

# Action Plan 2025-2030



**The Strategic  
Framework for  
a Cyber Resilient  
Scotland**

**2025-2030**



**From risk to opportunity**

This Action Plan sets out the key actions during 2025 – 2030 to deliver the priorities set out in the [Strategic Framework for a Cyber Resilient Scotland \(2025-2030\)](#).

<b>Vision</b>			
<b>Scotland thrives by being a digitally secure and resilient nation</b>			
<b>Outcomes</b>			
1. People recognise the cyber risks and are well-prepared to manage them.	2. National cyber security and resilience coordination and response arrangements are effective.	3. Scotland’s digital public services are secure and cyber resilient.	
4. Public sector organisations effectively manage their cyber risk.	5. Businesses recognise the cyber risks and are well prepared to manage them.	6. Third sector organisations recognise the cyber risks and are well prepared to manage them.	
7. Scotland has a flourishing cyber security industry, research community and a skilled cyber security professional workforce			
<b>Principles of Approach</b>			
Inclusive and ethical	Whole-of-society	Agile leadership	Collaborative partnership
Effective communication	Adaptive and agile programme management	Optimal use of data and evidence of impact	Anticipating change and understanding emerging threats
<b>Supported by delivery of the Action Plan</b>			

## How the Action Plan will be delivered, monitored and evaluated

Activities will align with government fiscal planning.

Cyber resilience is a shared responsibility and we are committed to working with government, the public, private and third sectors and individuals.

The Scottish Government's National Cyber Resilience Unit (SG NCRU) will lead coordination, monitoring and performance assessment of the Action Plan. The Plan's effectiveness will be measured against specific metrics, including national (Scottish) and UK cyber resilience indicators. Progress will be tracked annually and evaluated every two years and the plan will be updated as necessary.

Scotland has an ecosystem of delivery partners who all contribute to realising the outcomes of the Strategic Framework. The Action Plan below highlights the key actions that are being delivered by the Main Delivery Partners.

### Main Delivery Partners (as of Spring 2026)



**Working together, we will ensure Scotland thrives as a digitally resilient nation.**

## Outcome 1

### People recognise the cyber risks and are well prepared to manage them

#### 1.1 Raising Awareness

The public better understand cyber risks and know how to protect themselves online, thanks to clear, consistent and inclusive messaging as well as wide-reaching local and national outreach.

**The CyberScotland Partnership will:**

- position the [CyberScotland Portal](#) as the trusted national gateway for cyber resilience advice and guidance
- deliver quarterly national cyber resilience awareness-raising campaigns for the public and organisations in both English and Gaelic
- provide key awareness raising resources in community languages, easy-to-read and British Sign Language
- tailor cyber awareness messaging for priority groups including adult learners, older and younger people, ethnic minority groups and parents, guardians and carers
- increase awareness of, and participation in, CyberScotland Week during February each year
- collaborate to increase Scottish participation in CyberUK (Glasgow 2026) and future CyberUK events, as well as during Cyber Security Awareness Month each year.

#### 1.2 Empowering Action

People can easily report cyber crime and access trusted support when needed.

**Police Scotland and other CyberScotland partners will:**

- embed clear reporting routes for cyber crime and phishing attempts in all cyber resilience awareness campaigns and training.

#### 1.3 Embedding Resilience in Learning

Cyber resilience, digital security and responsible online behaviours are integrated into our lifelong and life-wide learning system from the earliest stages through to adulthood.

**Educators across the lifelong learning system will:**

- access practitioner training to support them to deliver effective cyber resilience learning and awareness.

**Education Scotland will:**

- continue to embed cyber resilience as a core competency within the 5–18 curriculum
- continue to increase the number of schools delivering cyber security learning and qualifications
- continue to increase the number of pupils taking cyber security qualifications

- continue to support teachers to develop their capabilities to effectively deliver cyber resilience and security learning.

**The Scottish Government’s National Cyber Resilience Unit (SG NCRU) and Education Scotland** will:

- produce and distribute an Early Level book introducing basic cyber security concepts to primary school-aged children.

**YouthLink Scotland and Community Learning & Development partners** will:

- embed cyber resilience within community learning opportunities.

**The SG NCRU, Abertay University, Universities Scotland, Colleges Scotland and the College Development Network** will:

- strengthen cyber awareness across colleges and universities by rolling out the [Cyber Resilience and You!](#) online learning tool to all students in Scotland, including translating it into Gaelic.

