

Cyber resilience update

Committee Audit and Standards

Date of meeting 27 August 2021

Date of report 18 August 2021

Report by Director of Finance

1. Object of report

To advise the committee on the issue of a Scottish Government report titled *'the Strategic Framework for a Cyber Resilient Scotland'*, outline SPT's response to the key actions contained therein and update the committee on progress to meet the Cyber Resilience Framework requirements.

2. Background

Members will recall at the Audit & Standards Committee meeting on 19 February 2021, the Committee agreed that the Director of Finance present a further update report on the Cyber Resilience Framework in August 2021.

Since that time, Scottish Government have now published a report titled *'the Strategic Framework for a Cyber Resilient Scotland'*.

The report states that cyber threats to security continue to expand in number and sophistication. Hackers, organised crime and state-sponsored criminals are continually attempting to access personal information, bank accounts, intellectual property, critical national data and to disrupt public services.

The report adds that cyber incidents vary in nature and in degree of impact. As new technologies and their applications develop and are adopted (for example, the Internet of Things (IoT) and Artificial Intelligence (AI)), new threats will emerge. Responding to these threats in the context of rapid technological change, alongside other societal, economic and political demands, will require organisations to keep pace, adapt and evolve systems of response and recovery.

Cyber resilience is more than making technologies and systems secure. It is about preparedness to manage cyber risk, and how well-equipped organisations are to withstand, and defend against, manage, recover quickly and learn from cyber incidents. Agility and responsiveness are key.

The report can be found at:

<https://www.gov.scot/publications/strategic-framework-cyber-resilient-scotland/documents/>

3. Outline of findings

The report contains a Public Sector Action Plan 2021-2023 for public bodies.

The ten overarching aims contained within the action plan have been reviewed and SPT's response to the action plan are outlined in the following table.

Overarching aim	SPT's actions and response
<p>1. Increase public sector organisations' understanding of cyber risks that may affect them.</p>	<p>SPT has increased access to, and use of, threat intelligence, situational awareness reports and alerts to inform understanding of risk;</p> <p>SPT has membership of the NCSC's Cyber Security Information Sharing Partnership (CiSP);</p> <p>SPT utilises research and tools (including the Cyber Resilience Framework) from government and innovation centres.</p>
<p>2. Improve cyber resilient behaviours within public sector organisations.</p>	<p>SPT has increased staff communications including intranet articles and emails to all staff and members on cyber threats with signposting to National Cyber Security Centre (NCSC) training resources.</p>
<p>3. Improve and increase opportunities for professional development of IT and cyber security staff across the public sector.</p>	<p>SPT has sourced specialised training on cyber security, undertaken by Digital staff;</p> <p>SPT has recruited a Cyber Security and Continuity Lead officer.</p>
<p>4. Embed cyber security standards, regulations and compliance across public sector organisations.</p>	<p>SPT utilises research and tools (including the Cyber Resilience Framework) from government and standard bearers;</p> <p>SPT have adopted the use of a baseline security standard, incorporating Cyber Essentials and Cyber Essentials Plus.</p>
<p>5. Embed cyber resilience into the governance, policies and processes of public sector bodies.</p>	<p>SPT is working to further advance cyber resilience into governance arrangements to ensure decision-makers are fully equipped and supported to manage cyber risk;</p> <p>SPT continues to utilise and review the Scottish Public Sector Cyber Resilience Framework in light of changing technologies and standards.</p>
<p>6. Raise awareness of the cyber security services available to public sector organisations.</p>	<p>SPT is working with stakeholders and suppliers to assist them to understand the high levels of cyber security arrangements required to deliver SPT services.</p>

7. Support public sector organisations to prepare for, respond to and recover from cyber incidents.	SPT utilises tools and services available from the NCSC Active Cyber Defence programme; SPT is embedding cyber resilience into procurement and audit process.
8. Ensure effective national cyber incident response.	SPT continues to participate in national cyber exercises and initiatives to align with effective ongoing cross-agency co-ordination arrangements.
9. Protect the digital systems that underpin Scotland's essential services.	SPT is collaborating with stakeholders and suppliers to align cyber security arrangements.
10. Ensure that developments relating to Smart Cities are secure.	SPT is engaging with Glasgow smart city policy leads on this initiative.

An officer group has been set up and meets regularly to review progress against the cyber resilience framework tool and related matters outlined in the above table. A full review of the tool is scheduled to be conducted annually. An interim review was conducted by the Cyber Security and Continuity Lead, this has triggered actions to review and update the hierarchy and content of policies and procedures which underpin all cyber security activities and training. This action is currently evolving as we work to embed more of the cyber resilience framework into SPT.

4. Conclusions

The Scottish Government published a report titled '*the Strategic Framework for a Cyber Resilient Scotland*'.

Cyber resilience is more than making technologies and systems secure. It is about preparedness to meet cyber risk, and how well-equipped organisations are to withstand, and defend against, manage, recover quickly and learn from cyber incidents.

The overarching aims contained within Public Sector Action Plan 2021-2023 for public bodies have been assessed with actions identified and implemented to strengthen SPT's cyber resilience arrangements.

5. Committee action

The committee is asked to note the contents of this report and the Scottish Government report titled '*the Strategic Framework for a Cyber Resilient Scotland*' and SPT's commitment to cyber security improvement.

6. Consequences

Policy consequences	<i>In accordance with the Information Security Policy.</i>
Legal consequences	<i>None directly.</i>
Financial consequences	<i>The resources required to implement the Cyber Resilience Framework will be met from SPT's capital and revenue budgets.</i>

Personnel consequences	<i>None directly.</i>
Equalities consequences	<i>None directly.</i>
Risk consequences	<i>Cyber resilience arrangements reduce the impact of cyber risks.</i>

Name Neil Wylie

Title **Director of Finance**

Name Valerie Davidson

Title **Acting Chief Executive**

For further information, please contact Neil Wylie, Director of Finance on 0141 333 3380.
















Scottish Government
Riaghaltas na h-Alba
gov.scot

The Strategic Framework for a Cyber Resilient Scotland



Contents

	Joint Foreword Deputy First Minister and Chair of the National Cyber Resilience Advisory Board	3
	Introduction	5
	Overview of The Strategic Framework for a Cyber Resilient Scotland	11
	Understanding the Framework	12
	Vision	12
	Outcomes	12
	Cross-cutting Enablers	18
	Principles for Delivery	21
	Links between the Framework, the National Performance Framework and the UN Sustainable Development Goals - Annex A	23
	Governance Structure - Annex B	24
	The Action Plans - Annex C	25
	Measurement Indicators - Annex D	36
	CyberScotland Partnership - Annex E	38

Joint Foreword



The past year has challenged us like no other time in recent history, but it has also served to highlight just how critical digital technologies are to our lives, and to the functioning of society and the economy.

Whether working or learning from home, running a business, or keeping in touch with friends and family, digital technologies have underpinned much of our response to the COVID-19 pandemic and they continue to support our Critical National Infrastructure.

Digital technologies cut across everything we do – as our forthcoming Digital Strategy will demonstrate. The secure and resilient ways we use them cannot be an afterthought. Cyber resilience cannot be viewed simply as an “IT issue”. It is, in fact, the very backbone to every public service, to every business and to every community in Scotland. It is a critical part of our economic and societal recovery and renewal, especially as Scotland embraces new technologies such as Artificial Intelligence, Smart Cities and 5G wireless networks.

Cyber resilience is key to operational resilience and business continuity, as well as our capacity to grow and flourish as we adapt to the demands of operating online. Our ability to deter, respond to and recover from national cyber attacks is our top priority. We need to plan, exercise and reflect continually and collaboratively, to ensure that Scotland is prepared to withstand cyber threats.

The Strategic Framework for a Cyber Resilient Scotland sets out what we need to do to make Scotland a digitally secure and digitally resilient nation. The cyber threats we face cannot be met by government alone. We all have a role to play in protecting ourselves, our families and our communities. Our public, third and private sector organisations need to work together with the Scottish Government to minimise the harm and disruption that can result from a cyber incident, and thus making the very most of technological advances.

The pandemic has reminded us of the importance of resilience and agility. We will review the implementation of our Framework regularly, monitoring indicators against the four outcomes and the action plans that will guide delivery.

