Agenda item 13

Committee report

Digital controls review of cyber resilience arrangements

Committee Audit and Standards

Date of meeting 9 February 2018 **Date of report** 26 January 2018

Report by Assistant Chief Executive (Business Support)

1. Object of report

To advise the committee on the findings of a digital controls review of cyber resilience arrangements. This engagement is included in the annual Internal Audit plan for 2017/18.

2. Background

Cyber resilience means being able to prepare for, withstand, and rapidly recover and learn from deliberate attacks (or accidental events) that have a disruptive effect on interconnected technologies. By building understanding of cyber risks and threats, SPT will be able to take appropriate measures to stay safe online.

On 8 November 2017, the Scottish Government issued *'Safe, secure and prosperous: a cyber-resilience strategy for Scotland; public sector action plan 2017/18'*, which states:

'this Public Sector Action Plan has been developed in partnership by the Scottish Government and the National Cyber Resilience Leaders' Board (NCRLB). It sets out the key actions that the Scottish Government, public bodies and key partners will take up to the end of 2018 to further enhance cyber resilience in Scotland's public sector. While there are already strong foundations in place, its aim is to ensure that Scotland's public bodies work towards becoming exemplars in respect of cyber resilience, and are well on their way to achieving this by the end of 2018.'

The strategy document can be found at Appendix 1.

The objective of this engagement was to review cyber resilience arrangements in accordance with the Scottish Government action plan.

Note: as at the date of engagement testing (November 2017) further guidance was awaited from the Scottish Government on central cyber incident reporting and coordination protocols, template(s) for cyber incident response plans, and core training and awareness raising approach, materials, etc. for use by the public sector, as part of wider security training and awareness raising package.

This engagement tested elements of the internal controls and mitigation against SPT 7: Prolonged IT failure and SPT 22: Governance arrangements, as identified in the corporate risk register.

3. Outline of findings

Engagement testing found that good progress has been made to implement the actions outlined by the Scottish Government for cyber resilience.

SPT will seek to achieve cyber essentials plus (CE+) certification by mid-2018.

The engagement identified a requirement to review current arrangements to ensure compliance and adherence with the timelines set in the Scottish Government Cyber Resilience Public Sector Action Plan.

There are areas for improvement, and these areas have been addressed by one recommendation. Digital management have agreed to implement the recommendation, which is currently being actioned.

4. Conclusions

The Audit and Assurance team has undertaken a digital controls review of cyber resilience arrangements. One recommendation has been agreed from this engagement.

Key controls exist and are applied consistently and effectively in the majority of areas tested in this engagement.

Reasonable assurance can be taken from the controls in place for the areas covered in this engagement.

5. Committee action

The committee is asked to note the contents of this report and agree that the Audit and Assurance Manager submits a follow-up report on the implementation of the recommendation to a future meeting.

6. Consequences

Policy consequences	*None*
Legal consequences	*None*
Financial consequences	*None*
Personnel consequences	*None*
Social Inclusion consequences	*None*
Risk consequences	*As detailed in the report*

Name	Valerie Davidson	**Name**	Gordon Maclennan
Title	**Assistant Chief Executive (Business Support)**	**Title**	**Chief Executive**

For further information, please contact Iain McNicol, Audit and Assurance Manager on 0141 333 3195.

www.gov.scot/cyberresilience

Scottish Government
Riaghaltas na h-Alba
gov.scot

SAFE, SECURE AND PROSPEROUS: A CYBER RESILIENCE STRATEGY FOR SCOTLAND

PUBLIC SECTOR ACTION PLAN 2017-18

PUBLIC SECTOR ACTION PLAN ON CYBER RESILIENCE – JOINT FOREWORD

DIGITAL TECHNOLOGY OFFERS HUGE OPPORTUNITIES FOR SCOTLAND AS A MODERN, PROGRESSIVE NATION.

Whether in the public, private or third sectors, our ability to inform and interact with citizens and consumers is being transformed by the digital world. Scottish public bodies, businesses and charities are developing ambitious plans to embrace these opportunities.

Trust and confidence are fundamental to the success of these plans. As the threat from cyber criminals and other hostile actors in cyberspace grows, we must do all we can to ensure our digital services are as secure as possible, and can recover quickly when cyber-attacks succeed.

The ambition of the Scottish Government and the National Cyber Resilience Leaders' Board is for Scotland to be a world leading nation in cyber resilience.

We start from solid foundations. Scotland's cyber resilience strategy, Safe, Secure and Prosperous, provides an ambitious framework for action. Many organisations in Scotland's public, private and third sectors have already prioritised putting in place sound cyber security measures. But we are realistic about the need for further, concrete actions to help achieve our ambition.

The Programme for Government sets out a commitment to develop a suite of action plans to help move Scotland as a whole towards greater cyber resilience. The overall aim of those action plans will be to develop a culture in which our nation's cyber resilience is, rightly, seen as everyone's business – from the smallest micro business or charity, to the largest, most complex public and private sector organisations.

This Public Sector Action Plan, developed jointly by the Scottish Government and the National Cyber Resilience Leaders' Board, represents an initial, significant step towards establishing that wider culture of cyber resilience in Scotland.

While many Scottish public bodies already have sound standards of cyber security in place, our aim is for the Scottish public sector as a whole to become an exemplar in this field over time.

By undertaking the actions set out in this plan, Scottish public bodies will be committing to implementing a common approach to cyber resilience, offering greater assurance to those who make use of our digital public services.

Further, complementary action plans, developed in partnership with the Scottish private and third sectors, will follow.

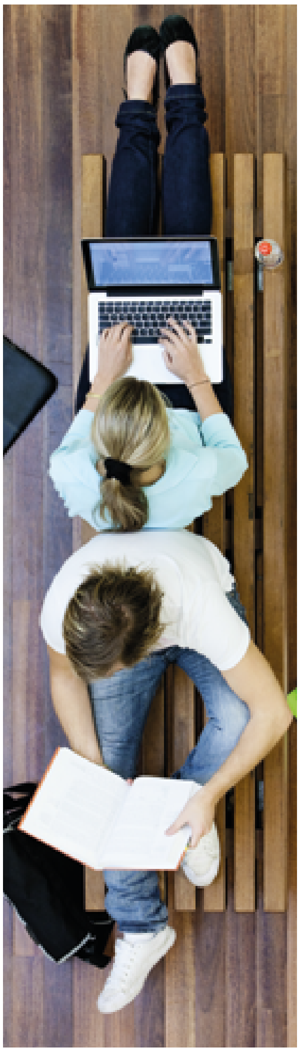
We look forward to continuing to work together with partners across Scotland, the UK and internationally to realise our goal of being a world leading nation in cyber resilience.

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

Hugh Aitken
Chair, NCRLB

CONTENTS

EXECUTIVE SUMMARY



EXECUTIVE SUMMARY

1. The importance of cyber resilience in Scotland's public bodies has never been greater. Digital technologies bring enormous opportunities for Scottish public services – but they also bring with them new threats and vulnerabilities that we must take decisive action to manage.

2. This Public Sector Action Plan has been developed in partnership by the Scottish Government and the National Cyber Resilience Leaders' Board (NCRLB). It sets out the key actions that the Scottish Government, public bodies and key partners will take up to the end of 2018 to further enhance cyber resilience in Scotland's public sector. While there are already strong foundations in place, its aim is to ensure that Scotland's public bodies work towards becoming exemplars in respect of cyber resilience, and are well on their way to achieving this by the end of 2018.

3. The action plan focuses on public bodies. Delivery of the action plan will be coordinated and led by the Scottish Government's Cyber Resilience Unit, working in partnership with the NCRLB and Scottish public bodies. Wherever possible, the Scottish Government will work with key partners in the wider public sector, including local authorities, and universities and colleges, to promote an aligned approach to work on cyber resilience.

KEY ACTIONS

A. Developing a common approach to cyber resilience in Scottish public bodies

4. **Key Action 1:** The Scottish Government will work with the NCRLB, the National Cyber Security Centre (NCSC), the Scottish Public Sector Cyber Catalysts[1] and other key partners to develop a Cyber Resilience Framework for Scottish public bodies by end June 2018. This framework, with associated guidelines and requirements, will help promote a common, effective, risk-based approach to cyber resilience across Scottish public bodies. A high-level concept framework can be found at Annex B.

B. Initial baseline cyber resilience requirements for Scottish public bodies

5. The Scottish Government has worked with the NCRLB to identify the requirements that will form the "initial baseline progression stage" under the Scottish Public Sector Cyber Resilience Framework. The Scottish Government will ask public bodies to achieve the following requirements to the following timelines:

- **Key Action 2:** Have in place minimum cyber risk governance arrangements, by end June 2018.
- **Key Action 3:** Ensure that public bodies that manage their own networks become active members of the NCSC's Cybersecurity Information Sharing Partnership (CiSP), in order to promote sharing of cyber threat intelligence, by end June 2018.

[1] See Key Action 10 in the action plan.

- **Key Action 4:** Ensure they have in place appropriate independent assurance of critical cyber security controls by end October 2018. To support this goal, funding will be made available for public bodies to undergo Cyber Essentials "pre-assessments", by end March 2018.

- **Key Action 5:** Implement as appropriate the NCSC's Active Cyber Defence Programme, which aims to make internet-based products and services safer to use, by end June 2018.

- **Key Action 6:** Have in place appropriate cyber resilience training and awareness-raising arrangements for individuals at all levels of the organisation, by end June 2018.

- **Key Action 7:** Have in place appropriate cyber incident response plans as part of wider response arrangements, and ensure these align with central incident reporting and coordination mechanisms, by end June 2018.