## **1.4 Strengthening the Workforce**

Employees across all jobs and sectors can identify and manage cyber risks, supported by a workplace culture that prioritises awareness and resilience.

**The CyberScotland Partnership** will:

- signpost organisations and staff to trusted cyber resilience training and resources through the [CyberScotland Portal](#) and the [NCSC](#) website
- work with unions, employer bodies and trade bodies to extend cyber resilience awareness to workers across sectors
- identify gaps in workforce cyber resilience and develop targeted guidance, resources and training to address them.

## **Outcome 2**

### **National cyber security and resilience co-ordination and response arrangements are effective**

#### **2.1 National Preparedness**

National cyber response capabilities are regularly tested and exercised, supported by strong cross-agency partnerships to ensure a coordinated and effective response.

**The Scottish Cyber Coordination Centre (SC3) will:**

- review the Scottish cyber incident response arrangements, ensuring alignment with the UK Government's response arrangements
- continue to raise awareness of the Scottish cyber incident multi-agency co-ordination arrangements to support consistent preparedness
- run an annual national multi-agency exercise to test response plans against current and emerging cross-cutting threats
- coordinate multi-agency responses to cyber incidents affecting the Scottish public sector, working with key partners including Police Scotland and the National Cyber Security Centre (NCSC).

#### **2.2 Testing Readiness at All Levels**

SC3 supports the public sector in regularly testing and exercising cyber response capabilities at strategic, tactical and operational levels.

**SC3 will:**

- facilitate and support the delivery of at least ten cyber exercises each year, helping public bodies across Scotland to test and strengthen their incident response plans
- develop a public sector exercising cadre trained to design, prepare and deliver cyber exercises at a local level
- produce and share a suite of exercising resources, including open-source materials
- collect annual data on cyber exercising across the Scottish public sector to identify gaps, to increase and to improve uptake.

#### **2.3 Keeping Plans Incident-Ready**

National response plans and playbooks are regularly reviewed and updated to reflect the evolving threat landscape.

**SC3 will:**

- update cyber incident response procedures and playbooks annually, ensuring all materials reflect lessons learned from real incidents and exercises, as well as emerging and evolving cyber threats.

#### **2.4 Delivering Early Warnings and Threat Intelligence**

SC3 creates a robust intelligence sharing network to provide and disseminate tailored and curated threat intelligence across sectors in order to enable quicker and more proactive defence and preparedness.

**SC3** will:

- continue to produce and disseminate daily and weekly curated threat intelligence reports
- provide tailored public sector intelligence products, including monthly Ransomware reports and quarterly Insight reports
- issue Cyber Resilience Early Warning (CREW) notices and Threat Intelligence Priority Reporting (TIPR) alerts on new and emerging threats, including recommended remediation or preventive actions
- host the CyberShield Scotland Malware Information Sharing Platform (MISP), expand public sector membership and strengthen cross government collaboration

## **2.5 Enhancing Vulnerability Awareness**

The monitoring and detection of, and response to, critical vulnerabilities are strengthened by enhancing vulnerability scanning capabilities and improving centralised vulnerability disclosure and reporting services.

**SC3** will

- evolve its approach to vulnerability identification by making use of the domain scanning services provided by Department of Science, Innovation & Technology (DSIT)
- establish a central Vulnerability Disclosure Programme for public sector organisations, building on the UK's Government Cyber Coordination Centre (GC3)'s existing Vulnerability Disclosure Programme
- monitor open and closed source intelligence on major vulnerabilities as part of SC3's Vulnerability Coordination Policy and share timely patching advice with public sector organisations.

## **2.6 Understanding the cyber maturity of the public sector**

The Cyber Observatory enhances our ability to understand and measure the cyber maturity of the public sector to improve targeted interventions and support.

**SC3** will:

- launch the national Cyber Resilience Assessment (CRA) in 2025 through the Cyber Observatory to gather self-assessed cyber resilience data from Scottish public sector bodies
- from 2026 onwards, require public sector organisations to complete and submit the CRA annually via the Cyber Observatory
- use the enhanced capabilities of the Cyber Observatory to analyse CRA responses alongside other relevant data sources to provide a more accurate picture of current public sector cyber maturity and risk, and to inform decision making and future action
- use these insights to design and deliver targeted interventions that will help strengthen cyber resilience across the Scottish public sector.