The UK Government plans to produce an interim National Cyber Security Strategy in 2021, and the Scottish Government will continue to work closely with the Cabinet Office to ensure alignment of our mutual strategic aims and ambitions. We will also continue to work closely with the National Cyber Security Centre and Police Scotland as we drive forward our shared aim to make Scotland digitally secure and resilient.

It is my wish that the National Cyber Resilience Advisory Board should continue to take national oversight of the Framework, providing drive and advice, and challenging me, my colleagues and the Scottish Government to maximise the digital opportunities. I thank the Board for its work to date, and extend my gratitude to all partners involved in delivering our shared strategic aims.

I look forward to working with you all to achieve our shared vision of Scotland that thrives as a digitally secure and cyber resilient nation.

John Swinney, MSP

Deputy First Minister and Cabinet Secretary for Education and Skills

A handwritten signature in black ink, appearing to read "John Swinney". The signature is written in a cursive style with a long horizontal stroke at the end.



The Strategic Framework sets out the approach Scotland will take to creating a digitally secure and resilient nation. A challenge which requires a community effort to raise the awareness of the cyber threat; to help prepare our people, our organisations and our businesses to deal with cyber risks and a growing cyber crime threat.

Our approach must be founded in a partnership which brings the public and private sectors together to help raise cyber resilience awareness, skills, standards and our collective ability to respond to a major cyber incident. In the midst of COVID-19 we saw cyber crime change to exploit the fear, uncertainty and doubt created by the pandemic for profit. We also saw people working together across Scotland to help deal with that threat. That community spirit is something we want to build on through the creation of the CyberScotland Partnership to collaborate on cyber security awareness campaigns and practical advice on how to counter cyber crime.

There are challenges in implementing any cyber resilience programme at a national level, and those often relate to achieving impact at scale, to embedding cyber resilience into the design and rollout of future services, and to a co-ordinated and effective response to a major cyber incident. Scotland is no different in this regard, and we will need to work closely with the National Cyber Security Centre to achieve these outcomes.

Scotland is a nation of small and medium sized enterprises, and we will continue to raise awareness and support those enterprises in improving their cyber defence, working through the Scottish Business Resilience Centre, through public and third sector organisations to achieve this. The NCSC's Active Cyber Defence programme will play a key role in protecting the broader community.

Looking forward, we must embed cyber resilience into the design of Scotland's future digital services, becoming a core element of the Digital Scotland strategy, as we ensure that the digital services we build for the future are trustworthy and resilient.

Recent cyber security incidents have demonstrated the need to be able to orchestrate a national response which can quickly mobilise the support which organisations need to detect, respond and recover from a major cyber attack. The time has passed when individual organisations can regard themselves as medieval castles each defending themselves. We now are all part of an increasingly interconnected digital ecosystem, requiring us to improve our collective threat intelligence, security operations and incident response capabilities.

David Ferbrache, OBE

Chair of the National Cyber Resilience Advisory Board

Introduction

THE FRAMEWORK

The Strategic Framework for a Cyber Resilient Scotland (“the Framework”) will enable the Scottish Government and its partners to achieve the following vision:

Scotland thrives by being a digitally secure and resilient nation

It builds on Scotland’s first cyber resilience strategy, *Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland*, expanding on its achievements and addressing ongoing – and new – challenges.

Four outcomes will underpin this vision, whilst defining the principles and enablers that will guide and maximise delivery. These are as follows.

1. People recognise the cyber risks and are well prepared to manage them
2. Businesses and organisations recognise the cyber risks and are well prepared to manage them
3. Digital public services are secure and cyber resilient
4. National cyber incident response arrangements are effective

The outcomes within the Framework contribute to a number of national outcomes in Scotland’s National Performance Framework (NPF). The table in Annex A shows how the Framework contributes to the NPF and how the NPF in turn contributes to the UN’s Sustainable Development Goals.

The Framework itself is not time-bound, but a suite of four action plans will run from 2021 until 2023 - the delivery of which will be reviewed on an annual basis, see Annex C.

The UK Government is producing an interim National Cyber Security Strategy in 2021. Scotland’s Framework and the UK Government’s strategy are mutually supportive. We recognise the importance of an integrated approach but also opportunities for Scotland to lead, innovate and tailor support for communities, organisations and businesses in Scotland. The National Cyber Security Centre (NCSC) provides defence and deterrence against higher-end state threats for the whole of the UK and the Scottish Government works with them to increase active cyber defence activities in Scotland.

GETTING THE MOST OUT OF DIGITAL TECHNOLOGIES

It is hard to imagine life without digital technologies. Almost every aspect of our daily lives depends on the internet, data and devices. Indeed, much of our national infrastructure (such as our transport systems and utilities) relies on technologies and online connectivity.

At least 88% of Scottish households have internet access,¹ and we find ourselves increasingly using – and being dependent on – digital technologies for work, doing business, learning, shopping and socialising. The COVID-19 pandemic has thrown this dependency into sharp focus. Businesses have moved wholly or partly online, many of us have increased our online financial transactions, and there has been a significant increase in the use of online platforms to connect with friends and family. During the national lockdown, children, young people and students have relied on digital access to continue their education.

Online digital technologies benefit individuals, our families, our communities, organisations, businesses, and society and the economy as a whole. The use of digital online technologies will only increase, becoming an even more critical enabler for our economic, social and cultural growth.

The Scottish Government’s Digital Strategy (due for publication in Spring 2021) sets out how digital should be at the heart of everything we do – how we ensure no one is left behind as we move online, deliver economic growth, reform our public services, and prepare our children for the workplaces of the future.

Our forthcoming AI Strategy² will seek to unlock the potential of Artificial Intelligence (AI) and position Scotland as a leader in the development and adoption of trustworthy and accountable artificial intelligence. Achieving this ambition requires that the very innovation, technological developments and infrastructure are secure and resilient to cyber attacks. AI in itself can help to protect networks from increasingly sophisticated cyber attacks. For instance, AI applications can be used in real-time monitoring and analysis of traffic, or use of services, to help identify and respond to potential threats.

As our use of digital technologies increases, and we become ever more dependent on them, it becomes critical that the services we use, our businesses and our country’s systems and infrastructure are cyber resilient and “secure by design”.

It is important that we see **cyber resilience as a critical enabler to our digital ambitions**, for digital public services, for digital inclusion, skills development, our business sector, the growth of our Tech sector, as well as meeting our statutory commitments to be a net zero society by 2045.

1 [Scottish household survey 2019: annual report - gov.scot \(www.gov.scot\)](https://www.gov.scot/publications/scottish-household-survey-2019-annual-report/pages/100-to-109.aspx)

2 [Scotland’s AI Strategy - Developing an AI Strategy for Scotland \(scotlandaistrategy.com\)](https://www.scotland.gov.uk/topics/ai-strategy)

WHAT WE MEAN BY CYBER RESILIENCE

Cyber resilience is more than making technologies and systems secure. It is about our preparedness to meet cyber risk, and how well equipped we are to withstand, and defend against, manage, recover quickly and learn from cyber incidents. Features of cyber resilience include:

- Knowledge and awareness of risk and threat
- Access to guidance, tools and resources
- Understanding policy and processes
- Learning and skills
- Effective incident management, response and recovery processes.

Figure 1. Cyber resilience in action



THE RAPIDLY EVOLVING CYBER THREAT

As the role of digital online technologies in our lives grows, so do the risks.

Cyber threats to our security continue to expand in number and sophistication. Hackers, organised crime and state-sponsored criminals are continually attempting to access personal information, bank accounts, intellectual property, critical national data and to disrupt our public services.

Cyber incidents vary in nature and in degree of impact. As new technologies and their applications develop and are adopted (for example, the Internet of Things (IoT) and AI), new threats will emerge. Responding to these threats in the context of rapid technological change, alongside other societal, economic and political changes, will require us to keep pace, adapt and evolve our systems of response and recovery. Agility and responsiveness are key.

As more people do business online, the payoffs from cyber crime increase, attracting more cyber criminals. From domestic use and businesses, to government and critical national infrastructure, we all face a constant and evolving threat.

It is not a straightforward task to identify specific cyber security risks, because the threats are so diverse and ever evolving. Mitigation can often be outside our direct area of control; for example, in relation to digital products or supply chains that are not secure.

The challenges for domestic users are unlikely to be the same challenges that our largest companies face. But it is clear that trust and confidence in the internet and our digital and online infrastructure are essential for Scotland: for our economy, for our society, and for our national security.