C. Cyber security of supply chain and grant recipients

6. **Key Action 8:** Supply chain cyber security arrangements will form a key part of the Scottish Public Sector Cyber Resilience Framework. As part of due diligence, it makes good sense to ensure that other recipients of public money, such as grant recipients, also demonstrate that they take cyber security seriously. As part of work to develop the Framework, the Scottish Government will:

- develop a proportionate, risk-based policy in respect of supply chain cyber security (aligned appropriately with GDPR requirements), to be applied by public bodies in all relevant procurement processes. Industry partners will be consulted on a draft policy early in 2018, with a view to it forming part of the Scottish Public Sector Cyber Resilience Framework.

- develop guidance on the need for recipients of public grant funding to have in place appropriate, proportionate and risk-based cyber security arrangements. These requirements will align with the new supply chain policy and take effect alongside them.

D. Ensuring Scottish public bodies can access cyber security expertise and support

7. **Key Action 9:** To ensure that Scottish public bodies can access appropriate expertise in support of their work on cyber resilience, the Scottish Government will put in place an innovative Dynamic Purchasing System for Digital Services (including cyber security), by end October 2017.

E. Leadership and knowledge sharing

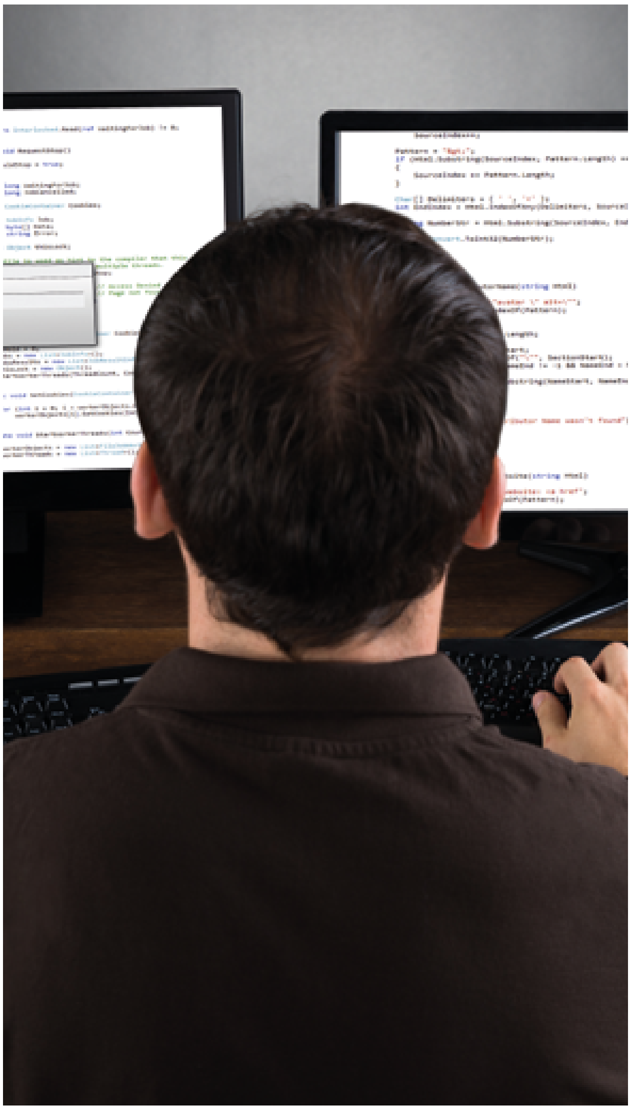
8. **Key Action 10:** To promote leadership and knowledge sharing, the Scottish Government will coordinate a Public Sector Cyber Catalyst scheme, under which a number of leadership bodies will commit to work towards becoming exemplars in respect of cyber resilience, helping identify common issues and solutions, and sharing learning and knowledge with the wider public sector.

F. Monitoring and Evaluation

9. **Key Action 11:** The Scottish Government will put in place a monitoring and evaluation framework to assess progress against this action plan and, once finalised, the Cyber Resilience Framework.

A summary of the key actions different bodies should take, along with timelines, can be found at Annex A to this action plan.

INTRODUCTION AND BACKGROUND



1

1. INTRODUCTION AND BACKGROUND

10. **Safe, secure and prosperous: a cyber resilience strategy for Scotland**[2], was published in 2015. It set out the Scottish Government's vision for Cyber Resilience in Scotland:

> ***Scotland can be a world leader in cyber resilience and be a nation that can claim, by 2020, to have achieved the following outcomes:***
>
> ***(i) Our people are informed and prepared to make the most of digital technologies safely.***
>
> ***(ii) Our businesses and organisations recognise the risks in the digital world and are well prepared to manage them.***
>
> ***(iii) We have confidence in, and trust, our digital public services.***
>
> ***(iv) We have a growing and renowned cyber resilience research community.***
>
> ***(v) We have a global reputation for being a secure place to live and learn, and to set up and invest in business.***
>
> ***(vi) We have an innovative cyber security goods and services industry that can help meet global demand.***

These outcomes are interdependent – progress towards one may underpin or drive progress towards others.

11. "Safe, secure and prosperous" is closely aligned with the **UK National Cyber Security Strategy**[3], which sets out the UK Government's strategic approach to making the UK secure and resilient in cyberspace. Cyber security is a reserved matter, but it has strong implications for the delivery and resilience of devolved services – as such, the Scottish Government works closely with key partners such as the UK National Cyber Security Centre to ensure appropriate alignment between work on cyber resilience at the UK and Scottish levels.

12. This action plan has been developed in partnership by the Scottish Government and the National Cyber Resilience Leaders' Board (NCRLB). It sets out the action the Scottish Government intends to take, working closely with the NCRLB and its partners in the wider Scottish public sector, in order to make progress during 2017-18 towards outcome (iii) above:

We have confidence in, and trust, our digital public services.

This outcome aligns closely with the outcome set out in Scotland's Serious Organised Crime Strategy[4] for Scotland's public sector organisations to protect themselves from cyber threats.

[2] http://www.gov.scot/Publications/2015/11/2023

[3] https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

[4] http://www.gov.scot/Resource/0047/00479632.pdf

13. The immediate focus of the action plan is on Scotland's public bodies[5] – timelines and monitoring requirements will apply to them as set out under the key actions in this document. The Scottish Government will also seek to work constructively with areas such as local government and the universities and colleges sector, in order to align action on cyber resilience across the wider public sector wherever possible, and facilitate the spread of good practice.

14. Work is also being taken forward by the Scottish Government, the NCRLB, and partners in the **private and third** sectors to make progress towards our strategic outcomes. The NCRLB is of the view that providing strong leadership on cyber resilience in the public sector will assist in raising awareness and activity in the private and third sectors. Every effort will be made to align the approach taken in the public sector with the approach taken in the private and third sectors.

15. This action plan will form part of wider work on improving the overall security and resilience of Scotland's public sector, including in respect of **Critical Infrastructure**. While a specific focus on cyber resilience is appropriate at this stage in view of the urgency of the cyber threat, our intention is that the actions set out in this plan should in due course form an integral part of coherent wider security and resilience arrangements, including in respect of **physical** and **personnel** security – both of which are key to cyber resilience.

16. While the focus of this action plan is on cyber resilience, the actions set out in this plan will also help ensure that Scottish public bodies are meeting key requirements in respect of **protecting personal data**, which will be strengthened by the General Data Protection Regulation (GDPR)[6] from May 2018. The Information Commissioner has, for example, noted publicly that achieving Cyber Essentials accreditation can assist with preparing for GDPR. Public bodies should consider how work on cyber resilience aligns with their wider work on GDPR compliance.

The importance of cyber resilience to Scotland's public bodies

17. "Cyber resilience" means being able to prepare for, withstand, and rapidly recover and learn from deliberate attacks (or accidental events) that have a disruptive effect on interconnected technologies. Cyber security is a key element of being resilient, but cyber resilient people and organisations recognise that being safe online goes far beyond just technical measures. By building understanding of cyber risks and threats, they are able to take the appropriate measures to stay safe and get the most from being online.

[5] An accompanying implementation toolkit, available at www.gov.scot/cyberresilience, provides further detail on the applicability of this plan to public bodies. Arrangements in respect of **Scottish health boards** and **Scottish Water** must align with the requirements of the new EU NIS Directive as implemented at UK level, details of which are still being developed. As these requirements become clearer in early 2018, the Scottish Government Cyber Resilience Unit will work closely with the new Competent Authority/ies set up under the NIS Directive to consider how best to apply this action plan to the health and water sectors.

[6] https://ico.org.uk/for-organisations/data-protection-reform/

18. The importance of ensuring cyber resilience in Scotland's public bodies has never been greater, because of:

(i) The scale and nature of the cyber threat, and the risks it presents to our ambitions for Scotland's digital public services and our overall security and resilience: Scotland's refreshed digital strategy[7] makes clear that digital connectivity offers huge opportunities to redefine the relationship between Scottish public bodies and the people they serve. The Scottish Government is committed to establishing all new government organisations as digital businesses, designed around the needs of their users, in order to benefit from these new technologies. But with these opportunities come new threats and vulnerabilities. If we are to realise the enormous opportunities technology offers to our citizens, businesses, and public services, we must develop our understanding of the new risks the digital environment presents – and respond in an **effective**, **coherent** and **proportionate** way across all of Scotland's public bodies.

The global cyber-attack on 12 May 2017, which affected more than 150 countries worldwide and had an impact on some areas of the NHS in Scotland and England, underlined the potential seriousness of the cyber threat. The NCSC assesses that the number and severity of cyber incidents affecting public (and private) sector organisations will continue to increase. These threats come from a variety of sources, including hostile state actors, cyber criminals, political activists and others.

