclear organisations.	Industry
Small dutyholders take appropriate action to manage their cyber risk	**33**	**Set baseline standards for suppliers (Cyber Essentials + or equivalent)**	**Organisations will set contractual cyber security standards for suppliers (Cyber Essentials+ or equivalent), to drive up cyber security across the supply chain.**	**Industry**
	34	**Explore extending security regulation of wider supply chain**	**Conduct a sectoral risk assessment on security threats to, and vulnerabilities of, the civil nuclear supply chain to clearly articulate and evidence the risk. This will inform reviews on expanding the scope of security regulations.**	**BEIS**
	35	Modernising ONR's security assurance process of SNI holders	Delivery of the modernisation programme for ONR's security assurance process of SNI holders.	ONR
	36	Refresh the Nuclear Industry Association's guidance for suppliers	Supply chain industry groups and trade associations to refresh and promote its guidance for suppliers operating in the civil nuclear industry.	Supply Chain
	37	Increase engagement with industry associations, including through the provision of threat briefings	Increase engagement with supply chain industry groups and trade associations (e.g. Nuclear Industry Association and Defence Industry Security Association) to raise awareness of the threat and promote best practice.	BEIS, ONR
INCIDENT RESPONSE				
	38	**Deliver incident response exercise programme**	**Deliver an incident response exercise programme targeted at the senior level decision-makers (e.g. SOAS, SIRO) from across the civil nuclear sector, in order to**	**BEIS**

Strengthen exercising programmes		**targeted at SOAS/SIRO level**	**raise awareness of likely cyber threat scenarios, test senior decision-making processes, and encourage cross-sector working in the event of an incident.**	
	39	**Deliver a sector wide government led exercise with the NCSC**	**Deliver a sector-wide live incident response exercise at the strategic-level, building on the learning from the annual technical exercises and the senior TTXs to stretch and test our processes and response, and identify learning.**	**BEIS**
	40	Support ongoing annual technical cyber exercise programme	Continue the highly successful sector-wide technical cyber exercises delivered annually, which bring together cyber and incident response teams across the sector to respond to a challenging set of cyber attack scenarios.	BEIS Industry (NDA)
	41	Promote guidance on HMG and ONR incident response procedures	Regularly review and promote cyber incident response guidance for the civil nuclear sector, to facilitate effective joint working with the ONR and with BEIS in the event of a cyber incident.	BEIS ONR
	42	Promote the NCSC's *Exercise in a Box* and share best practice on use	Promote the NCSC's *Exercise in a Box* (an online tool developed by the NCSC for organisations to test and practice their response to a cyber attack) and share best practice on its use.	NCSC
Improve network monitoring trend identification	**43**	**Further develop and deploy logging and monitoring capability for OT**	**Further develop and deploy logging and monitoring capability for OT environments. We want to replicate the success of ACD tools in corporate IT systems by developing OT equivalents, where logging and monitoring can be more challenging.**	**Industry**
	44	Create MISP for civil nuclear	Create a Civil Nuclear Malware Information Sharing Platform (MISP) to foster the sharing of cyber threat intelligence and	NCSC

			cyber security indicators across the civil nuclear cyber community.	
	45	*Deploy monitoring tools across networks as appropriate*	*As per the recommendation from the Civil Nuclear Maturity Assessment, nuclear organisations should deploy monitoring tools across their networks.*	*Industry*
Respond and coordinate effectively during cyber incidents	**46**	**Improve access to secure comms across the sector**	**Improve access to secure communications capabilities to ensure those who have a legitimate use case have the capability and to improve sharing of sensitive information across the sector.**	**Industry**
	47	Maintain CISO contact network, supported by CISO WG and WiRed	Regularly review and maintain the CISO network to facilitate CISO engagement across the civil nuclear sector, as well as support timely and dynamic communications in an incident.	Industry
	48	Improve BEIS/HMG/ONR coordination in incidents	Continuously identify opportunities to strengthen coordination between Government and the regulator during cyber incidents and notable cyber events.	BEIS ONR
	49	*Develop ransomware recovery guidance*	*The NCSC will develop ransomware recovery guidance to support civil nuclear organisations in preparing for, and recovering from, a successful ransomware attack.*	*NCSC*
	50	*Ensure OT-specific cyber incident response plans are in place*	*It is crucial that incident response plans are in place for both corporate and operational systems, which may require different capabilities and processes, and which may need to take into account different risks and considerations.*	*Industry*
CULTURE, COLLABORATION AND SKILLS				
Collaboration across sector	**51**	**Share information across common platforms**	**Promote sector-wide collaboration and proactive sharing of information sharing across common**	**Industry ONR**