Police Scotland has a duty to protect the people of Scotland in the public, private and virtual space. Its strategy, *Keeping people safe in the digital world*,³ is a key part of our national response to address cyber crime and will contribute to all four outcomes of the Framework.

MOST COMMON TYPES OF CYBER CRIME

Computer Misuse Offences

- Hacking
- Ransomware
- DDoS attacks

Financial/Economic Offences

- Business email compromise
- Fraudulent transactions and identity fraud
- Online shopping/auction frauds
- Scams
- Blackmail spam

Sexual Offences

Threatening Behaviour/Communications Offences

- Stalking
- Hate crime
- Hoaxes

Source: Police Scotland

³ [cyber-strategy.pdf \(scotland.police.uk\)](https://www.scotland.police.uk/cyber-strategy.pdf)

FIRM FOUNDATIONS – RECOGNISING ACHIEVEMENTS AND CHALLENGES

In November 2020, the Scottish Government published a progress report on *Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland*. The report, entitled *Firm Foundations*⁴, demonstrates evidence of progress and celebrates a number of successes, including:

- commitment and collaboration of national partners
- strong and productive relationship with the National Cyber Security Centre
- establishment of the National Cyber Resilience Advisory Board
- an increased take up of the NCSC's Active Defence Tools across the public sector
- increased awareness of the cyber threat in the third sector
- substantial developments in our education and lifelong learning system
- establishment of CyberScotland Week – an annual showcase of cyber security awareness raising and services in Scotland
- stimulation and early growth in Scotland's cyber security goods and services industry.

It also identified a number of areas requiring development, including in relation to:

- securing our hundreds of thousands of SMEs
- reaching our tens of thousands of third sector organisations
- further strengthening our skills pipeline, drawing on industry expertise.

4 <https://www.gov.scot/publications/firm-foundations-progress-report-safe-secure-prosperous-cyber-resilience-strategy-scotland-2015-2020/>

THE NEED FOR AGILE POLICY MAKING AND RESPONSE IN RELATION TO CYBER RESILIENCE

The COVID-19 pandemic has demonstrated to us the need for our strategic planning and response to external and unexpected incidents to be agile and adaptable.

The pandemic has led to an acceleration in the scale and speed of digital adoption, including increased reliance on digital technologies to enable home working, learning, shopping and communication. Official statistics for Scotland and the whole of the UK show that:

- At the end of January 2021, 40% of workers in Scotland had worked from home at some point in the previous seven days, with the majority doing so as a result of the COVID-19 pandemic.⁵
- Between May and June 2020, 87% of parents said a child in their household had been learning at home because of the COVID-19 pandemic, with 44% of parents saying their children aged 16 to 18 had used real-time interactive online learning resources provided by schools (for example, live lessons) compared with 13% for children aged 5 to 10 years.⁶
- In 2020, the amount spent on online retail sales increased by 46% when compared to 2019 as a whole, the largest annual increase since 2008. All retail sectors reported large increases in the total of online sales in 2020.⁷

During this time the threat landscape has also changed, with the pandemic providing new opportunities for cyber criminals. According to EUROPOL data:⁸

- COVID-19 has led to an increase in vulnerabilities – what they term “the attack surface” – as the fast shift to remote working means some companies have relaxed their IT security policies, with some responsibility being transferred to the users, where varying levels of training have created a new security gap.
- Fake items claiming to help prevent or cure COVID-19 have emerged on the Internet.
- A number of phishing campaigns have taken advantage of COVID-19.
- The volume of online child sexual abuse material and the livestreaming of child sexual imagery, and self-generated child sexual imagery, has increased, exacerbated by the COVID-19 restrictions.
- Business e-mail compromise has increased across most EU Member States as a result of COVID-19.

Scotland, like other countries, has had to respond rapidly to these difficult and unexpected circumstances and the need to be digitally secure has been a critical component to the COVID-19 response. Cyber resilience has been a key underpinning factor to ensure Scotland is able to develop secure smart digital solutions to meet the needs of the situation in the immediate and longer-terms.

5 <https://www.ons.gov.uk/peoplepopulationandcommunity/wellbeing>

6 <https://www.ons.gov.uk/peoplepopulationandcommunity/educationandchildcare/articles/coronavirusandhomeschoolinggreatbritain/apriltojune2020>

7 <https://www.ons.gov.uk/businessindustryandtrade/retailindustry/bulletins/retailsales/december2020#online-retail>

8 [INTERNET ORGANISED CRIME THREAT ASSESSMENT \(IOCTA\) 2020 | Europol \(europa.eu\)](https://www.europol.europa.eu/internet-organised-crime-threat-assessment-iocta-2020)

The Strategic Framework for a Cyber Resilient Scotland

OUR VISION

Scotland thrives by being a digitally secure and resilient nation

Outcomes to achieve our vision

People recognise the cyber risks and are well prepared to manage them	Businesses and organisations recognise the cyber risks and are well prepared to manage them	Digital public services are secure and cyber resilient	National cyber incident response arrangements are effective
---	---	--	---

Cross-cutting enablers

Knowledge of risk and threat	Tools, processes, standards, regulations and compliance	Learning and skills	Incident management, response and recovery	Access to cyber security technical expertise	Research and innovation
------------------------------	---	---------------------	--	--	-------------------------

Principles for delivery

An inclusive and ethical approach	Whole-of-government approach	Strong leadership and good governance	Productive and collaborative partnerships	Effective communication	Adaptive and agile programme management	Robust evidence of impact
-----------------------------------	------------------------------	---------------------------------------	---	-------------------------	---	---------------------------

Delivery model (2021-23)

With our partners we will implement Actions Plans for:

- the Public Sector
- the Private Sector
- the Third Sector
- Learning and Skills (including awareness raising)

Understanding the Framework

VISION

“Scotland thrives by being a digitally secure and resilient nation”

Technology is key to Scotland’s future. Scottish Ministers’ vision is of a Scotland that thrives by being a digitally secure and resilient nation. Our forthcoming Digital Strategy will seek to realise Scotland’s full potential by setting out how we will make sure that digital is at the heart of everything we do – how we ensure no one is left behind as we move online, deliver economic growth, reform our public services, and prepare our children and young people for the workplaces of the future.

We want Scotland to reap the benefits of an increasingly connected world: cyber resilience enables this.

There are four outcomes to achieve this vision:

1. People recognise the cyber risks and are well prepared to manage them
2. Businesses and organisations recognise the cyber risks and are well prepared to manage them
3. Digital public services are secure and cyber resilient
4. National cyber incident response arrangements are effective

OUTCOMES

Outcome 1: People recognise the cyber risks and are well prepared to manage them

“Cyber crime is increasing worldwide, and Scotland is determined to keep its people and communities safe. Police Scotland is working with partners to tackle the threat, risk and harm from online crime to individuals, families and communities.”

DCC Malcolm Graham, Police Scotland

This outcome is about building a culture of awareness, knowledge and skills whereby people can use digital online technologies securely, keeping themselves and their families secure, and knowing what to do if they experience a cyber attack.

We know that almost 9 in 10 adults in Scotland use the internet either for work or personal use, with 86% of internet users accessing it through a smartphone. An increasing number of people are also using ‘smart’ technologies, for example to manage their heating, lighting, or security systems. The Scottish Household Survey reported that in 2019, 26% of people in Scotland used at least one type of smart appliance.⁹

⁹ [Scottish household survey 2019: annual report - gov.scot \(www.gov.scot\)](https://www.gov.scot/publications/scottish-household-survey-2019-annual-report/pages/100.aspx)

Such high levels of internet usage, however, expose people to a number of cyber threats: estimates for 2018/19 show that 8% of internet users in Scotland had their devices infected by a virus, and that 6% of adults had their credit and bank card details stolen (online or physically). Data also shows that the majority of victims of cyber crime choose not to report the incident to the authorities.¹⁰

The focus to achieve this outcome will be on:

- building people's cyber awareness and resilience through practical, regular awareness campaigns targeted to different groups of people, including those with particular access needs
- making it easier for everybody to report cyber crime and get help from relevant, trusted organisations
- increasing the availability of, and improving the access to, trusted and authoritative information, advice, guidance and tools so people can be secure online
- increasing people's cyber resilience by embedding it into relevant curricula and qualifications
- building the cyber awareness and cyber resilience of people at work.