(ii) Forthcoming legislative changes and their potential legal, financial and reputational impact: The new General Data Protection Regulation (GDPR) and the Security of Network and Information Systems (NIS) Directive both come into force in May 2018, and place new duties on public (and private and third) sector organisations to ensure the protection of personal data, and the continuity of essential services reliant on network and information systems, and to report cyber security breaches. Public sector organisations could face significantly increased administrative fines of up to €20 million for data breaches and/or cyber security failures leading to service failure. The UK Government has indicated its intention to implement GDPR and the NIS Directive in full.

(iii) Economic opportunity: There is a significant opportunity for Scotland to leverage work on cyber resilience in the public, private and third sectors to promote **economic growth**. The Scottish Government's goal is to ensure that the demand created by an enhanced focus on cyber resilience, along with the wider reputational benefits of ensuring cyber resilient organisations, results in the growth of a world-leading **cyber security goods and services sector** in Scotland, with benefits for inward investment and exporting.

[7] http://www.gov.scot/Resource/0051/00515583.pdf

19. Scottish Ministers have made clear their expectation that Scottish public bodies will play a **leadership role** in driving forward higher standards of cyber resilience in Scotland. Whether provided by central or local government, executive agencies, non-departmental public bodies (NDPBs), emergency services, NHSScotland, our education sector, or other public bodies, it is crucial that our citizens, businesses and organisations have confidence in, and can trust digital public services.

20. The NCRLB has articulated its view that, in time, cyber resilience should be "baked into" Scottish public sector processes and infrastructure. It emphasises that cyber resilience is as much a **cultural** issue as a technical one. They view it as vital that Scotland's public bodies understand and manage the cyber threat at Board/Senior Management level, and take action to promote a culture of cyber security at all levels of the organisation. Coherent action is required across organisations in both the technical and personnel domains to ensure a genuinely effective response to the cyber threat.

Current levels of cyber resilience in Scotland's public sector

21. A strong strategic framework for action across all sectors already exists in the form of Scotland's Cyber Resilience Strategy ("Safe, Secure and Prosperous"). In the public sector, many bodies are already taking forward work to improve their cyber resilience, with reference to a range of existing standards, guidelines and controls. These include:

- The Public Service Network (PSN) Connection Obligations
- The Public Service Network in Policing (PSNP) Obligations
- The NHS Security Policy Framework (aligned to ISO 27001 and the SANS Top 20 critical controls)
- The UK Government Security Policy Framework
- Cyber Essentials (Plus)
- The 10 Steps to Cyber Security
- ISO 27001
- Payment Card Industry Data Security Standard (PCI DSS) accreditation

22. The overall picture of cyber resilience across the Scottish public sector remains unclear, partly as a result of a complex and confusing landscape of different standards and guidelines that public bodies are operating to.

23. Important work is underway to improve our understanding of the picture in respect of Critical National Infrastructure in the Government Sector. Work to develop this action plan has also provided further assurance that many Scottish public sector organisations have a range of robust measures in place to protect against cyber risks. It is clear that some public bodies have complex IT infrastructures that include legacy systems, and an effective approach to managing the risk presented by these arrangements is required. Given the pace of technological development in this area, it is important that Scottish public bodies are monitoring, and can respond to, future cyber threats, including in areas such as the Internet of Things (IoT).

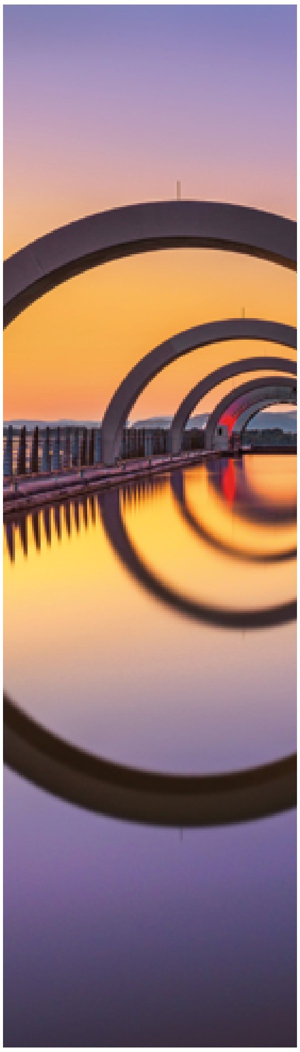
24. There is currently a lack of guidance making clear the minimum standards of cyber resilience that all Scottish public bodies should strive for. Nor is there any well-defined monitoring and reporting framework to allow Scottish Ministers, the NCRLB and the Scottish Parliament to secure a clear picture of cyber resilience across the Scottish public sector. Unless we address this, measuring progress and providing assurance to citizens and businesses will be challenging, with the potential for knock-on consequences for our public services and our digital economy.

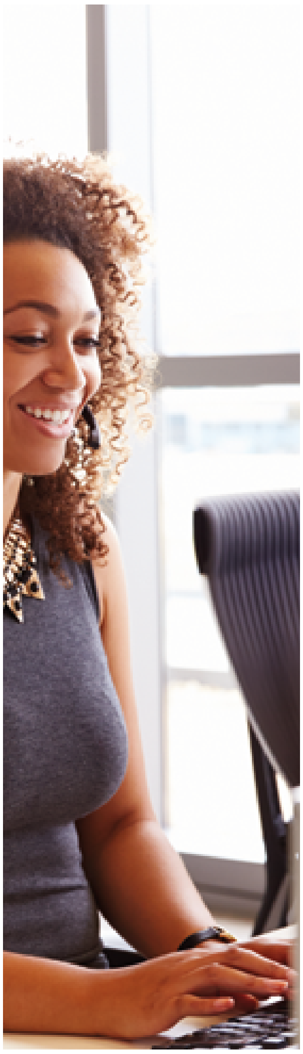
The goals of this action plan

25. This action plan aims to ensure that:

- Scottish public bodies work to become **exemplars** in respect of cyber resilience, and play a leadership role in driving higher standards of cyber resilience in Scotland and further afield.
- A **common, effective, risk-based approach** to cyber resilience is in place across all Scottish public bodies, providing appropriate **assurance** to Ministers, Parliament, and the public.
- The public sector sends **strong messages to the private and third sectors about the importance of cyber resilience**, and supports the **economic opportunity** that work on cyber resilience brings.

KEY ACTIONS





2

2. KEY ACTIONS

Introduction

26. This Action Plan sets out the key actions that the Scottish Government and its partners will take during 2017-18 to help address these issues and ensure confidence in standards of cyber resilience in Scotland's public bodies.

27. The Scottish Government is clear that, within the public sector, it must **lead by example** on cyber resilience. It views cyber resilience as a fundamental requirement and an enabler in a digital world. It acknowledges that it must work to ensure the highest standards of cyber resilience are in place in its own organisation, and it is committed to undertaking this work at pace during 2017-18 and sharing learning with others.

28. The Scottish Government is also clear that it cannot achieve a strong, cyber resilient public sector in Scotland on its own. This will require **all Scottish public bodies**, and the wider public sector, to take responsibility for resourcing and implementing priority actions to develop their own cyber resilience, while drawing on available support and expertise from the wider private and public sectors. The Scottish Government stands ready to offer support and advice to public bodies, and share learning to assist them in their journey towards enhanced cyber resilience. Some specific aspects of this support are outlined in this action plan – other potential areas of support will be identified in further discussion with public bodies. As work is taken forward to drive higher levels of cyber resilience in Scotland's private and third sectors, potential links or opportunities for cross-sectoral knowledge-sharing and support will also be identified.

29. Delivery of the action plan will be coordinated and led by the Scottish Government's Cyber Resilience Unit, working in partnership with the NCRLB, other key parts of the Scottish Government, Scottish public bodies and the UK Government's National Cyber Security Centre.

30. Our intention is for this action plan to be **adaptable** to ever-changing circumstances. The cyber security landscape continues to evolve at pace. If changed circumstances dictate that amendments to some of the key actions outlined in this action plan are required after its publication, the Scottish Government will work closely with the NCRLB and Scottish public bodies to adapt our approach and ensure we are pursuing the best outcomes in support of Scotland's cyber resilience.

31. Action to promote cyber resilience in Scotland's public bodies will of course continue beyond 2018. This action plan will then be refreshed, to take stock of progress to date and ensure continued progress.

Collaborative working, levers and influence

32. One of the goals of this action plan is to address a lack of consistency, and ensure a **common approach** to cyber resilience across all Scottish public bodies. Among other things, this will be key to providing effective assurance to Ministers, Parliament and the public about the levels of cyber resilience across Scotland's public bodies.

33. To achieve this the Scottish Government will seek to work collaboratively with public bodies to ensure implementation of this action plan. We will also make full use of available levers and influence in order to achieve the plan's goals. In particular, the Scottish Government will pursue the following approaches in respect of public bodies:

- Scottish Ministers will **write to the Chief Executives of all Scottish public bodies**, asking them to take action in line with the timescales set out in this action plan to ensure they are cyber resilient.
- In view of the increasing importance of cyber resilience to protecting assets acquired with public money, the **Scottish Public Finance Manual (SPFM)** and its associated guidance on Governance Statements and Certificates of Assurance processes will be updated at appropriate points in time to clarify how the requirements developed under this action plan apply to bodies subject to the SPFM. All such public bodies will then be required to provide assurance, via the Governance Statement and Certificates of Assurance process, that they are adopting the practice set out in this action plan.
- Where appropriate and necessary, key requirements set out in this action plan will also be incorporated into relevant **guidance**, **framework documents**, **memoranda of understanding**, **budget allocation and monitoring letters**, **letters of strategic guidance** and **chairs' appraisals** as far as they apply to certain public bodies.