## **2.7 Learning and Improving**

Lessons learned from real incidents and exercises are captured, analysed and shared to continuously improve deterrence and response capabilities.

**SC3 will:**

- publish and disseminate the first annual Scottish Cyber Activity Report (SCAR) in 2026, sharing lessons identified from cyber incidents and exercises to support wider learning and improvement
- deliver lessons learned projects for the Scottish public sector in 2025 and 2026, initially focusing on Legacy Technology and Multi Factor Authentication (MFA) as priority areas for improvement and organisational guidance.

## **2.8 Strengthening Collaboration**

Partnerships between the Scottish Government, SC3, NCSC, Police Scotland, CSP, public sector bodies, academia and the cyber security industry are deepened to enhance incident response, horizon scanning, sharing knowledge and expertise to encourage innovation and solutions.

**SG NCRU, alongside SC3, will:**

- regularly convene the Public Sector Network as a key channel for sharing knowledge, resources and best practice.

**SC3 will:**

- engage routinely with SC3 Core Partners, including Scottish Government, Police Scotland, NCSC, Digital Office - Scottish Local Government, NHS National Services Scotland, HEFESTIS and GC3, to share insights and identify solutions that support national cyber resilience in line with the SC3 Strategic Plan
- continue operating as a multi-agency function, with embedded resources from Police Scotland, NCSC and other partners to strengthen capabilities, collaboration and ensure rapid, co-ordinated responses to emerging threats and incidents.

## Outcome 3

# Scotland's digital public services are secure and cyber resilient

### 3.1 Securing legacy systems and ensuring secure-by-design and by-default systems

Appropriate mitigations are in place to secure legacy systems. A secure-by-design and by-default approach is embedded across digital public systems, services and infrastructure.

**The Scottish Government and national digital service providers will:**

- continue to identify legacy IT systems and fully understand the cyber risks they pose
- replace legacy systems as a critical step in improving cyber resilience. Where legacy systems remain in use, cyber risks are actively managed with clear risk ownership until replacement is possible
- ensure that new systems are secure by design and secure by default throughout their lifecycle, with maintenance, support and long-term sustainability planned from the outset to prevent future legacy challenges.

### 3.2 Adhering to Cyber Security Standards and Regulations

Digital public services align with the relevant recognised standards and regulations.

**The Scottish Government and national digital service providers will:**

- use NCSC's [Cyber Assessment Framework](#) (CAF) as their guiding framework for managing cyber resilience
- apply the [GovAssure](#) scheme for assessing critical systems in order to meet CAF objectives
- follow the principles of secure-by-design when building digital services and technical infrastructure.

### 3.3 Securing the Supply Chain

Digital public service supply chains are secure to protect against cyber threats. This includes regular risk assessments, enforcing security requirements in procurement and monitoring third-party compliance.

**The Scottish Government and national digital service providers will:**

- establish a risk-based Supply Chain Security Framework and standardise its use across digital procurement, ensuring suppliers understand the baseline security requirements expected of them
- align supply chain security policies with [NCSC Supply Chain Security Principles](#) and UK Government [Procurement Security Guidelines](#)
- ensure suppliers meet relevant certifications, such as Cyber Essentials Plus, ISO/IEC 27001 and other appropriate industry standards

- embed security requirements into public sector supplier contracts - mandating clear and enforceable clauses covering data protection, incident reporting and compliance auditing.

### **3.4 Enhancing incident response and recovery**

A national framework for cyber incident response is strengthened, ensuring rapid recovery and continuity of essential digital public services.

**The Scottish Government and national digital service providers will:**

- enhance and refine their Cyber Incident Response Plans (CIRPs) to ensure continuous improvement and alignment with NCSC [Incident Management Guidance](#) and recognised industry best practice
- conduct regular crisis management exercises, tabletop simulations and live attack drills to test organisational readiness
- define clear incident severity levels, escalation procedures and response playbooks for a range of attack scenarios, including ransomware, insider threats and nation state attacks
- foster a culture of cyber resilience and integrate cyber incident response with Business Continuity and Disaster Recovery (BCDR) plans to ensure coordinated recovery
- maintain and regularly test alternative communication channels for use during incidents where primary IT infrastructure is compromised
- ensure backup and recovery processes are robust, immutable and tested frequently to enable rapid restoration of services and minimise operational disruption
- maintain a joined-up approach to incident response in collaboration with the SC3.