Outcome 2: Businesses and organisations recognise the cyber risks and are well prepared to manage them

“We live in a rapidly evolving, and hyper-connected, digitalised society that presents us with opportunities to flourish. This constantly evolving digital landscape in which our organisations and businesses find themselves in also presents new opportunities for criminal exploitation. A cyber resilient organisation is a competitively strong and trusted organisation.”

Kate Forbes, MSP
Cabinet Secretary for Finance

Cyber risk needs to be seen as a business risk for any organisation.

This outcome is about ensuring that, across the public, private and third sectors, businesses and organisations are aware of the cyber risks they face, have access to up-to-date information, advice and guidance, and can withstand, respond to and manage incidents, knowing where to find the right kind of support.

Cyber threats can come from organised crime groups, business competitors, disgruntled employees, hackers, those driven by political or ideological factors. Some threats are more invasive and harmful than others, but they can all be disruptive for the unprepared victim.

The Cyber Breaches Survey 2020 identified that almost half of businesses in the UK (46%) and a quarter of charities (26%) reported having cyber security breaches or attacks in the previous twelve months, with an increasing number of businesses experiencing these issues at least once a week. The estimated average cost of cyber security breaches to businesses is £3,230. For medium and large firms, the average cost is £5,220.

¹⁰ [Scottish Crime and Justice Survey 2018/19: main findings - gov.scot \(www.gov.scot\)](https://www.gov.scot/resources/documents/2019/06/Scottish-Crime-and-Justice-Survey-2018-19-main-findings.pdf)

Scotland is a nation of small and medium-sized enterprises (SMEs). Although small, they can be a vital part of the wider supply chain across sectors. Many are likely to be less aware of their exposure to cyber threats and have reduced ability to invest in cyber security skills and services than larger organisations. Some simply don't see it as a priority business or organisational risk. Often cyber attacks are untargeted and any organisation can fall victim. The impact on SMEs can be significant. Indeed, smaller businesses are often seen as the most vulnerable point in the supply chain. It is clear that cyber attacks are a risk for any business with a digital footprint.

Moreover, there is a commercial advantage in a business positioning itself as being cyber resilient in its operation, its provision of goods and services and in the protection of data and information.

In the Scottish public sector, we have made significant headway with our public bodies, with the majority now routinely including cyber risks as part of their business risk management processes and utilising the Active Cyber Defence programme provided by the NCSC¹¹ – the UK's national agency that provides cyber security advice and support for the public and private sectors. In addition, 88% of eligible Scottish public sector organisations have now achieved Cyber Essentials¹² accreditation. However, public bodies and public services remain at significant risk from cyber threat and it is imperative that the public sector should continue to remain a key priority focus.

In relation to the Third Sector, UK research shows that between 2018 and 2019, 22% of charities identified cyber security breaches or attacks, with an average annual cost of lost data or assets of £9,470.¹³ It remains a priority that we work to support our third sector organisations to become more cyber resilient, and we will engage with national intermediary and regulatory bodies such as the Scottish Council for Voluntary Organisations (SCVO), the Association of Chief Officers of Scottish Voluntary Organisations (ACOSVO) and the Office of the Scottish Charity Regulator (OSCR) to achieve this.

There is a great deal of guidance and support available that, if used appropriately, could reduce organisations' exposure to cyber risk and help build cyber resilience.

The focus to achieve this outcome will be on:

- increasing businesses' and organisations' understanding of cyber risks, how to report cyber incidents, and get help from trusted sources of advice and support
- embedding cyber resilience into organisations' governance structures, policies and processes
- increasing awareness and building cyber resilient behaviours of staff in all posts at all levels
- increasing opportunities for professional development of cyber security professionals
- embedding cyber security standards, regulations and compliance across businesses and organisations, including into governance processes
- promoting and encouraging uptake of the range of tools and services within the NCSC's Active Cyber Defence programme
- increasing efforts to educate the supply chain and small businesses of cyber risks.

11 [The NCSC's Active Cyber Defence programme - NCSC.GOV.UK](https://www.ncsc.gov.uk/active-cyber-defence)

12 [About Cyber Essentials - NCSC.GOV.UK](https://www.ncsc.gov.uk/cyber-essentials)

13 [Cyber Security Breaches Survey 2019: Statistical Release \(publishing.service.gov.uk\)](https://www.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/421113/cyber-security-breaches-survey-2019-statistical-release.pdf)

Outcome 3: Digital public services are secure and cyber resilient

“New technologies for delivering public services have brought incredible gains in terms of efficiency and effectiveness. However, they also bring new vulnerabilities. For the public to trust government with their data, we need to make sure that our digital services are secure and resilient by default.”

Michael Matheson, MSP
Cabinet Secretary for Transport, Infrastructure and Connectivity

This outcome is about ensuring that our digital public services are secure and cyber resilient and where possible, security is built in by design.

The world is changing at pace. Innovation and technological advances, including artificial intelligence, quantum technology, the “Internet of Things”, and 5G, are driving what is being referred to as the Fourth Industrial Revolution, and digital technologies have the power to reshape almost every sector. Scotland is well placed to capitalise on this global revolution, and we are already seeing the development of ‘Smart City’ approaches addressing urban challenges such as traffic congestion, waste management and pollution, as well as increasingly underpinning the critical services and infrastructure necessary to keep Scotland running. It is imperative that security is built in from the design stage of these connected technologies and the NCSC has produced guidance that will help ensure the security of a connected place and its underlying infrastructure.

As more public services go online, users need to be able to trust service providers with their data and interactions. This is especially the case for people who are reluctant to move to digital versions of familiar services. Strong security needs to be built in to digital public services by design.

The focus to achieve this outcome will be on:

- improving the security capabilities and resilience of digital public services
- protecting the digital systems that support Scotland’s infrastructure and essential services
- ensuring a secure-by-design approach is adopted across the supply chain and aligning with the UK Government’s proposal for regulating the cyber security of smart products
- ensuring that developments relating to Smart Cities and other new digital infrastructures build in cyber resilience from the outset, and by design
- encouraging Scotland-based cyber security companies to provide products and services that can meet the cyber resilience needs of our public sector and its digital public services.

Outcome 4: National cyber incident response arrangements are effective

“Digital technologies and the internet offer significant economic, social and personal benefits for Scotland and its people. Harnessing these benefits also creates risks. Managing cyber risks is a shared responsibility. The Scottish Government, business and individuals have a collective responsibility to safeguard their use of the internet and digital systems, being prepared and able to withstand and manage the cyber threat. Effective cyber resilience cannot be achieved in isolation. Partnerships between the Scottish Government, other governments, law enforcement and the cyber security industry are key to advancing and protecting Scotland’s interests online through co-ordinated national leadership in relation to incident response.”

John Swinney, MSP
Deputy First Minister and Cabinet Secretary for Education and Skills

This outcome is about ensuring that our national cyber incident response arrangements are effective.

We only have to look back to 2017 and the global Wannacry incident to understand how a large part of the public sector (on that occasion, the health sector) was affected by a single malicious operation. In 2020 the Scottish public sector saw significant disruptive attacks on Dundee and Angus College and the Scottish Environment Protection Agency. At the end of 2020 the SolarWinds global cyber incident focused attention on supply chain vulnerability. In this instance a total of 18,000 SolarWinds customers worldwide fell victim to a compromised software update. It is thought that the purpose of the attack was to target a small number of key organisations, however the consequences of the attack, including the cost of clean-up, have been felt across a much wider customer base.

Cyber attacks can have far-reaching consequences, and it is critical that the Scottish Government has national arrangements in place to manage and co-ordinate its response to incidents with a focus on potential wider consequences and impacts resulting from the original attack. This will ensure that incidents are managed effectively, involving relevant partners such as Police Scotland’s cyber threat intelligence team, the NCSC and the National Cyber Crime Unit within the National Crime Agency, and in turn, help maintain public confidence in Scotland’s ability to deal with cyber incidents.

Figure 2: Cyber incident response process



Building on its tried and tested civil contingency arrangements, the Scottish Government has developed national cyber incident processes to co-ordinate responses to critical national incidents. These align with existing civil contingency planning and the UK's cyber incident management arrangements. Testing and exercising are key requirements to ensure that Scotland is prepared to handle a national cyber incident effectively.