34. The Scottish Government will also seek commitments from other Scottish public sector organisations and representative bodies to work collaboratively on a programme of activity that aligns with this action plan. While it is possible that not all of the recommendations set out in this action plan will be appropriate for these more diverse areas of the public sector, our discussions with the wider sector suggest a strong appetite for alignment wherever possible. In pursuing this, the Scottish Government will work closely with key bodies and influencers in the following areas:

Local authorities

- The Scottish Government recognises that local authorities face particular challenges in respect of the complexity of their networks and requirements that, for example, schools have to maintain an open digital learning environment. The Scottish Government will work closely with key partners including COSLA, SOLACE, the Scottish Local Authority Information Security Group and the Local Authority Digital Office to align work at the local authority level with this action plan wherever possible.
- £100,000 has been made available under the UK Cyber Security Funding Programme to support the appointment of a Chief Information Security Officer (CISO) to the Scottish Local Government Digital Office, who will lead on the development of a programme of cyber security support for local authorities that is aligned with this action plan.

Universities and colleges

- The Scottish Government recognises that universities and colleges face particular challenges in maintaining a vibrant research and learning environment that draws on the opportunities of digital technologies whilst ensuring appropriate levels of cyber security. It also notes the status of universities as independent charities. The Scottish Government will seek to work closely with key bodies including Universities Scotland, Colleges Scotland, Higher Education Information Directors for Scotland (HEIDS) and Universities and Colleges Shared Services (UCSS) to align the scope of cyber security work in Scotland's universities and colleges with this action plan.

35. The accompanying toolkit[8] provides further information about the applicability of this action plan and the approach that will be taken by the Scottish Government and public bodies delivering on its aims.

KEY ACTIONS

A. Developing a common approach to Cyber Resilience across the Scottish public sector

Key Action 1

The Scottish Government will work with the NCRLB, the NCSC, the Scottish Public Sector Cyber Catalysts[9] and other key partners to develop a Cyber Resilience Framework for Scottish public bodies by end June 2018.

This framework, with associated guidelines and requirements, will help promote a common, effective, risk-based approach to cyber resilience across Scottish public bodies.

36. As noted above, Scottish public bodies currently operate to a wide range of standards, requirements and guidelines in respect of cyber resilience, with variations in applicability and coverage. In addition, at the time of writing new requirements are being developed that will add to the complexity of this landscape. These issues are not unique to the Scottish public sector – they are evident in all sectors across the UK and beyond.

37. The UK Government will introduce legislation early in 2018 to implement the NIS Directive by **May 2018**. Only some key devolved Scottish public bodies are expected to be subject to the NIS Directive – particularly those in the health and water sectors. The UK Government has, at the time of writing, published the **High Level Cyber Security Principles**[10] that these bodies will be required to adopt. More detailed guidance on what action will be required to ensure compliance with the NIS Directive, along with a self-assessment framework, is expected to be published by the UK Government in 2018.

[8] Available at: www.gov.scot/cyberresilience

[9] See Key Action 10.

[10] https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive – see p.38

38. The UK Government has also indicated its intention to introduce a new mandatory Technology Security Standard under the Security Policy Framework (SPF) before the end of 2017. The SPF applies primarily to the UK Government and its departments and agencies, but public bodies are encouraged to have reference to it. The Scottish Government has to date aligned its approach to security with the SPF. This new cyber security standard will, once implemented, establish a baseline level of cyber security across UK Government departments and their arm's length bodies.

39. The landscape of cyber resilience standards, guidelines and requirements that will apply to, or be influential with, Scottish public bodies in the immediate future is therefore **evolving**. Any effort to develop a common cyber resilience framework for all Scottish public bodies must take account of this uncertainty and provide clarity with regard to the relevance of existing standards and guidelines.

40. To address these issues the Scottish Government will work with the NCRLB, the NCSC, the Scottish Public Sector Cyber Catalysts[11] and other key partners to develop and disseminate a **Cyber Resilience Framework** for Scottish public bodies by end **June 2018**.

41. The Framework will aim to:

- Provide a **common, effective approach** for Scottish public bodies to **assess their levels of cyber resilience**, ensure they adhere to **minimum cyber resilience requirements**, and **progress** towards achieving higher levels of cyber resilience on a risk-based and proportionate basis.
- Align with the new **NIS Directive legislation and guidance** and **other key measures,**[12] to ensure consistency with forthcoming developments. Clarity on the key requirements of these initiatives is expected to have been achieved by **early in 2018.**[13]
- Take account of **foreseeable technological developments**, such as a move to greater reliance on cloud systems and the further development of Smart City technologies and the "Internet of Things".
- As far as possible, **minimise any additional burdens** on Scottish public bodies, including by making clear **how the Framework relates to existing standards or requirements**, and taking account of these when providing guidance on compliance. Wherever possible, the Scottish Government will work closely with the UK Government to promote rationalisation and alignment of different standards, although this will take time to achieve.
- Help to provide **clarity and assurance** to individual organisations, Ministers, the Scottish Parliament and the public that appropriate levels of cyber resilience are in place across Scottish public bodies. Appropriate **monitoring and evaluation arrangements** will be put in place to align with the Framework (see Key Action 11). These arrangements will ensure alignment with, and support for, existing arrangements in respect of Critical Infrastructure. Consideration will be given to clarifying appropriate penetration testing and audit requirements under the framework, and aligning these with existing requirements such as PSN accreditation.
- Seek to align with a similar framework/hierarchy under development as part of work on **private and third sector action plans on cyber resilience** by the Scottish Government and the NCRLB.

[11] See Key Action 10.

[12] Including the new Technology Security Standard under the Security Policy Framework and the GDPR.

[13] Alignment with wider, non-cyber security focused requirements under the Security Policy Framework will also be taken into consideration where appropriate.

42. While completion of the Scottish Public Sector Cyber Resilience Framework will not be possible until clarity is achieved on the contents of the legislation implementing the EU NIS Directive, work has begun on its development.

43. It is expected that the Scottish Public Sector Cyber Resilience Framework will take as its starting point the new **NIS Directive** legislation and guidance (which itself draws on existing frameworks such as the NIST Cyber Security Framework). Subject to the final shape of the legislation implementing the NIS Directive, the Scottish Public Sector Cyber Resilience Framework is expected to cover **4 key domains** of cyber resilience (Identify, Protect, Detect and Respond and Recover), and have **3 progression stages.** These are expected to consist of an "**initial baseline**" stage, a "**target**" stage (which all public bodies will be expected to work towards on a risk-based and proportionate basis) and an "**advanced**" stage (which will align with the requirements of the EU NIS Directive and apply automatically to public bodies in health and water – other key public bodies may also be encouraged to work towards these more advanced requirements).

44. An initial outline of **a high-level concept framework** is at **Annex B** to this action plan. This incorporates some **initial baseline cyber security requirements** that all Scottish bodies will be encouraged to begin work on immediately, with a view to meeting the majority of them as a minimum by **end June 2018**[14]. It is expected that the majority of Scottish public bodies will already in effect be meeting these requirements. However, the requirements set out under the initial baseline stage will provide clarity and assurance that this is the case.

45. Once completed, in view of its importance to protecting assets acquired with public money, the Scottish Public Finance Manual (SPFM) and its associated guidance on Certificates of Assurance processes will be updated to reflect the requirements of the Framework. In line with the accountability processes set out in the SPFM, public bodies subject to the SPFM that do not comply with the relevant standards and guidelines (e.g. for reasons of proportionality or on the basis of their assessment of risk) will be expected to provide reasons for this.

46. Pending finalisation of the Scottish Public Sector Cyber Resilience Framework, Scottish public bodies that are not currently working to advanced guidelines or standards may wish to refer to the NCSC's **10 Steps to Cyber Security**[15] for further guidance on how to ensure their organisational cyber resilience.

[14] With the requirement for Cyber Essentials certification or, exceptionally, alternative independent assurance of critical controls by end October 2018.

[15] https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

B. Initial baseline cyber resilience requirements for Scottish public bodies

47. The Scottish Government has already worked with the NCRLB to identify the **initial baseline cyber resilience requirements** that will form part of the Scottish Public Sector Cyber Resilience Framework. These initial baseline requirements are expected to provide a **strong foundation** for work to achieve the "target" and "advanced" progression stages of the Framework for Scottish public bodies.

(i) Identify (Governance and Risk-Management)

48. Under the **"Identify"** domain at the **initial baseline progression stage**, the following requirements will apply.

Key Action 2

The Scottish Government will seek assurances from all Scottish public bodies that they have in place a Board/Senior Management commitment to manage the risks arising from the cyber threat.

As part of this, Scottish public bodies will be asked to ensure they have minimum appropriate governance arrangements in place by end June 2018.

49. It is vital that the cyber threat is seen as a **business risk**, one of many that need to be managed on a daily basis by all public bodies. Only by ensuring senior-level focus on managing these risks, and devoting appropriate time and resource to doing so, will cyber resilience be mainstreamed into Scottish public bodies.

50. The Scottish Government will therefore seek assurances from all Scottish public bodies that they have in place a **Board/Senior Management commitment** to manage the risks arising from the cyber threat.

51. As part of this, Scottish public bodies will be asked to ensure they have the following minimum appropriate governance arrangements in place by **end June 2018**:

- A **named Board/Senior Management member** identified as responsible for organisational cyber resilience arrangements, with clear lines of responsibility and accountability for the cyber resilience of sensitive information and key operational services.
- **Regular Board/Senior Management-level consideration** of the cyber threat and the arrangements the organisation has in place to manage risks arising from it, with appropriate management policies and processes in place to direct the organisation's overall approach to cyber resilience.

52. Further practical advice on what the effects of these arrangements should be can be found in the accompanying implementation toolkit.[16] Pending finalisation of the Scottish Public Sector Cyber Resilience Framework, Scottish public bodies may wish to refer to the **10 Steps to Cyber Security** for further guidance on some of the key questions Boards/Senior Management may wish to address in respect of organisational cyber security and how to establish an effective risk management regime.[17]

Key Action 3

To promote greater awareness of cyber threat intelligence across the Scottish public sector, the Scottish Government will encourage Scottish public bodies who are responsible for managing their own networks to become active participants in the Cyber Security Information Sharing Partnership (CiSP) by end June 2018.