### **3.5 Enabling safe use of emerging technologies**

Guidance and governance are developed to ensure the secure deployment of AI, Automation, machine learning, quantum and IoT (Internet of Things) technologies in public services.

**The Scottish Government and national digital service providers will:**

- ensure appropriate governance is in place to support the secure adoption and use of new and emerging technologies
- maintain awareness of standards and guidance issued by relevant technical authorities and ensure these are integrated into organisational governance processes and technical design boards.

### **3.6 Maximising public-private collaboration**

The Scottish Government and other public bodies deepen engagement with industry and academia to access industry cutting-edge solutions, share threat intelligence and co-develop secure digital platforms.

**The Scottish Government and national digital service providers will:**

- ensure insights from NCSC's socio-technical research inform the design and development of digital platforms

- take into account the UK Government's cyber security [Codes of Practice](#) and relevant NCSC guidance including [Secure development and deployment guidance](#).
- consider sponsoring [Civtech](#) challenges that address public sector cyber resilience needs
- engage with industry and academia to explore the cyber security benefits of emerging technologies and identify opportunities to adopt them within government settings, for example, homomorphic encryption, crypto-agility for quantum-safe encryption, artificial intelligence agents and model context protocols.

## Outcome 4

### Public Sector organisations effectively manage their cyber risks

#### 4.1 Positioning Cyber Risk and Assurance as a Leadership Priority

Public sector leaders ensure that cyber risk and assurance are embedded in strategic planning and at board level, and that they drive a culture of accountability and resilience throughout the organisation.

**The SG NCRU and SC3 will:**

- establish and promote mandatory cyber security and resilience policies and baseline standards to ensure consistent and effective cyber risk management across the public sector
- strengthen public sector leaders' understanding of cyber risk through a targeted programme of awareness raising for Chief Executives, board members and audit and risk committee leads, and by promoting resources including NCSC's [Board Toolkit](#) and [Cyber Governance Training](#).

**Public sector organisations will:**

- designate a board member or senior leader to be responsible for assuring organisational cyber resilience.

#### 4.2 Embedding Cyber Resilience into Governance

Organisations integrate relevant cyber security standards, regulations and compliance into governance, business risk management, planning and daily operations

**The SG NCRU will:**

- promote the [UK Government Cyber Governance Code of Practice](#) to all public sector organisations.

**Public sector organisations will:**

- establish robust governance arrangements for cyber security and resilience, including:
  - incorporating cyber risks within strategic or corporate risk registers
  - regular consideration of cyber risks at senior management and audit and risk committee levels
  - appointing a designated board member responsible for cyber security and resilience
  - adopting appropriate cyber security standards, such as NCSC's [Cyber Assessment Framework](#)
  - obtaining independent assurance of critical technical controls, for example through [Cyber Essentials](#) and Cyber Essentials Plus

- understanding the organisation's critical systems and dependencies, implementing measures to mitigate impacts on essential functions and maintaining plans to restore services after an incident
- familiarising themselves with the UK Government's [cyber security Codes of Practice](#)
- improving cyber security measures based on lessons learned from exercises and incidents.
- promote the ScotlandIS [Cyber Directory](#) and [ITMS Directory](#) as the central source for Scotland based cyber products and services across the public sector

**Public sector advisory and regulatory bodies will:**

- embed cyber threat and risk information within their guidance to public bodies.

### 4.3 Ensuring Incident Readiness

Organisations have robust incident response capabilities and regularly test and exercise.

**Public sector organisations will:**

- participate in the Scottish Government's annual assessment (CRA) of the cyber maturity of the Scottish public sector
- continuously monitor networks and systems with secure logging in place
- maintain secure, reliable backups required to restore essential functions
- develop and maintain cyber incident response plans
- test incident response plans at least annually against common attack scenarios at technical, operational and strategic levels, following SC3 guidance, including using tools from SC3, NCSC and relevant open-source providers
- review and share lessons identified and learned from exercises and significant incidents through the Public Sector Cyber Resilience Network and SC3 reports
- act quickly on Cyber Resilience Early Warning Notices.

### 4.4 Securing legacy systems and introducing secure-by-design and default systems

Organisations plan to migrate to modern secure-by-design and secure-by-default systems and/or to put in place appropriate mitigations to secure legacy systems.