The focus to achieve this outcome will be on:

- regularly testing, exercising and reviewing our national cyber incident co-ordination arrangements
 - raising awareness of the national cyber incident co-ordination arrangements across government and its agencies
 - continuing to develop our cyber threat intelligence, monitoring, detection and response capabilities
 - communicating clearly with affected parties during and after a national cyber incident
 - ensuring effective ongoing cross-agency collaboration.
-

CROSS-CUTTING ENABLERS

There are a number of cross-cutting enablers that will help realise our national strategic ambitions. These enablers will ensure consistency of effort and impact across sectors, and assist with reporting against specific activities. We use them to structure our action plans relating to the public, private and third sectors.

Enabler 1: Knowledge of risk and threat

Actions relating to this enabler will contribute to the achievement of Outcomes 1, 2, 3 & 4.

Cyber threat intelligence and knowledge are core to cyber resilience. When used properly, this knowledge can enable better-informed security and business decisions and ultimately allow organisations to take decisive action to protect their users, their data, finances and reputations against adversaries.

This knowledge may come from different sources. The Scottish Government will work with key partners across all sectors to improve organisations' understanding of the cyber threats they face.

We will improve the co-ordination and amplification of threat messaging and encourage access to and use of threat intelligence, situational awareness reports and alerts, to inform the risk picture. We will encourage use of the National Cyber Security Centre's Cyber Security Information Sharing Partnership (CiSP).

Enabler 2: Tools, processes, standards, regulations and compliance

Actions relating to this enabler will contribute to the achievement of Outcomes 1, 2, 3 & 4.

Standards and regulations help ensure that organisations take appropriate steps to protect their data and the data of their users or customers. Compliance with regulations and standards can drive investment and ensure that organisations keep pace with technological advancements and take proportionate, risk-based decisions to avoid cyber incidents affecting the delivery of critical services. Regulations such as the Network Information and Systems (NIS) Regulations 2018 help to secure our critical sectors and the General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals.

Cyber Essentials Plus underpins the cyber resilience standards of much of our public sector as part of the Scottish Public Sector Cyber Resilience Framework.

The NCSC provides tools, resources and services to help organisations operate securely, including a Response and Recovery Guide, Top Tips for Staff Training guidance and a suite of Active Cyber Defence (ACD) measures. The ACD programme seeks to reduce the impact of internet borne cyber attacks, reduce harm and protect against a range of cyber security threats.

We will ensure that organisations and businesses are aware of the standards and regulations that they need to comply with, and where to find tools and guidance.

Enabler 3: Learning and skills

Actions to drive learning and skills are contained within the Learning and Skills Action Plan and contribute to Outcomes 1, 2, 3 & 4.

The Scottish Government will work with key partners to embed cyber awareness and resilience into workplace learning and development at all levels, and maximise employers' access to cyber security skills, so that roles and functions within organisations can be filled. We will align our plans with activity taken forward under the *STEM Education and Training Strategy*.¹⁴

We will continue to build a robust cyber security skills pipeline, embedding cyber security learning and skills development opportunities across our education and lifelong learning system.

As highlighted in the 2020-21 Programme for Government, the cyber security industry can play an important part in the economic recovery of Scotland and it is important that we are able to meet the demand for cyber security professionals, through meeting skills shortages. In the development of skills, we need to address the skills base, which is currently predominantly male and white. Our work in this area will seek to grow access to cyber security skills and careers for women, neurodivergent people and people from black and minority ethnic backgrounds and disadvantaged communities. We will also seek to better co-ordinate the role of industry in supporting cyber security skills development, from early engagement and inspiration, through to providing work experience, mentoring and other vocational learning opportunities.

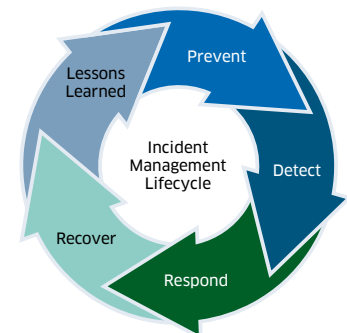
Enabler 4: Incident management, response and recovery

Actions relating to this enabler will contribute to the achievement of Outcomes 2, 3 & 4.

A fundamental aspect of cyber resilience relates to incident management, response and recovery planning. All organisations need to regard cyber risk as a business risk and put in place incident response plans that are tested regularly through exercising.

We will encourage businesses and organisations to develop cyber incident response plans or include these into existing Business Continuity Plans.

We recognise that smaller businesses and organisations are often unclear on what to do, or who to turn to, if faced with a cyber incident. The Scottish Business Resilience Centre and its partners (including the NCSC, Police Scotland and the Scottish Government) offer a Cyber Incident Response "triage" service to help small businesses take the necessary steps to respond to and recover from a cyber security incident.



¹⁴ [Science, Technology, Engineering and Mathematics: education and training strategy - gov.scot \(www.gov.scot\)](https://www.gov.scot/publications/science-technology-engineering-and-mathematics-education-and-training-strategy/pages/14.aspx)

Enabler 5: Access to cyber security technical expertise

Actions relating to this enabler will contribute to the achievement of Outcomes 2 & 3.

Access to technical expertise in cyber security is critical to cyber resilience.

Cyber security service providers, including managed services, can help protect businesses and organisations. The growth of the cyber security industry in recent years reflects the scale of the cyber challenge facing organisations.

'I learned in government that whether it's in the UK, Europe, the US or globally, the common cyber threats we face can only be solved if there is a strong, innovative private sector taking care of huge swathes of the problem.

That presents enormous economic opportunities for talented technologists and entrepreneurs."

Ciaran Martin
Former Head of the National Cyber Security Centre

The UK's cyber security industry is now worth an estimated £8.3 billion, with total revenues in the sector up 46% in 2017.¹⁵

The number of cyber security products and services companies in Scotland has increased substantially over the past five years, with the number now standing at around 230. There has been significant growth in revenue and employment and we are beginning to see investment in early-stage companies. This growth has been aided by a number of factors, including Scotland's growing innovation in technology sector, talent pool and academic research.

There is potential for growing an eco-system between the private and public sectors to find solutions and to develop innovative services.

We will work with our key partners to raise awareness amongst businesses and organisations of the range of cyber security technical expertise available to them.

Enabler 6: Innovation and academic research

Actions relating to this enabler will contribute to the achievement of Outcome 1, 2, 3 & 4.

It is important that Scotland's cyber security research capabilities and capacity continue to grow and evolve, and that our universities continue to expand knowledge by collaborating closely with industry. We will seek to embed an evidence-based approach to drive innovation and to find solutions to emerging challenges that support Scotland's businesses and organisations to increase their cyber resilience.

Activities to take forward research, innovation and to improve links between academia and industry are included in the Learning and Skills Action Plan. The sectoral action plans will also include actions to better link organisations and sectors, possibly through representative, intermediary and membership bodies, to take advantage of cutting-edge knowledge and capabilities.

¹⁵ <https://www.gov.uk/government/news/uks-booming-cyber-security-sector-worth-83-billion>

PRINCIPLES FOR DELIVERY

The Framework is underpinned by a set of guiding principles. We are committed to transparency and accountability in government, reducing inequality and promoting sustainable economic development. Our approach embodies the principles of the Christie Commission, which is ten years old in 2021. Christie's pillars of Prevention, Partnership, Workforce Development and Performance Improvements chime well with the principles for delivery of our Framework and associated Action Plans.

Principle 1: An inclusive and ethical approach

The Scottish Government stands by an inclusive and ethical approach to cyber resilience. This includes encouraging responsible behaviours online, promoting individuals' rights online and increasing the participation of disadvantaged groups, for example, in cyber security skills development. Cyber resilience is a matter for everyone, and we need to have a keen focus on accessibility around messaging, information, advice and guidance – especially for people who require information in alternative and accessible formats.

Principle 2: A whole-of-government approach

Digital technologies and cyber resilience are increasingly relevant to the achievement of Scotland's ambitions, as set out in the National Performance Framework. We will continue to engage across the Scottish Government's directorates to support the embedding of cyber resilience within Ministerial portfolios and policies, taking a meaningful, whole-of-government approach with shared workstreams, outcomes and indicators where possible.

Principle 3: Strong leadership and good governance

Scottish Ministers take lead responsibility for this Framework and task the National Cyber Resilience Advisory Board (NCRAB) to continue its role in taking the lead on advice, guidance, advocacy and challenge in relation to the implementation of the Framework and its Action Plans (see the governance structure at Annex B). The Action Plans (Annex C) are intended to drive activity that will support Scotland to become a cyber-resilient nation, with one plan for each sector, and a fourth that will drive developments in cyber-related learning and skills across our education and lifelong learning system.