53. Many public bodies in Scotland have responsibility for managing their own networks. In order to respond to emerging cyber threats and implement effective policies and actions to manage risk, it is vital that they have access to intelligence about cyber threats.

54. The National Cyber Security Centre hosts a secure threat intelligence sharing extranet known as the **Cyber Security Information Sharing Partnership (CiSP)**. CiSP is specifically designed to enable its membership to gather and share cyber threat intelligence and good practice, in order to enable swift mitigation of emerging cyber threats. This is a free resource for network defenders, and the Scottish Government will make use of the levers and influence available to it to ensure that Scottish public bodies who manage their own networks become members.[18]

55. Scotland has its own community group within the CiSP called the **Scottish Cyber Information Network (SCiNET)** and Scottish public bodies and businesses within the CiSP are encouraged to engage in this community group. Key update documents such as the Napier Meridian Cyber Weekly for Scotland, funded under the UK Cyber Security Programme for Scotland, are made available through SCiNET. The Scottish Local Authority Information Security Group (SLAISG) actively supports and encourages the use of the CiSP platform within the public sector and has established its own dedicated subgroup for cross-agency collaboration.

56. The accompanying **toolkit**[19] provides further information on how Scottish public sector organisations can become members of the CiSP.

[16] Available at www.gov.scot/cyberresilience

[17] https://www.ncsc.gov.uk/guidance/10-steps-information-risk-management-regime

[18] Eligibility rules may exclude certain regulatory bodies.

[19] Available at www.gov.scot/cyberresilience

(ii) Protect

57. Under the **"Protect"** domain at the **initial baseline progression stage**, the following requirements will apply.

Key Action 4

The Scottish Government will support Scottish public bodies to ensure they have in place appropriate independent assurance that critical technical controls are in place to protect against the most common internet-borne threats by end October 2018.

Funding will be made available to support all public bodies to undergo a Cyber Essentials "pre-assessment" by end March 2018, with a view to: a) promoting a common approach wherever possible, and b) ensuring well-founded senior-level decisions on the most appropriate way of achieving assurance that critical controls are in place.

58. The NCSC advises that the most common internet borne threats are not targeted, are opportunistic in nature, and can be prevented by implementing basic, cost-effective cyber security measures. They recommend the adoption, **as a minimum**, of five critical network controls:

(i) Boundary firewalls and internet gateways – information, applications and computers within the organisation's internal networks should be protected against unauthorised access and disclosure from the internet, using boundary firewalls, internet gateways or equivalent network devices.

(ii) Secure configuration – computers and network devices should be configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

(iii) Access control – user accounts, particularly those with special access privileges (e.g. administrative accounts) should be assigned only to authorised individuals, managed effectively and provide the minimum level of access to applications, computers and networks.

(iv) Malware protection – Computers that are exposed to the internet should be protected against malware infection through the use of malware protection software.

(v) Patch management – Software running on computers and network devices should be kept up-to-date and have the latest security patches installed.

59. There is a range of ways of achieving independent assurance that these critical controls are in place. One widely available certification scheme is **Cyber Essentials,**[20] which offers a mechanism, endorsed by the National Cyber Security Centre, for organisations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions. Its effectiveness has been independently assessed and verified by researchers at Lancaster University.[21] There are two types of certification under this scheme:

- **Cyber Essentials** requires the organisation to complete a self-assessment questionnaire, with responses independently reviewed by an external certifying body.
- **Cyber Essentials Plus** covers the same requirements as Cyber Essentials, but tests of the systems are carried out by an external certifying body using a range of tools and techniques.

60. As these are basic technical controls, the Scottish Government expects that the majority of Scottish public bodies will already adhere to these requirements – indeed, many will have more advanced standards of cyber security in place, and may already benefit from independent assurance or certification to this effect.

61. There are nevertheless benefits in ensuring, as far as possible, a **common approach** to providing independent assurance that these critical cyber security controls are in place in all Scottish public bodies, thus reinforcing public trust in digital public services in Scotland. The public sector adopting an approach to independent assurance around these critical controls that is widely available across Scotland would, for example, help raise awareness of their importance and promote uptake amongst suppliers and the wider private and third sectors.

62. To promote the development of such a common approach, the Scottish Government will support the achievement of **Cyber Essentials** and **Cyber Essentials Plus** certification across Scottish public bodies wherever possible. It will do so by requiring and supporting the following approach under this action plan:

- The Scottish Government will make available **funding for all public bodies** to access external expertise to undergo a **Cyber Essentials "pre-assessment"** by **end March 2018.**[22]
- The output of these pre-assessments should include a **report** to the **Boards/Senior Management Teams** of public bodies, providing them with independent analysis of their current conformity with the five critical controls under the scheme, and supporting them to understand their exposure to risk from the most common internet-borne threats.
- On the basis of this pre-assessment and any other key factors (including the organisation's appetite for further independent assurance that the five critical controls are being met, and their assessment of costs and benefits) the Board/Senior Management Teams of Scottish public bodies should then make an **informed decision** on which of the following certifications to opt for:

[20] See: https://www.cyberaware.gov.uk/cyberessentials/files/scheme-summary.pdf

[21] http://www.research.lancs.ac.uk/portal/en/publications/cyber-security-controls-effectiveness(a09a2d28-d121-41dc-86d6-cc24595d8968)/export.html

[22] Evidence suggests this process can help significantly with achieving Cyber Essentials or Cyber Essentials Plus certification.

- **Cyber Essentials Plus certification:** This is the option strongly preferred by the Scottish Government and the National Cyber Resilience Leaders' Board in the absence of any other independent assurance that the five critical controls are being met.

- **Cyber Essentials certification:** This option may be chosen where the organisation has alternative independent assurance that the five critical controls are in place. The benefits of nevertheless adopting Cyber Essentials certification in these circumstances are expected to include clear, consistent messaging to citizens, suppliers and the private and third sectors in Scotland that Scottish public bodies take cyber security seriously, and insist on the five critical controls being in place. Public bodies that opt for Cyber Essentials (as opposed to Cyber Essentials Plus) will be invited to justify their reasoning.

Individual public bodies will be asked to bear the costs of achieving certification and any remediation work required to meet the critical controls.

63. Public bodies should then go on to ensure that they **achieve either Cyber Essentials** or **Cyber Essentials Plus certification** by **end October 2018**. In the event that this deadline cannot be met for legitimate reasons, Scottish public bodies will be asked to demonstrate (under initial monitoring arrangements – see Key Action 11) that they have in place **plans to achieve appropriate certification as soon as possible thereafter.**[23]

64. It is possible that, in exceptional cases and for some particularly complex public bodies, the pre-assessment will make clear that Cyber Essentials or Cyber Essentials Plus is not an appropriate standard to work towards. This may be the case for certain complex environments such as schools, universities and colleges, where a more risk-based approach is required to issues such as access control than is currently encompassed in the Cyber Essentials scheme. Where this is the case, the Scottish Government Cyber Resilience Unit will work with public bodies and (where appropriate) the wider public sector to identify alternative ways of providing independent assurance that the five critical controls are in place.

65. It is also possible that, as the process of undergoing Cyber Essentials/Plus pre-assessments or certification for public bodies proceeds, wider issues or challenges in the operation of the scheme will be identified. Where this is the case, public bodies will be encouraged to raise this with the Scottish Government Cyber Resilience Unit who will draw these issues to the attention of the NCSC, and alternatives to Cyber Essentials may be considered.

[23] Discussions with **local authorities** and the **college and university sectors** have indicated that a **targeted and phased** approach to achievement of Cyber Essentials may be appropriate for these sectors with very complex networks. Achievement of Cyber Essentials within the timelines set out above may, for example, only be feasible or desirable for the **central** or **"core"** networks of these organisations, assuming the scoping requirements of the Cyber Essentials scheme as applied to these specific organisations' networks permits this. The Scottish Government will work closely with bodies such as the Local Government Digital Office, HEIDS and UCSS to support the development of an appropriately targeted and phased approach for the wider public sector.

66. The Scottish Government expects the following key benefits to be realised by adopting this overall approach:

- ensuring that Boards/Senior Management in all Scottish public bodies have given **appropriate, informed consideration to the cyber threat to their key assets**, and are satisfied that they have **appropriate independent assurance** that the five critical controls are in place to protect against the most common cyber threats to key assets (or understand what remediation action needs to be taken to address issues identified); and

- sending a **clear, consistent message to the public and key partners in the private and third sectors** that common baseline levels of cyber security are in place across Scottish public bodies, **lending greater weight to work to promote Cyber Essentials across Scotland**.

67. The accompanying **toolkit**[24] provides more information on how public bodies can approach the issue of Cyber Essentials certification, and how funding for the pre-assessment stage will be made available.

68. It is important to note that, while Cyber Essentials offers a sound foundation of basic cyber hygiene measures, it only concerns itself with technical controls that prevent the most common internet-borne attacks. It will not remove all cyber security risk; for example, it is not designed to address more advanced, targeted attacks. Additional controls to address more advanced threats will form part of the "target" and "advanced" progression stages of the Scottish Public Sector Cyber Resilience Framework.

69. The aim of achieving Cyber Essentials certification (or alternative independence assurance around the five critical controls) is expected to be an ongoing one as part of the wider Scottish Public Sector Cyber Resilience Framework. Further details will be decided upon once the Framework has been finalised.

[24] Available at www.gov.scot/cyberresilience

Key Action 5

The Scottish Government will work with Scottish public bodies to ensure they are aware of, and implement appropriately, services available under the National Cyber Security Centre's Active Cyber Defence (ACD) Programme by end June 2018.