**Public sector organisations will:**

- review and understand their use of legacy systems
- mitigate vulnerabilities associated with legacy systems in the short term
- replace legacy systems with secure-by-design and secure-by-default alternatives in the longer term.

### 4.5 Using Trusted Tools

Organisations use proven security solutions, including NCSC's Active Cyber Defence services.

**Public sector organisations will:**

- adopt NCSC [Active Cyber Defence measures](#) (where eligible), including Early Warning and Protective DNS (PDNS).

#### 4.6 Securing the Supply Chain

Organisations actively manage third-party risks with confidence and throughout the life cycle of contracts.

**The SG NCRU and SC3 will:**

- support public bodies with advice, guidance and common solutions to secure their supply chains.

**Public sector organisations will:**

- build appropriate cyber assurance into procurement and contract management processes.

#### 4.7 Building Professional Capability

Organisations develop their professional cyber security workforce, through inclusive recruitment, training, professional development and career progression. Cyber security staff will be encouraged to register with the UK Cyber Security Council, with a view to gaining a relevant professional standard.

**The SG NCRU will:**

- encourage public sector organisations to support the continuous professional development of their cyber security workforce
- promote the [UK Cyber Security Council](#) and the benefits of professionalisation, creating opportunities for engagement with cyber professionals across Scotland
- provide employers with practical guidance to attract, recruit and retain diverse cyber talent by identifying and removing barriers, including those affecting women and those with disabilities.

**Public sector organisations will:**

- encourage continuous professional development of their cyber security staff.

#### 4.8 Raising Workforce Awareness

The public sector workforce demonstrates strong cyber resilient behaviours.

**Public sector organisations will:**

- provide appropriate cyber resilience training and awareness for staff at all levels
- signpost staff to authoritative cyber resilience training and resources via [CyberScotland Portal](#) and the [NCSC](#) website.

#### 4.9 Reporting Cyber Incidents

Organisations report cyber incidents to Police Scotland, NCSC, SC3, ICO, where appropriate.

**Public sector organisations will:**

- use the [Scottish Public Sector Cyber Incident Notification Process](#) to report incidents to SC3, Police Scotland and NCSC, where appropriate
- report a cyber crime to Police Scotland on 101
- notify relevant regulatory authorities, such as the [ICO](#), to report cyber security incidents within required timescales.

#### **4.10 Strengthening Cross-Sector Collaboration**

The Public Sector, government, academia and industry continue to build stronger partnerships to improve incident response and share knowledge, innovation and expertise

**The SG NCRU and SC3 will:**

- exchange and co-develop briefing materials for the public sector
- organise quarterly Public Sector Cyber Resilience Network events
- utilise the expertise of the [National Cyber Resilience Advisory Board](#) to provide strategic advice and constructive challenge to support effective delivery of the Strategic Framework for a Cyber Resilient Scotland
- encourage widespread use of [CyberScotland Portal](#) for best practice guidance and support.

## Outcome 5

### Businesses recognise the cyber risks and are well prepared to manage them

#### 5.1 Positioning Cyber Risk and Assurance as a Leadership Priority

Business leaders ensure that cyber risk and assurance are embedded in strategic planning and at board level, and that they drive a culture of cyber resilience throughout the business.

**The CyberScotland Partnership will:**

- encourage business leaders' awareness to build their understanding of cyber risk by promoting NCSC resources, including the [Cyber Security Toolkits for Boards](#) and [Cyber Governance Training](#), where appropriate.

#### 5.2 Embedding Cyber Resilience into Governance

Businesses integrate relevant cyber security standards, regulations and compliance into governance, business risk management, planning and operations.

**The CyberScotland Partnership will:**

- encourage private sector organisations to embed cyber resilience into their governance arrangements so decision makers are equipped to manage cyber risk
- support private sector organisations to assess and improve their cyber resilience maturity, including through NCSC's [Cyber Action Toolkit](#)
- promote the UK Government's [Cyber Governance Code of Practice](#) to all private sector organisations
- encourage adoption of [Cyber Essentials](#) and Cyber Essentials Plus as baseline protection, using the Cyber Action Toolkit as a pathway
- build awareness of emerging risks linked to new technologies (e.g. AI, machine learning, IoT, quantum technologies).