The Scottish Government will align this Framework to broader digital and resilience governance structures.

Principle 4: Productive and collaborative partnerships

Collaboration has been a huge success factor in the effective delivery of Scotland's first cyber resilience strategy. The continued commitment of partners will be critical to the successful delivery of this Framework and how we monitor progress and continuously improve.

We will build on our success to date by formalising the CyberScotland Partnership which brings together our national partners (further details in Annex E). The Partnership will help to ensure access to authoritative sources of advice, guidance and information for different audiences and provide leadership around shared national initiatives such as the annual CyberScotland Week.

Principle 5: Effective communication

We will continue to communicate with our partners, our stakeholders and across government to help us achieve our vision, looking at ways to continually improve the effectiveness of our messaging and the extent of our reach. We will report on progress towards the outcomes under our vision each year.

Specifically we will seek to amplify key messages from the National Cyber Security Centre and other authoritative sources. We will do this by utilising the collective co-ordination and collaboration provided by the formation of the CyberScotland Partnership and the online portal www.cyberscotland.com. We will also develop a National Cyber Resilience Communications Plan to support effective communication across the Partnership.

Principle 6: Adaptive and agile programme management

Cyber risks are continually evolving and it is essential that we can flex to meet rapidly changing situations. Cyber criminals can be adept at exploiting vulnerabilities. We responded rapidly to new cyber criminal activity during the COVID-19 pandemic and will plan to meet new, unexpected challenges, based on learning from this experience.

We will manage the implementation of the Framework and Action Plans using agile programme management approaches to ensure our activity is proactive, current and responsive.

Principle 7: Robust evidence of impact

We will take a robust approach to evidencing impact, drawing on up-to-date national and international qualitative and quantitative data. We have taken an outcome-focused approach and used logic models that are linked to measurable indicators to ensure we can measure progress towards our outcomes. The table in Annex D outlines the indicators we have identified at this stage to measure our progress. New indicators and/or sources of evidence may become available as we move forward, and we will include these where appropriate.

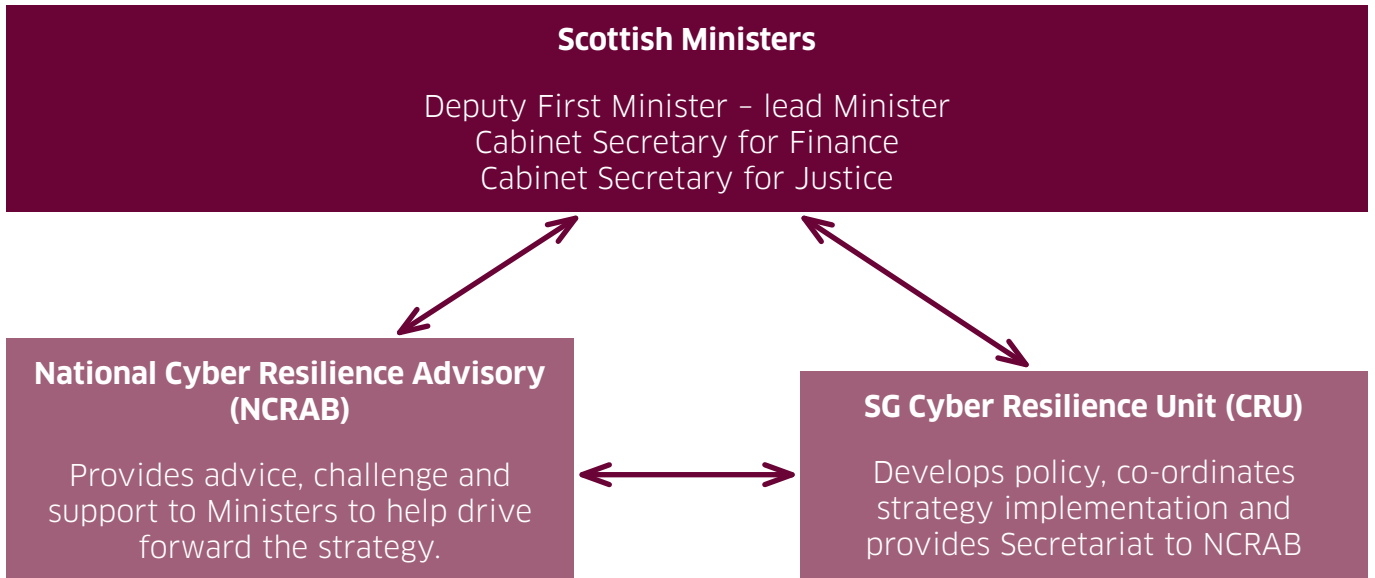
ANNEX A

LINKS BETWEEN THE FRAMEWORK, THE NATIONAL PERFORMANCE FRAMEWORK AND THE UN SUSTAINABLE DEVELOPMENT GOALS

	Contributes to	Contributes to
Cyber Resilience Strategic Framework Outcomes	National Performance Framework Outcomes	UN Sustainable Development Goals
People recognise the cyber risks and are well prepared to manage them	We tackle poverty by sharing opportunities, wealth and power more equally	1. No poverty 10. Reduced inequalities
	We are well educated, skilled and able to contribute to society	4. Quality education 10. Reduced inequalities
	We live in communities that are inclusive, empowered, resilient and safe	11. Sustainable cities and communities
Businesses and organisations recognise the cyber risks and are well prepared to manage them	We live in communities that are inclusive, empowered, resilient and safe	9. Industry, innovation and infrastructure 11. Sustainable cities and communities
	We have thriving and innovative businesses, with quality jobs and fair work for everyone	8. Decent work and economic growth 9. Industry, innovation and infrastructure
	We have a globally competitive, entrepreneurial, inclusive and sustainable economy	8. Decent work and economic growth 9. Industry, innovation and infrastructure
Digital public services are secure and cyber resilient	We live in communities that are inclusive, empowered, resilient and safe	9. Industry, innovation and infrastructure 11. Sustainable cities and communities
	We respect, protect and fulfil human rights and live free from discrimination	16. Peace, justice and strong institutions
National cyber incident response arrangements are effective	We live in communities that are inclusive, empowered, resilient and safe	9. Industry, innovation and infrastructure

ANNEX B

GOVERNANCE STRUCTURE



Strategy implementation - delivery model (2021-23)			
Public Sector Action Plan	Private Sector Action Plan	Third Sector Action Plan	Learning and Skills Action Plan

ANNEX C

ACTION PLANS 2021-23

The Scottish Government will work with its partners to implement the action plans.

Public Sector Action Plan

Overarching aims	Actions
1. Increase public sector organisations' understanding of cyber risks that may affect them	1.1 Increase access to, and use of, threat intelligence, situational awareness reports and alerts to inform understanding of risk
	1.2 Promote the use of NCSC's Cyber Security Information Sharing Partnership (CiSP)
	1.3 Review and improve the processes for alerting the public sector organisations to cyber threats, risks and incidents
	1.4 Include information on cyber threat and risk into the advice and guidance from advisory/regulatory bodies
	1.5 Support organisations to make use of research and innovation and engage with academia and innovation centres
2. Improve cyber resilient behaviours within public sector organisations	2.1 Promote staff awareness raising and workplace learning as a significant defence against cyber threats
3. Improve and increase opportunities for professional development of IT and cyber security staff across the public sector	3.1 Promote skills development opportunities within the workplace including: <ul style="list-style-type: none"> • increasing the uptake of cyber security apprenticeship training • ensuring skills development opportunities are inclusive • ensuring that cyber security upskilling and reskilling opportunities are available nationwide • supporting the cyber security profession by promoting the adoption of best practice and professional standards
	3.2 Encourage employer engagement with education in order to inspire young people into careers in cyber security