70. The NCSC's Active Cyber Defence (ACD) programme aims to:

- make internet infrastructure and internet-based technologies, products and services automatically safer in ways that users won't even notice; and
- make internet-based products and services easier to use safely by organisations and individuals.

71. The NCSC has made available to public services a number of free-to-use measures under the ACD programme. None of them requires additional money to implement, nor are they overly technically complex to implement. They are:

- **Protected DNS**, which takes the data GCHQ and commercial partners have about known malicious addresses, and then simply blocks users in public sector bodies from going there. In this way it automatically prevents public servants visiting infected sites whilst using work systems.
- **DMARC anti-spoofing**, which is a protocol that makes it much harder for attackers to send fake emails that look as if they come from Scottish public sector bodies (which is often done in email spoofing and spear-phishing, the most common way of introducing malware into victims' systems). What this means for the citizen is that instead of being advised 'not to open a dodgy looking email' the 'dodgy email' does not arrive. In parallel, NCSC have built the **MailCheck service**, which monitors adoption of the standard and provides data on trends. MailCheck also processes DMARC reports centrally, to generate data which further enhances the NCSC's knowledge of the threat picture.
- **Webcheck**, which helps public bodies fix vulnerabilities on their websites. One thing victims and attackers both do is scan for vulnerabilities in Internet facing services so that they know what to defend, or attack. Commercial services are available to do this. But for smaller public bodies the cost of these services might prove prohibitive, and they may not be able to afford to employ anyone who understands the results. The NCSC offers a free service known as Webcheck to scan the websites of public bodies and generate a report on what needs fixing, and how to fix it.
- **Phishing and malware mitigation (Netcraft)**, a service that NCSC have worked on with Netcraft, a private sector company, which public bodies will benefit from automatically without having to do anything. However, public bodies can help augment the service by notifying Netcraft if they themselves discover they are the target of a phishing campaign, or if there are malicious emails purporting to be from them. Netcraft will then issue takedown notifications to the hosts of the email and phishing sites.

72. The Scottish Government will work with Scottish public bodies to **raise awareness** of these services, and any similar new services being made available in the future, and encourage public bodies to make appropriate use of them. It will, however, be open to Scottish public bodies to make use of alternative commercial solutions if they wish to do so.

73. The accompanying **toolkit**[25] provides further information on how Scottish public bodies can take advantage of the Active Cyber Defence Programme. It should be noted that some measures may not be available to the wider Scottish public sector, such as universities and colleges.

Key Action 6

The Scottish Government will seek assurances from Scottish public bodies that they have in place appropriate staff training, awareness-raising and disciplinary processes with regard to cyber resilience for staff at all organisational levels.

To support this the Scottish Government will work with key partners to provide access to appropriate materials and guidance.

74. Technical measures alone are insufficient to defend against cyber threats. To ensure a minimum level of cyber security, it is vital that users of technology in Scottish public bodies technology (often referred to as "digital end users") understand the risks presented by cyber threats, and adopt appropriate behaviours to mitigate them. The Scottish Government believes that people are the strongest line of defence against the cyber threat to the public sector. Because of the links between cyber security and physical and personnel security, training and awareness raising activity around cyber resilience should ideally be situated within wider arrangements for the security education of staff.

75. The new NIS Directive, applicable to the devolved health and water sectors, will include requirements in respect of staff training, awareness raising and disciplinary procedures. The Scottish Public Finance Manual already sets out requirements for Accountable Officers to ensure that managers at all levels have the information, training and access to expert advice which they need to exercise their responsibilities effectively.

76. It is for individual public bodies to decide how best to implement these obligations, taking account of the needs of their staff. Many Scottish public bodies will already have some or all of these measures in place, and it is the responsibility of their Boards/Senior Management Teams to ensure this is the case.

77. However, to help support a core common approach across the Scottish public sector, the Scottish Government will:

- **in the immediate term, signpost Scottish public bodies to existing, high quality learning resources** that encompass aspects of cyber security, for use to meet initial baseline progression stage requirements by **end June 2018**; and
- **in the medium term**, make available **Scottish public sector-focused guidance and e-learning products** to support organisational cyber resilience. This material will be drawn from a range of funded training and awareness raising initiatives that are currently under development or implementation in Scotland. These include a significant **security behavioural change programme** that will be developed and implemented within the **Scottish Government** between 2018-20. An outline of this specific programme of work can be found at **Annex D**.

[25] Available at www.gov.scot/cyberresilience

78. Materials developed from these initiatives will be disseminated as they become available during the course of 2018 onwards. The Scottish Government will also make available information to Scottish public bodies about any specialist skills development opportunities that are identified under a separate learning and skills action plan that is being developed in partnership with the NCRLB. This information may assist with identifying, for example, retraining and/or up-skilling opportunities for staff in order to plug skills shortages in public bodies.

79. The **toolkit**[26] accompanying this action plan provides details on existing high quality training resources, **ongoing training and awareness raising projects** that public bodies may wish to make use of, and a range of **scenarios** that public bodies can use to explore their organisational cyber resilience.

80. These resources, in combination, should help provide appropriate training and awareness-raising materials for:

- Boards, senior executives and their support functions
- Managers
- Security-focused staff (including cyber security and front of house staff)
- Specialist staff, including IT, HR, finance, audit, legal and procurement
- Privileged users
- All staff in both policy and delivery roles, whether permanent, temporary or contractors

81. As noted in Key Action 7, a series of specialist training courses is being organised to support the development of specific skills and capability in cyber security incident response.

(iii) Respond and recover

82. Under the **"respond and recover"** domain at the **initial baseline progression stage**, the following requirements will apply.

Key Action 7

The Scottish Government will work with the NCSC, Police Scotland and other key partners to ensure that Scottish public bodies have cyber incident response policies and processes in place, and that these can integrate with robust, clear, central cyber incident notification and coordination protocols by end June 2018.

83. Even the most robust preparations cannot prevent the most sophisticated cyber-attacks from successfully penetrating cyber-defences. When this happens, it is vital that Scottish public bodies are able to detect such attacks, respond appropriately and rapidly, and take action to recover and restore vital public services.

84. The new NIS Directive guidelines are expected to include requirements in respect of response and recovery planning, and the ability to make improvements to these arrangements on an ongoing basis.

[26] Available at www.gov.scot/cyberresilience

85. It is for individual public bodies to put in place cyber incident response policies and processes that best suit their organisational needs. However, to help support a core common approach across the Scottish public sector, the Scottish Government will work with the NCSC, Police Scotland and other key partners to:

- **develop and disseminate robust, clear central cyber incident notification and coordination protocols for the Scottish public sector.** While maintaining the position of the NCSC as the primary reporting route for significant cyber incidents, these protocols will align with the tried and tested Scottish Government Resilience Room arrangements, and ensure that the NCSC, Police Scotland and Scottish Ministers are made aware of, and can offer appropriate support to the management of, significant cyber incidents in the Scottish public sector.

- **develop and disseminate a template Cyber Incident Response Plan for Scottish public bodies**, which can be adapted to individual public bodies' needs, including as part of their wider incident response arrangements.

- **put in place a series of specialist training courses to support the development of specific skills and capability in respect of cyber security incident response.** Funding is being made available to a project led by Napier University to produce a series of training courses for Scottish public sector staff involved in cyber incident response. These will be delivered at strategic locations around Scotland in order to ensure coverage and develop national capability. It is part of a programme of work coordinated by the Scottish Government and supported by funding from the UK Cyber Security Strategy Programme.

86. Scottish public bodies will be asked to provide assurance (under initial monitoring arrangements – see Key Action 11) that they have cyber incident response plans in place, and that these are aligned appropriately with the central incident reporting and coordination protocols.

C. Preparing for the "Target" and "Advanced" progression stages – supply chain cyber security

87. While the Scottish Public Sector Cyber Resilience Framework is still under development, it is nevertheless clear that **supply chain security** will form a key part of the requirements under the "Identify" domain. Work on supply chain cyber security has been identified by Scottish public sector organisations as a particular challenge requiring careful thought and attention.

88. The Scottish Government will therefore take action to begin preparations for this aspect of the "target" and "advanced" progression stages under the Framework.

Key Action 8

The Scottish Government will develop a proportionate, risk-based policy in respect of supply chain cyber security, which should then be applied by public bodies in all relevant procurement processes. The views of Scottish business organisations will be sought on a draft policy early in 2018, with a view to implementation as part of the Scottish Public Sector Cyber Resilience Framework.

Additionally, the Scottish Government will develop guidance on the need for recipients of public grant funding to have in place proportionate and risk-based cyber security arrangements. These requirements will align with the new supply chain cyber security policy.

89. Scottish public bodies contract with a wide range of suppliers in the private and third sectors to help support the delivery of vital public services. The NCSC notes[27] that, when information and security arrangements are shared across a supply chain or business information chain, the cyber security of any one organisation within the chain is potentially only as strong as that of the weakest member of the supply chain. Cyber criminals can make use of this by identifying the organisation with the weakest cyber security within the supply chain, and using the vulnerabilities present in their systems to gain access to other members of the supply chain. Whilst not always the case, it is often the smaller organisations within a supply chain who, due to more limited resources, have the weakest cyber security arrangements.