**ScotlandIS and other CyberScotland partners will:**

- promote the ScotlandIS [Cyber Directory](#) and [ITMS Directory](#) as the central source for Scotland based cyber products and services across the private sector.

#### 5.3 Ensuring Incident Readiness

Businesses regularly test and exercise incident response plans and recovery capabilities.

**The SG NCRU and other CyberScotland Partners will:**

- encourage private sector organisations to test and exercise their incident response arrangements regularly against a range of cyber incident scenarios, including through tools such as the open-source [TTX Gym](#) and NCSC's exercising resources
- promote NCSC incident [response and recovery](#) guidance.

## 5.4 Addressing Legacy Systems

Businesses identify and manage risks associated with legacy systems. Where feasible, implementing mitigation measures or planning for system upgrades to reduce exposure to cyber threats.

**The CyberScotland Partnership will:**

- encourage private sector organisations to review their legacy systems and manage them as part of overall business risk
- encourage private sector organisations to adopt short-term mitigations for legacy vulnerabilities and long-term replacement with secure-by-design and secure-by-default systems
- promote NCSC [guidance](#) to help organisations design, review and secure the connectivity within and to their Operational Technology (OT) systems
- promote NCSC [device security](#) guidance to help organisations manage device security and reduce risks from obsolete or unsupported technologies.

## 5.5 Using Trusted Tools

Businesses use proven security solutions, including NCSC's Active Cyber Defence services.

**SG NCRU and other CyberScotland Partners will:**

- promote the range of trusted cyber resilience resources available to private sector organisations via the [CyberScotland Portal](#), including NCSC [Active Cyber Defence](#) services, [NCSC Small Business Guide](#) and [NCSC Cyber Action Toolkit](#).

## 5.6 Raising Workforce Awareness

All staff, at every level, demonstrate strong cyber resilient behaviours and know where to go to access the appropriate advice, guidance and support.

**The CyberScotland Partnership will:**

- signpost staff to authoritative cyber resilience resources and training via the [CyberScotland Portal](#) and the [NCSC](#) website.

**Private sector organisations will:**

- provide relevant cyber resilience training and awareness raising for staff at all levels of the organisation.

## 5.7 Reporting Cyber Incidents

Businesses report cyber incidents to Police Scotland, the NCSC and the ICO, where appropriate.

**Private sector organisations will:**

- report cyber incidents to Police Scotland (via 101) and to NCSC through the [Report a Cyber Incident](#) service
- notify relevant regulatory authorities of incidents, such as the [ICO](#), to report cyber security incidents within required timescales.

## 5.8 Securing the Supply Chain

Businesses manage and actively monitor third-party risks.

**The CyberScotland Partnership will:**

- encourage businesses to assess the cyber resilience of their supply chains and adopt secure-by-design principles-by-design principles
- promote NCSC [supply chain security guidance](#) to help businesses improve their awareness of supply chain security
- encourage businesses to embed appropriate cyber assurance into procurement and contract management.

## 5.9 Building Professional Capability

Businesses develop their professional cyber security capabilities through clear entry points, training and career progression pathways.

**The CyberScotland Partnership will:**

- encourage businesses to support the continuous professional development of their cyber security workforce
- promote the value of professionalising the cyber security workforce and raise awareness of the [UK Cyber Security Council](#), creating opportunities for the Council to engage with practitioners in Scotland
- provide employers with practical guidance to attract, recruit and retain diverse cyber talent by identifying and removing barriers and biases, including those affecting women and those with disabilities.

## 5.10 Strengthening Cross-Sector Collaboration

Businesses, government, academia and industry continue to build stronger partnerships to improve incident response and share knowledge, innovation and expertise

**The CyberScotland Partnership will:**

- strengthen partnerships between the private sector, public sector and academia by sharing knowledge, innovation and expertise, and collaborating on awareness and delivery alignment
- collaborate on the development and exchange of briefing materials for the private sector
- promote the use of [CyberScotland Portal](#) for signposting resources, good practice guidance and support to private sector organisations.

## Outcome 6

### Third sector organisations recognise the cyber risks and are well prepared to manage them

#### 6.1 Positioning Cyber Risk and Assurance as a Leadership Priority

Third sector leaders ensure that cyber risk and assurance are embedded in strategic planning and at board level, and that they drive a culture of accountability and resilience throughout the organisation.

