The Strategic Framework for a Cyber Resilient Scotland

Action Plans (2023-25)

Vision

"*Scotland thrives by being a digitally secure and resilient nation*"

Digital technology is key to Scotland's future. Scottish Ministers' vision is of a Scotland that thrives by being a digitally secure and resilient nation.

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.

The Scottish Government and its partners will work towards realising these outcomes by implementing four Action Plans: public, private and third sector and a learning and skills Action Plan, delivered by the Scottish Government and its partners between 2023 and 2025.

Scottish Government
Riaghaltas na h-Alba

Public Sector Action Plan (2023-25)

1. Public sector organisations embed cyber resilience into their governance, policies and processes

1.1 All public bodies include cyber resilience within their governance structures, by managing cyber risk as part of business risk and by designating a board member/senior manager to be responsible for cyber resilience within the organisation.

2. Public sector organisations improve their understanding of cyber risks

2.1 All public bodies increase their access to and use of threat intelligence, situational awareness and alerts to inform understanding of risk and mitigation.

2.2 All public bodies become active members of the Scottish Public Sector Group within NCSC's Cyber Security Information Sharing Partnership (CISP) (where eligible).

2.3 The Scottish Government works with advisory and regulatory bodies to embed cyber threat and risk information within their advice and guidance for public bodies.

3. Public sector organisations advance their cyber assurance by embedding cyber security standards and regulations and actively managing compliance

3.1 All public bodies adopt appropriate and relevant cyber security standards and assurance mechanisms.

3.2 All public bodies align with the most appropriate tier of the Public Sector Cyber Resilience Framework, self-assess and report on their cyber maturity to the Scottish Government on an annual basis.

3.3 All public bodies put in place appropriate and regular independent assurance of their critical technical security controls, such as through the Cyber Essentials Plus scheme.

3.4 All public bodies secure their supply chains, building in appropriate cyber assurance as part of their procurement practices, contract management and grant making processes.

3.5 The Scottish Government reviews the Scottish Public Sector Cyber Resilience Framework every three years to ensure relevance in light of changing technologies, risks, threats, regulations and standards.

4. Public sector organisations improve their staff’s cyber resilient behaviours

4.1 All public bodies provide appropriate and relevant cyber resilience training and awareness-raising for staff at all levels of the organisation.

5. Public sector organisations increase opportunities for professional development of their IT and cyber security staff

5.1 All public bodies promote and encourage development opportunities for their cyber security workforce, including:

- ensuring that development opportunities are inclusive

- ensuring that cyber security upskilling and reskilling opportunities are available whenever possible, including the uptake of cyber security apprenticeships
- promoting the adoption of best practice and cyber security professional standards

6. **Public sector organisations are prepared for, and can effectively respond to and recover from, cyber incidents**

6.1 All public bodies have effective cyber incident response plans in place and test them at least annually.

6.2 All public bodies exercise against the most common cyber attack scenarios at a technical, operational and strategic level.

6.3 The Scottish Government supports public bodies to build their exercising capabilities.

6.4 All public bodies use the Scottish Public Sector Cyber Incident Notification Process, where appropriate.

6.5 All public bodies implement NCSC's Active Cyber Defence Measures (where eligible), including:

- Early Warning
- Mail Check
- Web Check
- Protective Domain Name Service (PDNS)

7. **The Scottish Government ensures national cyber incident response arrangements are effective**

7.1 The Scottish Cyber Coordination Centre works with its national partners to conduct an annual national cyber exercise which ensures effective cross-agency coordination.

7.2 The Scottish Cyber Coordination Centre reviews national cyber incident and vulnerability coordination arrangements at least annually, and after all significant events.

7.3 The Scottish Cyber Coordination Centre reviews and shares lessons identified from exercises and from significant cyber incidents which have value to the wider public sector.