90. The new NIS Directive requirements are expected to include requirements in respect of supply chain security. In order to support these provisions, and mitigate supply chain risks, the Scottish Government will work closely with the NCSC and other key partners to:

- develop a **proportionate, risk-based policy in respect of supply chain cyber security policy**. A draft policy will be produced for comment by Scottish business organisations by **early 2018**, allowing any key developments in respect of NIS Directive implementation to be incorporated. **Cyber Essentials accreditation** is expected to form a core part of this policy.
- following consultation, publish a **Scottish Procurement Policy Note** (SPPN) by **May 2018**. This will form part of the Scottish Public Sector Cyber Resilience Framework from **June 2018**
- work with key partners to **ensure Scottish public bodies have plans in place to implement the SPPN** as part of the Scottish Public Sector Cyber Resilience Framework, and under refreshed requirements set out in the Scottish Public Finance Manual. Where bodies are not subject to the SPFM, they will nevertheless be encouraged to adopt similar policies; and
- update the **Scottish Government Procurement Journey**, the online best practice manual available to the whole Scottish public procurement community, to reflect these requirements.

[27] https://www.ncsc.gov.uk/guidance/cyber-security-risks-supply-chain

91. To help move this work forward at pace, the Scottish Government has opened a dialogue with business representative bodies regarding the potential impact of requiring cyber security accreditation on the business community (particularly SMEs). The Scottish Government has also started a **review of existing Scottish Government contracts** to assess potential cyber risks and address these.

92. Clear guidance on how and by which dates **existing contracts** to which the finalised procurement policy applies should be brought into conformity will be provided.

93. The Scottish Government, in common with other public bodies, provides significant levels of **grant funding** to public, private and third sector organisations. Grants are awarded for specific purposes, often covered by legislation, and depend on eligibility and the availability of funds. Awarding grants helps the Scottish Government deliver its policies and contributes to the achievement of strategic objectives.

94. Currently, central guidance makes clear that **due diligence** should be conducted by Scottish public bodies on recipients of grant funding. Cyber resilience can be fundamental to recipient organisations' ability to deliver on the objectives of grant funding and safeguard public funds.

95. To ensure that consideration of organisational cyber resilience is included in wider due diligence in respect of grant funding, the Scottish Government will:

- update central guidance on grant funding and the SPFM, to require proportionate and risk-based cyber security arrangements to be in place for recipients of grant funding. These requirements will align with supply chain requirements set out in a new SPPN.
- make other Scottish public sector organisations aware of the policy set out in this guidance and the SPFM, and encourage them to adopt similar policies.

D. Ensuring Scottish public sector organisations can access cyber security expertise and support

Key Action 9

The Scottish Government will put in place a Dynamic Purchasing System by end October 2017 to ensure that Scottish public sector organisations can access expertise in support of their work on cyber resilience.

96. In taking forward work to assure their levels of cyber resilience, Scottish public sector organisations can approach the Scottish Government's Cyber Resilience Unit, iTECS and the Digital Transformation Service for initial, high level advice on implementation of the requirements in this action plan. A toolkit[28] has been produced to support implementation of this action plan.

[28] Available at www.gov.scot/cyberresilience

97. However, for more in-depth support and expertise it is expected that the private and/or third sectors will play a key role. It is vital that Scottish public sector organisations can access appropriate cyber security expertise in support of their work on cyber resilience in an open, transparent and agile way. To assist with this, the Scottish Government will:

- develop a **dynamic purchasing system** with a list of **cyber resilient specialist suppliers** which Scottish public bodies can access to help support their cyber security **by end October 2017.**

98. This system will ensure that cyber security service companies of all sizes (particularly SMEs) can access and tender for relevant public sector contracts. One of the aims of the framework will be to support the growth of a cyber security cluster in Scotland, thus supporting inclusive economic growth. It will be available as a route to market for:

- Central Government
- Health
- Local authorities
- Universities and colleges
- Third Sector (voluntary organisations and charities registered in Scotland)
- Other public bodies

E. Scottish public sector cyber resilience – leadership and knowledge sharing

Key Action 10

The Scottish Government will introduce a Public Sector Cyber Catalyst scheme, under which Chief Executives of key Scottish public bodies will commit their organisations to working to become exemplars in respect of cyber resilience.

The Public Sector Cyber Catalysts will support the development of the new Scottish Public Sector Cyber Resilience Framework, undertake work to implement it once finalised, and share learning and knowledge gained as a result. The Scottish Government will itself become a Public Sector Cyber Catalyst.

Appropriate support will be made available to the Public Sector Cyber Catalyst programme to help drive this work forward.

99. Achieving effective practice in respect of cyber resilience across the public sector, including through compliance with the proposed "target" and "advanced" stages of progression under the Scottish Public Sector Cyber Resilience Framework, will require commitment, resource and leadership on the part of the Scottish Government and its partners.

100. To help provide this leadership, the Scottish Government has agreed with a number of key Scottish public bodies that they will commit to acting as leaders in respect of cyber resilience and the work set out in this action plan. In view of the expectation that this work will help "catalyse" learning and action by other Scottish public sector organisations over time, they will be referred to as the **Scottish Public Sector Cyber Catalysts**. A list of confirmed cyber catalyst organisations is set out at **Annex E**.

101. Agreement has been reached at Board/Senior Management level within these organisations that appropriate priority and resource will be devoted to this work. The Public Sector Cyber Catalysts will be asked to:

- work with the Scottish Government, the NCRLB, the NCSC and other key partners to **finalise the Scottish Public Sector Cyber Resilience Framework** by end June 2018;
- thereafter, **develop individual action plans** to drive forward work to achieve the target and/or advanced progression stages, and ensure arrangements are in place to satisfy their internal Boards/Senior Management as to progress;
- **share knowledge and learning with:**
  - **one another on the basis of this activity**, including in respect of any challenges or difficulties they have encountered, or any innovative solutions they have identified to overcome barriers and ensure effective implementation;
  - **the UK NCSC and the UK Government Cabinet Office**, **as well as NIS competent authorities,** to help inform the future development of the NIS standards and guidelines and other relevant requirements. Over time, the expectation is that these standards and guidelines will mature and improve to take account of experience in implementing them and technological developments;
  - **other Scottish public, private and third sector organisations** in order to help drive best practice in respect of cyber resilience across Scotland. At an appropriate stage, Public Sector Cyber Catalysts may be invited to partner with other Scottish public bodies to help share their knowledge and support them on their journey towards higher levels of cyber resilience. This will be a key way of catalysing wider activity across the Scottish public sector.
- **report to the Scottish Government and/or (where appropriate) competent authorities on their progress against the Scottish Public Sector Cyber Resilience Framework**, either in line with relevant legal obligations (for bodies subject to the EU NIS Directive) or on a voluntary basis (for other bodies). Further details on how this will be achieved are set out in **Section F** (Monitoring and Evaluation).

102. The Scottish Government is clear it must itself be an exemplar organisation if it is to provide effective leadership in respect of cyber resilience in Scotland. It will assume a lead role as one of the Public Sector Cyber Catalysts.

103. The Scottish Government will consider what practical support may be required to drive forward this work following further discussions with cyber catalyst bodies. This may include alignment with future CivTech challenges where it appears there is a potential requirement for technical solutions to issues identified as a result of the cyber catalyst process. The Scottish Government will also provide support to ensure that knowledge and learning is captured and shared between the Public Sector Cyber Catalysts and across the wider Scottish public sector, as well as the private and third sectors where appropriate.

F. Monitoring and Evaluation

Key Action 11

The Scottish Government will put in place an effective monitoring and evaluation framework to help assess progress against this action plan and, once developed, the Scottish Public Sector Cyber Resilience Framework.

104. It is important that Scottish Ministers, the NCRLB and other key bodies are provided with a clear picture of levels of cyber resilience across Scottish public bodies, so that they can provide challenge and support where there is a need for improvement, and supply information to the public and the Scottish Parliament to reinforce trust in Scotland's digital public services.

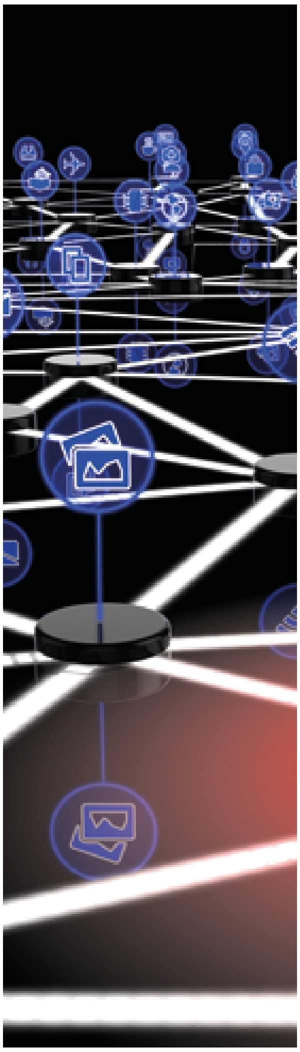
105. To help achieve this, the Scottish Government will:

- Request all Scottish public bodies to provide **one-off written updates**, setting out progress on implementing key actions against the initial baseline progression stage under this action plan. These updates will be requested at **end June 2018** (for the majority of actions) and **end October 2018** (in respect of Cyber Essentials certification or, exceptionally, alternative independent assurance that critical controls are in place).
- Put in place **appropriate monitoring and evaluation processes** to support the implementation of the Scottish Public Sector Cyber Resilience Framework from end June 2018 onwards. Consideration will be given to the development of appropriate tools to support these arrangements and minimise burdens on public bodies.

106. Appropriate information on progress will be made available to the public, Ministers, Parliament and the NCRLB, with due regard to cyber security considerations. Further details of proposed monitoring arrangements can be found at **Annex C**.

107. If, as a result of this monitoring and reporting work, it becomes apparent that public bodies are falling short of the standards of cyber resilience expected of them, appropriate action will be taken. This may include the Scottish Government making direct contact with the relevant public bodies at Board/Senior Management level to request assurance that action is being taken to address any deficiencies, and to establish whether further assistance or support is required. It is also expected that inclusion of key requirements in the Scottish Public Finance Manual will ensure appropriate accountability of public bodies for their activity in respect of cyber resilience, via the provision of governance statements and certificates of assurance, internal and external audit and, ultimately, accountability arrangements to Ministers and to Parliament.