to tackle shared challenges			**platforms, including the Hub, Ecosystem, CISP, MISP and WiRed.**	
	52	Create CISO resource pack to facilitate information and best practice-sharing	Create a Civil Nuclear CISO resource pack to facilitate sharing of information and best practice, and support new CISOs joining the civil nuclear sector.	Industry
	53	Collaborate internationally to develop guidance and share practice	Collaborate internationally to develop guidance and participate in peer reviews to share best practice and drive improvements.	BEIS ONR
	54	Maximise use of CISO WG network to tackle common challenges and develop cross-sector solutions	Maximise use of industry and sector-wide forums to tackle common challenges and collaboratively develop sector-wide solutions.	Industry
	55	Create a lessons learned group via the Cyber Security Information Sharing Partnership (CISP)	Create a lessons learned group on the NCSC CISP platform for civil nuclear to collectively share and identify lessons from cyber incidents and events.	NCSC
Improve the skills and experience of nuclear cyber professionals and promote a positive security culture	**56**	**Articulate cyber skills required for non-cyber roles**	**Pilot an articulation of the cyber skills required for non-cyber expert roles in an organisation, in order to inform cross-organisation cyber training needs, and support recruitment and induction processes.**	**Industry**
	57	Build on the *Chilcott Report* and other research to identify issues and track progress towards avoiding group-think and promoting a positive security culture	Utilise the *Chilcott Report*, the NCSC's *Decrypting Diversity* report, and other research to identify issues in the civil nuclear sector. Track progress over the life of the strategy on metrics regarding diversity of thought and avoidance of group-think, as well as promotion of a positive security culture.	BEIS

	58	Promote/establish mentoring and reverse mentoring programmes	Promote and establish mentoring, reverse mentoring and/or Shadow Boards programmes that work closely with senior decision-makers to provide constructive challenge and support innovation and diverse perspectives.	Industry
	59	Set organisational objectives to promote a diverse and inclusive workforce	Encourage organisations to set explicit objectives and/or targets in respect of workforce diversity, inclusivity and positive culture.	Industry
	60	Continue and extend cyber apprentice graduates and i100 Scheme	Maintain and encourage sector-wide participation in the sector's cyber apprentice graduates scheme and the NCSC's i100 scheme.	Industry
	61	Support secondments (sector-wide and across sectors)	Support secondments (sector-wide and across sectors) to enable information-exchange, training, best-practice sharing and capability-building.	Industry
Embed cyber security training and accountability across organisations	62	Develop cyber community of interest (COI) for engineering personnel through cross-sector training programme	Engineering personnel are critical in ensuring the cyber security of civil nuclear operational technology (OT), but are not usually cyber professionals. We will develop a cyber 'community of interest' for engineering personnel through a cross-sector training programme, aimed at improving awareness and promoting best practice across the sector on OT cyber security.	Industry
	63	Adopt basic cyber training across all sector personnel	Adopt basic cyber training across all sector personnel to improve cyber security awareness and embed responsibility for cyber security across civil nuclear organisations.	Industry
	64	Drive adoption of cyber security training within supply chain	Embed cyber security training across the civil nuclear supply chain to improve awareness and support the adoption of appropriate cyber security practices.	Supply Chain

	65	Scrutinise organisational cyber security culture through regulatory activities	As part of their regulatory activities and enforcement, the ONR will place increased attention on organisational cyber security culture, recognising this is a core enabler for successful cyber security.	ONR
	66	Promote use of CPNI security culture assessment tool	Promote the use of CPNI's *SeCuRE 4, a* security culture self-assessment survey tool to help organisations assess their security culture and identify and drive improvements.	Industry