Overarching aims	Actions
<p>4. Embed cyber security standards, regulations and compliance across public sector organisations</p>	<p>4.1 Promote the range of cyber security standards and regulations available to support informed choices for the public sector based on their exposure to risk and their risk appetite</p>
	<p>4.2 Promote a baseline security standard, incorporating Cyber Essentials and Cyber Essentials Plus, to protect against the most common non-targeted cyber attacks</p>
	<p>4.3 Encourage the cyber resilience of the public sector's supply chains, including their adoption of a secure by design approach</p>
	<p>4.4 Influence the development of the NCSC's Cyber Essentials standard to ensure it stays relevant and appropriate for Scottish organisations</p>
<p>5. Embed cyber resilience into the governance, policies and processes of public sector bodies</p>	<p>5.1 Embed cyber resilience into governance arrangements to ensure decision-makers are equipped and supported to manage cyber risk</p>
	<p>5.2 Support organisations to continue to identify and increase their cyber resilience maturity, including exploring options for an online self-assessment tool to enable organisations to assess their own cyber resilience maturity and provide assurance to the Scottish Government on an annual basis</p>
	<p>5.3 Encourage organisations to progress past the baseline standards of the Scottish Government's Public Sector Cyber Resilience Framework and aim to align with a higher progression stage (Target or Advanced)</p>
	<p>5.4 Review the Scottish Public Sector Cyber Resilience Framework every two years to ensure relevance in light of changing technologies and standards</p>
	<p>5.5 Seek to embed the Scottish Public Sector Cyber Resilience Framework into the Scottish Public Finance Manual and Scottish Government grant processes</p>

Overarching aims	Actions
<p>6. Raise awareness of the cyber security services available to public sector organisations</p>	<p>6.1 Support cyber security and managed IT service providers to become more secure and resilient</p>
	<p>6.2 Support organisations to understand what services they need from cyber security and managed IT service providers</p>
	<p>6.3 Maintain and promote the use of the Dynamic Purchasing Scheme to enable the public sector to have rapid access to cyber security expertise</p>
	<p>6.4 Encourage Scotland-based cyber security companies to provide goods and services that can meet the cyber resilience needs of our public sector and digital public services</p>
<p>7. Support public sector organisations to prepare for, respond to and recover from cyber incidents</p>	<p>7.1 Increase good incident response arrangements across the public sector including:</p> <ul style="list-style-type: none"> • promoting testing and exercising, and in particular expanding the take up of the NCSC’s Exercise in a Box Toolkit • encouraging the use of NCSC Response and Recovery guidance
	<p>7.2 Promote and actively encourage uptake of the range of tools and services within the NCSC Active Cyber Defence programme and explore options for increasing accessibility for all public sector organisations</p>
	<p>7.3 Embed cyber resilience into procurement and audit process</p>
	<p>7.4 Explore options to migrate to an online incident reporting mechanism, as an evolution of the current central incident notification and reporting policy</p>
	<p>7.5 Explore options for improving the cyber security operations (SOC) capabilities for the public sector as a whole</p>
	<p>7.6 Use current evidence to inform effective and innovative approaches for improving cyber resilience across the public sector, engaging with innovation centres and academia</p>

Overarching aims	Actions
<p>8. Ensure effective national cyber incident response</p>	<p>8.1 Establish an annual national cyber exercise to ensure effective ongoing cross-agency co-ordination arrangements</p>
	<p>8.2 Raise awareness of national cyber incident management arrangements across government and its agencies to ensure preparedness</p>
	<p>8.3 Review national cyber incident management arrangements on an annual basis</p>
	<p>8.4 Improve cyber threat intelligence across agencies</p>
<p>9. Protect the digital systems that underpin Scotland's essential services</p>	<p>9.1 Ensure a secure by design approach is adopted across the supply chain and aligns with the UK Government's proposal for regulating the cyber security of smart products</p>
<p>10. Ensure that developments relating to Smart Cities are secure</p>	<p>10.1 Work with Smart Cities policy leads to ensure a secure by design approach is adopted in policy and aligns with the UK Government's proposal for regulating the cyber security of smart products as well as the uptake of NCSC's guidance to help authorities to build awareness and understanding of the security needed to design, build, and manage their connected places</p>

Private Sector Action Plan

Overarching aims	Actions
<p>1. Increase businesses' understanding of cyber risks that may affect them</p>	<p>1.1 Increase access to, and use of, threat intelligence, situational awareness reports and alerts to inform understanding of risk and improve the co-ordination and amplification of cyber threat messaging</p>
	<p>1.2 Increase senior leaders' understanding and management of cyber risk to their organisations through a range of engagement activities</p>
	<p>1.3 Promote the use of NCSC's Cyber Security Information Sharing Partnership (CiSP)</p>
	<p>1.4 Work with key business touchpoints such as Banks, Solicitors, Accountants Managed Service Providers, Enterprise Agencies & Insurance Brokers to improve knowledge and awareness of Client/Business Relationship Managers on the range of cyber resilience resources in order that they can improve their portfolio of advice and guidance being offered to businesses/clients</p>
<p>2. Improve cyber resilient behaviours within businesses</p>	<p>2.1 Promote staff awareness raising and workplace learning as a significant defence against cyber threats</p>
<p>3. Improve and increase opportunities for professional development of IT and cyber security staff across the private sector</p>	<p>3.1 Promote skills development opportunities within the workplace including:</p> <ul style="list-style-type: none"> • increasing the uptake of cyber security apprenticeship training • ensuring skills development opportunities are inclusive • ensuring that cyber security upskilling and reskilling opportunities are available nationwide • supporting the cyber security profession by promoting the adoption of best practice and professional standards
	<p>3.2 Encourage employer engagement with education in order to inspire young people into careers in cyber security</p>

Overarching aims	Actions
<p>4. Encourage the embedding of cyber security standards, regulations and compliance across the private sector</p>	<p>4.1 Promote the range of cyber security standards and regulations available to support informed choices for businesses, based on their exposure to risk and their risk appetite</p>
	<p>4.2 Promote Cyber Essentials and Cyber Essentials Plus as the baseline security standards to protect against the most common non-targeted cyber attacks</p>
	<p>4.3 Encourage the cyber resilience of the private sector's supply chains, including their adoption of a secure by design approach</p>
<p>5. Embed cyber resilience into the governance, policies and processes of businesses in Scotland</p>	<p>5.1 Embed cyber resilience into governance arrangements to ensure decision-makers are equipped and supported to manage cyber risk</p>
	<p>5.2 Support organisations to continue to identify and increase their cyber resilience maturity, including exploring options for an online self-assessment tool to enable organisations to assess their own cyber resilience maturity</p>
	<p>5.3 Explore options to adapt the Scottish Government's Public Sector Cyber Resilience Framework for businesses, particularly SMEs</p>
<p>6. Raise awareness of cyber security services and expertise available to businesses</p>	<p>6.1 Encourage Scotland-based cyber security companies to provide goods and services that can meet the cyber resilience needs of our public sector and digital public services. Support cyber security and managed IT service providers to ensure they are secure and resilient</p>
<p>7. Support businesses to prepare for, respond to and recover from cyber incidents</p>	<p>7.1 Increase good incident response arrangements of SMEs including:</p> <ul style="list-style-type: none"> • promoting testing and exercising and in particular expanding the take up of the NCSC's Exercise in a Box Toolkit • encouraging the use of NCSC's Response and Recovery guidance
	<p>7.2 Encourage cyber resilience into procurement and audit processes</p>
	<p>7.3 Use current evidence to inform effective and innovative approaches for improving cyber resilience across the private sector, engaging with innovation centres and academia</p>

Third Sector Action Plan

Overarching aims	Actions
<p>1. Increase third sector organisations' understanding of cyber risks that may affect them</p>	<p>1.1 Increase access to, and use of, threat intelligence to inform understanding of risk</p>
	<p>1.2 Promote the use of NCSC's Cyber Security Information Sharing Partnership (CiSP)</p>
	<p>1.3 Include information on cyber threat and risk in advice and guidance from third sector advisory and regulatory bodies</p>
	<p>1.4 Support organisations to make use of research and innovation and to engage with academia and innovation centres</p>
<p>2. Improve cyber resilient behaviours within third sector organisations</p>	<p>2.1 Promote staff awareness raising and workplace learning as a significant defence against cyber threats</p>
<p>3. Improve and increase opportunities for professional development of IT and cyber security staff across the Third Sector</p>	<p>3.1 Promote skills development opportunities within the workplace including:</p> <ul style="list-style-type: none"> • ensuring skills development opportunities are inclusive • ensuring that cyber security upskilling and reskilling opportunities are available nationwide • supporting the cyber security profession by promoting the adoption of best practice and professional standards
	<p>3.2 Encourage employer engagement with education in order to inspire young people into careers in cyber security</p>
<p>4. Embed cyber security standards, regulations and compliance across third sector organisations</p>	<p>4.1 Promote the range of cyber security standards and regulations available to support clearer choices for the Third Sector based on their exposure to risk and their risk appetite</p>
	<p>4.2 Promote Cyber Essentials and Cyber Essentials Plus as the baseline security standards to protect against the most common non-targeted cyber attacks</p>
	<p>4.3 Encourage the cyber resilience of the third sector's supply chains, including their adoption of a secure by design approach</p>
	<p>4.4 Work to simplify the complexity of the range of standards/regulation around information security</p>