**SCVO and other CyberScotland Partners** will:

- encourage third sector leaders to build their understanding of cyber risk by promoting NCSC and other authoritative resources, including the [Cyber Security Toolkits for Boards](#) and [Cyber Governance Training](#), where appropriate.

**Third sector organisations** will:

- designate a board member or senior leader responsible for overseeing cyber resilience within the organisation
- foster a culture of accountability and resilience
- keep up to date with common threats to inform risk management and mitigation.

#### 6.2 Embedding Cyber Resilience into Governance

Third Sector organisations integrate relevant cyber security and resilience standards, regulations and compliance into governance, business risk management, planning and daily operations.

**Third sector organisations** will:

- embed cyber resilience within their governance structures, managing cyber risk as part of overall business risk and strategic planning
- incorporate cyber resilience principles, including the [Cyber Governance Code of Practice](#) into their operational policies and processes
- adopt trusted mechanisms to gain assurance that their digital systems and data are protected.

**SCVO and other CyberScotland Partners** will:

- support third sector organisations to assess and improve their cyber resilience maturity, including through NCSC's [Cyber Action Toolkit](#)
- encourage adoption of [Cyber Essentials](#) and Cyber Essentials Plus as baseline protection, using the Cyber Action Toolkit as a pathway.

**Third sector advisory and regulatory bodies** will:

- promote the ScotlandIS [Cyber Directory](#) and [ITMS Directory](#) as the central source for Scotland based cyber products and services across the third sector
- include cyber and risk information within their guidance and support broader cyber awareness across the sector.

### 6.3 Ensuring Incident Readiness

Third Sector organisations have robust incident response capabilities and regularly test and exercise.

**Third sector organisations will:**

- implement appropriate protective measures to strengthen their cyber security posture
- regularly test and exercise their incident response arrangements against a range of cyber incident scenarios, including through tools such as the open-source [TTX Gym](#) and NCSC's exercising resources
- use NCSC's incident [response and recovery](#) guidance.

### 6.4 Addressing Legacy Systems

Third sector organisations identify and manage risks associated with legacy systems. Where feasible, implement mitigation measures and/or plan for system upgrades to reduce exposure to cyber threats.

**SCVO and other CyberScotland Partners will:**

- promote NCSC [device security](#) guidance to help organisations manage device security and reduce risks from obsolete or unsupported technologies.

**Third sector organisations will:**

- review their legacy systems and manage them as part of overall business risk.

### 6.5 Using Trusted Tools

Third sector organisations use proven security solutions, including NCSC's Active Cyber Defence services.

**Third sector organisations will:**

- implement appropriate protective measures to improve their cyber security.

**SCVO and other CyberScotland partners will:**

- Promote a range of trusted cyber resilience resources available to third sector organisations via [CyberScotland Portal](#), including NCSC [Active Cyber Defence](#) services and [NCSC Cyber Action Toolkit](#).

### 6.6 Raising Workforce and Volunteers' Awareness

The third sector workforce, including volunteers, demonstrate strong cyber resilient behaviours.

**SCVO and other CyberScotland partners will:**

- signpost staff, including volunteers, to authoritative cyber resilience resources and training via the [CyberScotland Portal](#), SCVO and the [NCSC](#) website.

**Third sector organisations will:**

- raise workforce awareness on how to identify cyber risks and take appropriate action.

## **6.7 Reporting Cyber Incidents**

Third sector organisations report cyber incidents to Police Scotland, SG, NCSC, OSCR and the ICO where appropriate.

**Third sector organisations will:**

- report cyber incidents to Police Scotland (via 101) and to the NCSC through the [Report a Cyber Incident](#) service
- notify relevant regulatory authorities, such as the [ICO](#), of incidents where required. Scottish charities should also report cyber crime to OSCR via [raise a concern form](#).

## **6.8 Securing the Supply Chain**

Third sector organisations actively manage third-party risks with confidence and throughout the life cycle of contracts.

**SCVO and other CyberScotland Partners will:**

- encourage third sector organisations to assess the cyber resilience of their supply chains and adopt secure-by-design principles
- promote NCSC [supply chain security guidance](#) to help third sector organisations improve their awareness of supply chain security
- encourage third sector organisations to embed appropriate cyber assurance into procurement and contract management.

## **6.9 Building Professional Capability**

Third sector organisations develop their professional cyber security capabilities, through inclusive recruitment, training, professional development and career progression, including volunteers.