Annex B - Glossary of Terms

Active Cyber Defence (ACD)	Provides tools and services that protect organisations from a range of cyber attacks.
Advanced Gas-Cooled Reactors (AGRs)	A type of nuclear reactor using carbon dioxide as a coolant and graphite as the neutron moderator. These make up the majority of the existing nuclear generation fleet in the UK.
Department for Business, Energy and Industrial Strategy (BEIS)	The government department responsibilities for energy policy and delivery, including civil nuclear.
Cyber Assessment Framework (CAF)	A guidance framework developed by the NCSC for assessing the management of cyber risks within an organisation.
Chief Information Security Officer (CISO)	The senior-level executive typically responsible for developing and implementing an organisation's cyber and information security programme.
Cyber Security Information Sharing Partnership (CISP)	A joint industry and government information sharing initiative run by the NCSC.
Civil Nuclear Constabulary (CNC)	The dedicated police force responsible for providing a physical security response at nuclear sites within the UK, and of nuclear materials in transit.
Critical National Infrastructure (CNI)	Infrastructure, systems and networks which, if lost or compromised, would have a major detrimental impact on essential services, the economy or society, or a significant impact on national security or the functioning of the state.
Centre for the Protection of National Infrastructure (CPNI)	The United Kingdom's National Technical Authority for physical and personnel protective security.
Cyber Security Oversight Group (CSOG)	The sector-wide forum for civil nuclear cyber security, with senior-level representation. CSOG supports greater collaboration and provides leadership on implementing the UK Civil Nuclear Cyber Security Strategy.
Cyber Adversary Simulation (CyAS)	A threat-led security assurance/penetration testing framework for IT and OT systems developed by the NCSC.

Design Basis Threat (DBT)	A profile developed by BEIS describing the capabilities of potential insider and external adversaries who might attempt unauthorised removal of nuclear and other radioactive material or sabotage.
Generic Design Assessment (GDA)	An assessment programme developed by the ONR and the Environment Agency to assess the safety, security and environmental protection implications of nuclear reactor and plant designs that is intended to be deployed in the United Kingdom.
International Atomic Energy Agency (IAEA)	An international non-governmental organisation for international cooperation on the safe, secure and peaceful use of nuclear technologies.
Industrial Control Systems (ICS)	A collection of various types of control systems and instruments used to operate and automate industrial processes (e.g. water treatment, chemical processes, cooling or heating).
Intellectual Property (IP)	Information, innovations, software or designs developed by an organisation which could provide value to a competitor.
Malware	Viruses, trojans, worms or any digital code or content that could have an adverse impact on organisations or individuals.
Malware Information Sharing Platform (MISP)	A threat information sharing platform (e.g. threat intelligence, threat actor information).
Managed Service Providers (MSPs)	Third party companies that provide services such as networks, applications, infrastructure and security to support an organisation in managing its infrastructure and services.
National Cyber Security Centre (NCSC)	The United Kingdom's national technical authority for cyber and information security.
Net-Zero	The point at which a state removes as many greenhouse gas emissions from the atmosphere as it emits. Her Majesty's Government has committed to a target of achieving net zero emissions in the UK by 2050.
Office for Nuclear Regulation (ONR)	The United Kingdom's independent nuclear regulator for safety, security and safeguards.
Operational Technology (OT)	Technology that interfaces with the physical world and includes Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS).

Ransomware	Malicious software that makes data or systems unusable until the victim makes a payment.
Senior Information Risk Owner (SIRO)	A senior management board member who will take ownership of the organisation's information security risk policy.
Sensitive Nuclear Information (SNI)	Whilst not taking precedent over the legal definitions, a simple, working definition of SNI is "information relating to activities carried out on or in relation to civil nuclear premises; and deemed to be of value to an adversary planning a hostile act".
Security Assessment Principles (SyAPs)	A framework developed and used by the ONR to guide regulatory judgements and recommendations when undertaking assessments of dutyholders' security submissions, such as site security plans and transport security statements.
Well Informed Regulatory Decisions (WIReD)	The ONR's modernised system for collecting and assessing regulatory information.

This publication is available from: www.gov.uk/government/publications/civil-nuclear-cyber-security-strategy-2022

If you need a version of this document in a more accessible format, please email enquiries@beis.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use.