Overarching aims	Actions
<p>5. Embed cyber resilience into the governance, policies and processes of third sector organisations</p>	<p>5.1 Embed cyber resilience into governance arrangements to ensure decision-makers are equipped and supported to manage cyber risk</p>
	<p>5.2 Support organisations to continue to identify and increase their cyber resilience maturity, including exploring options for an online self-assessment tool to enable organisations to assess their own cyber resilience maturity</p>
<p>6. Raise awareness of cyber security services and expertise available to third sector organisations</p>	<p>6.1 Support third sector organisations to understand what services they need from cyber security and managed IT service providers</p>
	<p>6.2 Encourage Scotland-based cyber security companies to provide goods and services that can meet the cyber resilience needs of our Third sector</p>
<p>7. Support third sector organisations to prepare for, respond to and recover from cyber incidents</p>	<p>7.1 Increase good incident response arrangements across the Third sector including:</p> <ul style="list-style-type: none"> • promoting testing and exercising and in particular expanding the take up of the NCSC’s Exercise in a Box Toolkit • encouraging the use of NCSC Response and Recovery guidance
	<p>7.2 Promote and actively encourage uptake of the range of tools and services within the NCSC Active Cyber Defence programme Work with NCSC to promote their Active Cyber Defence (ACD) Programme of tools and measures, and explore options for increasing accessibility for all third sector organisations</p>
	<p>7.3 Encourage the embedding of cyber resilience into procurement and audit processes</p>
	<p>7.4 Explore options for improving the cyber security operations (SOC) capabilities for the Third Sector as a whole</p>
	<p>7.5 Use current evidence to inform effective and innovative approaches to improving cyber resilience across the Third Sector, engaging with innovation centres and academia</p>

Learning and Skills

Overarching aims	Actions
<p>1. Increase people's cyber resilience through awareness raising and engagement</p>	<p>1.1 Disseminate general and targeted cyber awareness messages to individuals, groups and communities, and ensure these are in accessible/alternative formats where possible</p>
	<p>1.2 Monitor changes and improvements in cyber resilience behaviours among the general population</p>
<p>2. Explicitly embed cyber resilience throughout our education and lifelong learning system</p>	<p>2.1 Build capacity across school education for teachers to embed cyber resilience learning across the curriculum, with the support of training, resources and tailored guidance/support</p>
	<p>2.2 Work with key community learning and development (CLD) partners to further embed cyber resilience learning and skills development in non-formal learning</p>
	<p>2.3 Embed cyber resilience within initial training for education professionals</p>
	<p>2.4 Work with colleges, universities and training providers to embed cyber resilience across their delivery</p>
	<p>2.5 Support parents and carers to help with their children's cyber resilience</p>
	<p>2.6 Work with care providers whose staff are well placed to support their clients to be more cyber resilient</p>
<p>3. Increase people's cyber resilience at work</p>	<p>3.1 Increase workers' cyber resilience across all roles, levels and sectors</p>
	<p>3.2 Embed cyber resilience across multiple vocational and occupational areas</p>

Overarching aims	Actions
<p>4. Support the development of accessible cyber security skills training pathways and effective careers guidance to help ensure that skills supply meets demand</p>	<p>4.1 Maintain research evidence, updating knowledge where appropriate, in order to underpin an effective approach to cyber security skills development in Scotland, including understanding best practice globally</p>
	<p>4.2 Promote cyber security careers and a range of training pathways</p>
	<p>4.3 Grow numbers of people studying cyber security in Scotland at all levels</p>
	<p>4.4 Increase the uptake of cyber security apprenticeship training and provision</p>
	<p>4.5 Ensure education professionals have access to support and materials to enable them to deliver cyber-related qualifications, recognising the wider digital learning landscape</p>
	<p>4.6 Ensure cyber security skills development opportunities are inclusive, particularly of women and girls, people from disadvantaged backgrounds, people from BAME backgrounds, and neurodivergent people, including championing skills development opportunities for under-represented groups</p>
	<p>4.7 Ensure that cyber security upskilling and reskilling opportunities are available nationwide as part of wider strategies to reskill and upskill, especially to areas that have had historically low take up/access to opportunities</p>
	<p>4.8 Co-ordinate and shape added-value/extra-curricular programmes in cyber security for effective rollout in Scotland so that they are part of a coherent offer</p>
	<p>4.9 Support the cyber security profession by promoting the adoption of best practice and professional standards</p>
	<p>4.10 Support both individuals and employers navigate a complex cyber security profession, to help talent enter and develop a career in cyber security, working alongside the new UK Cyber Security Council to develop a career pathways framework built on the Cyber Security Body of Knowledge</p>
	<p>4.11 Work with partners at UK level to ensure appropriate alignment of cyber skills development plans</p>
	<p>4.12 Increase cyber security and cyber resilience research and innovation in our university sector</p>

Overarching aims	Actions
	4.13 Strengthen our ecosystem by better linking cyber security skills development, academia and innovation with industry
	4.14 Strengthen interaction between all parts of our education and lifelong learning system around cyber security skills development to grow new pathways and opportunities
	4.15 Co-ordinate, prioritise and target industry/employer engagement in education in order to promote cyber security careers and add value to cyber security skills development for young people

ANNEX D

MEASUREMENT

Strategic Indicators

This table outlines the indicators we have identified at this stage to measure our progress. New indicators and/or sources of evidence may become available as we move forward.

Strategic Outcome	Indicators	Sources
People recognise the cyber risks and are well prepared to manage them	Percentage of adults taking various security measures online; percentage of adults being confident in pursuing a number of online activities	Scottish Household Survey
	Number of young people taking part in learning and skills programmes at school, college and university level	Higher Education Statistics Authority (HESA); SG Data Heat Map for Schools
	Cyber crime statistics	Scottish Crime and Justice Survey
	Cyber literacy levels	Oliver Wyman Forum Global Cyber Risk Literacy and Education Index
	Young people's cyber security behaviours and knowledge	Young People in Scotland Survey

Strategic Outcome	Indicators	Sources
Businesses and organisations recognise the cyber risks and are well prepared to manage them	Businesses and third sector organisations' cyber security measures, experiences of cyber attacks	SG Digital Economy Business Survey
	Uptake of Cyber Essentials	IASME and SG data
	Record of reported cyber breaches	SBRC, Police Scotland and NCSC data
	Growth of cyber security industry	ScotlandIS data; UK Government data
	Mean salary offer for core cyber jobs postings and cyber jobs hotspots	Cyber security skills in the UK labour market surveys
	Businesses and individuals' engagement with: - the CyberScotland Partnership Portal - number of subscriptions to the CyberScotland Bulletin	CyberScotland Partnership data
	Scottish Public Sector Cyber Resilience Framework	Public Sector Action Plan monitoring arrangements
Digital public services are secure and cyber resilient	Cyber resilience and security of digital public services as an integral part of the new Digital Strategy	SG Digital Strategy
	Additional indicators to be developed	SG
National cyber incident response arrangements are effective	Number of times national plan is tested and exercised	SG

ANNEX E



The CyberScotland Partnership is a collaboration of key strategic stakeholders, brought together to focus efforts on improving cyber resilience across Scotland in a co-ordinated and coherent way.

It represents a commitment from partners to work together to drive the delivery of activities that will help achieve the outcomes of *The Strategic Framework for a Cyber Resilient Scotland*.

Partners will work collaboratively to:

- ✓ build Scotland-wide cyber resilience
- ✓ increase effectiveness and impact, avoiding duplication of effort
- ✓ improve communication and knowledge-sharing relating to cyber threats
- ✓ provide a single online portal for organisations, businesses and individuals seeking information, guidance and support on cyber resilience issues
- ✓ promote national events, in particular the annual CyberScotland Week
- ✓ collectively support the cyber security community.

CyberScotland Partners include:





Scottish Government
Riaghaltas na h-Alba
gov.scot

© Crown copyright 2021

OGL

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.

This publication is available at www.gov.scot

Any enquiries regarding this publication should be sent to us at
The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-80004-705-1

Published by The Scottish Government, February 2021

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS823306 (02/21)

W W W . g o v . s c o t