**SCVO and other CyberScotland partners will:**

- encourage third sector organisations to support the continuous professional development of their cyber security workforce
- promote the value of professionalising the cyber security workforce and raise awareness of the [UK Cyber Security Council](#), creating opportunities for the Council to engage with practitioners in Scotland
- provide employers with practical guidance to attract, recruit and retain diverse cyber talent by identifying and removing barriers and biases, including those affecting women and those with disabilities.

## 6.10 Strengthening Cross-Sector Collaboration

The third sector, government, academia and industry continue to build stronger partnerships to improve incident response and to share knowledge and threat intelligence, innovation and expertise.

**SCVO and other CyberScotland Partners** will:

- strengthen partnerships between the third sector, government and academia – sharing knowledge, innovation and expertise and collaborating on awareness and delivery alignment
- collaborate on the development and exchange of briefing materials for the third sector
- promote the use of [CyberScotland Portal](#) for signposting resources, good practice guidance and support to third sector organisations.

## Outcome 7

# Scotland has a flourishing cyber security industry, research community and a skilled cyber security professional workforce

### 7.1 Growing a Globally Competitive Industry

The Scottish cyber security industry will be seen as an attractive provider of cyber security goods and services both domestically and internationally.

**ScotlandIS and the Scottish Government** will:

- work with enterprise agencies, Scottish Development International and UK Government departments to identify domestic and international growth and trade opportunities for Scottish cyber security businesses
- promote the [ScotlandIS Cyber Directory](#) and [IT Managed Services Directory](#) as the central source for Scotland based cyber security products and services across the public, private and third sectors.

### 7.2 Strengthening Research and Innovation

Academic excellence in research and innovation across our universities continues to help map future cyber challenges and opportunities for government, industry and academia.

**Scottish universities** will:

- work with industry, government, innovation centres and enterprise agencies to support the commercialisation of cyber research, including proof of concept funding, spinouts, licensing and collaborative R&D with Scottish businesses.

**CRANE** ([Cyber Security Research Network](#)) will:

- work with the CyberScotland Partnership to help strengthen the UK cyber security research ecosystem by evaluating emerging technologies, threats and opportunities for novel research, helping to translate findings into tangible security interventions.

### 7.3 Understanding and Mitigating Cyber Risks from Emerging Technologies

Government and academic and industry partners build understanding and mitigation of the cyber threats associated with emerging technologies such as AI, quantum computing and machine learning.

**The Scottish Government, SC3 and the CyberScotland Partnership** will:

- promote authoritative guidance and codes of practice on securing emerging technologies, including those published by NCSC and the UK Government [cyber security Codes of Practice](#).

## 7.4 Strengthening the Talent Pipeline

Schools, colleges and universities increase the uptake of cyber security learning and qualifications, expanding access to apprenticeships and vocational routes and promoting diversity and inclusion at all levels. Young people will be encouraged to pursue cyber security careers.

**All learning providers, Skills Development Scotland (SDS) and other CyberScotland Partners** will:

- promote awareness of cyber security careers across schools, community learning, colleges and universities, helping learners and their parents or guardians understand available education and career pathways
- promote clear, accessible routes into cyber security roles, including entry level opportunities, reskilling and upskilling pathways and progression from digital and STEM (Science, Technology, Engineering and Mathematics) disciplines.

**The Scottish Government, SDS and other CyberScotland Partners** will:

- work with employers and training providers to further establish apprenticeships as a viable pathway into cyber security careers, ensuring the offer aligns with current and future workforce needs.

**The Scottish Government, including SG NCRU and Learning Directorate, and Education Scotland** will:

- work collaboratively with DSIT to align activity and maximise the impact of the cyber security initiatives of the TechFirst programme in Scotland.

## 7.5 Promoting Professional Standards

The Scottish Government will work with industry, the UK Cyber Security Council and the UK Government to enhance efforts to professionalise the cyber security workforce and promote continuous development.

**SG NCRU and other CyberScotland Partners** will:

- promote the value and benefits of professionalising the cyber security workforce and raising awareness of the [UK Cyber Security Council](#), creating opportunities for the Council to engage with cyber security practitioners in Scotland.



© Crown copyright 2026



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](https://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](mailto: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](http://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: 978-1-80643-847-1 (web only)

Published by The Scottish Government, February 2026

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA  
PPDAS1713726 (02/26)

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