ANNEXES



A

Annex A. Key Actions and Timelines – Summary

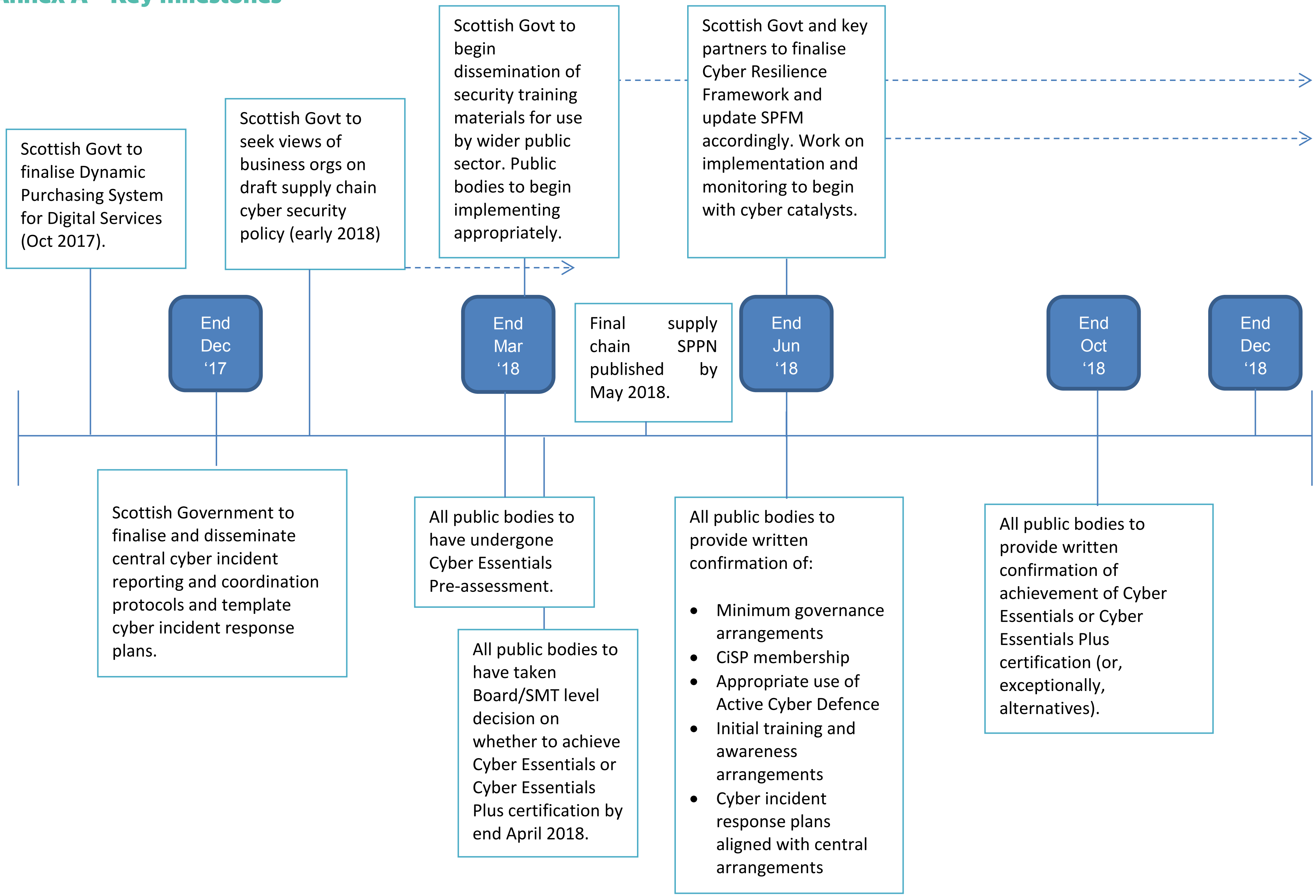
Key action no.	Action required of:	Requirements	Deadline	Page no. action plan
Preparatory	All Scottish public bodies	• Provide contact details for (i) Board/Senior Management, (ii) working-level, and (iii) incident response to SG Cyber Resilience Unit.	End November 2017	N/A
1	Scottish Government, NCRLB, NCSC, Cyber Catalysts Scottish Government	• Finalise **Scottish Public Sector Cyber Resilience Framework**, taking account of developments with NIS Directive and Security Policy Framework. • Update **Scottish Public Finance Manual** to reflect Framework requirements.	End June 2018 End June 2018	16-18
2	All Scottish public bodies	• Ensure **minimum cyber risk governance arrangements** in place.	End June 2018	19-20
3	All Scottish public bodies managing networks	• Ensure **membership of Cybersecurity Information Sharing Partnership**.	End June 2018	20
4	All Scottish public bodies	• Undergo **Cyber Essentials "pre-assessment"** funded (to defined limits) by Scottish Government. • Take **Board/Senior Management level decision** on whether to pursue Cyber Essentials or Cyber Essentials Plus Certification. • Achieve **Cyber Essentials** or **Cyber Essentials Plus** certification.[29]	End March 2018 End April 2018 End October 2018	21-24

[29] As noted in the action plan, it is possible that, in exceptional cases and for some particularly complex public bodies, the pre-assessment will make clear that Cyber Essentials or Cyber Essentials Plus is not an appropriate standard to work towards. It is also possible that, as the process of undergoing Cyber Essentials/Plus pre-assessments or certification for public bodies proceeds, wider issues or challenges in the operation of the scheme will be identified. Where this is the case, public bodies will be encouraged to raise this with the Scottish Government Cyber Resilience Unit who will draw these issues to the attention of the NCSC, and alternatives to Cyber Essentials may be considered.

5	All Scottish public bodies	• Ensure **appropriate implementation of Active Cyber Defence measures**	End June 2018	25-26
6	All Scottish public bodies	• Ensure **initial arrangements for appropriate training and awareness raising** in place.	End June 2018	26-27
	Scottish Government	• Develop and disseminate **core training and awareness raising approach, materials, etc.** for use by public sector, as part of wider security training and awareness raising package.	From March 2018-2020	
	All Scottish public bodies	• **Adapt and implement core training and awareness raising approach, materials, etc.** as it becomes available.	From March 2018-2020	
7	Scottish Government, NCSC, Police Scotland	• Finalise and disseminate **central cyber incident reporting and coordination protocols** and **template cyber incident response plans**.	End 2017	27-28
	All Scottish public bodies	• Ensure **cyber incident response plans in place** and **aligned with central protocols**.	End June 2018	
8	Scottish Government	• Seek views of Scottish business organisations on **draft supply chain cyber security policy on procurement**.	Early 2018	29-30
	Scottish Government	• Publish **Scottish Procurement Policy Note** as part of Scottish Public Sector Cyber Resilience Framework.	End May 2018	
	Scottish Government	• **Align grant funding guidance** and **SPFM**.	End May 2018	
	All Scottish public bodies	• **Implement Scottish Procurement Policy Note** and **grant funding guidance** as part of Scottish Public Sector Cyber Resilience Framework.	From June 2018	

9	Scottish Government	• Put in place **Dynamic Purchasing System** for **Digital services** (including **cyber security**) for Scottish public sector.	End October 2017	30-31
10	Public Sector Cyber Catalysts	• Work with Scottish Government, NCSC and NCRLB to **finalise Scottish Public Sector Cyber Resilience Framework**, and **identify key challenges** facing Scottish public sector.	By end June 2018	31-32
	All Scottish public bodies, inc. Cyber Catalysts	• Begin **implementation of**, and (in line with final arrangements) **reporting against**, Framework.	From end June 2018	
	Public Sector Cyber Catalysts	• **Share learning and knowledge** with wider public sector.	In line with progress	
11	All Scottish public bodies	• **Informal, working-level responses** to enquiries on progress from Scottish Government Cyber Resilience Unit.	Ongoing	33
		• Provide **one-off written assurance at Board/Senior Management level** on the following: ○ confirmation of (i) having undergone a Cyber Essentials pre-assessment, (ii) having taken a decision on whether to seek Cyber Essentials or Cyber Essentials Plus, and (iii) the expected timelines for achieving this. ○ Board/Senior Management level commitment and basic governance arrangements. ○ CiSP membership. ○ Appropriate use of Active Cyber Defence measures. ○ Appropriate training and awareness raising processes. ○ Cyber incident response protocols, aligned with central mechanisms.	End June 2018	
		• Provide **one-off written confirmation** that Cyber Essentials or Cyber Essentials Plus certification (or, exceptionally, alternative independent assurance) has been achieved.	End October 2018	
	Scottish Government	• Develop and implement appropriate **monitoring and evaluation arrangements** as part of **Scottish Public Sector Cyber Resilience Framework**, and communicate these to public bodies.	End June 2018	

Annex A – Key milestones



Scottish Govt to finalise Dynamic Purchasing System for Digital Services (Oct 2017).

End Dec '17

Scottish Government to finalise and disseminate central cyber incident reporting and coordination protocols and template cyber incident response plans.

Scottish Govt to seek views of business orgs on draft supply chain cyber security policy (early 2018)

Scottish Govt to begin dissemination of security training materials for use by wider public sector. Public bodies to begin implementing appropriately.

End Mar '18

All public bodies to have undergone Cyber Essentials Pre-assessment.

All public bodies to have taken Board/SMT level decision on whether to achieve Cyber Essentials or Cyber Essentials Plus certification by end April 2018.

Final supply chain SPPN published by May 2018.

Scottish Govt and key partners to finalise Cyber Resilience Framework and update SPFM accordingly. Work on implementation and monitoring to begin with cyber catalysts.

End Jun '18

All public bodies to provide written confirmation of:

- Minimum governance arrangements
- CiSP membership
- Appropriate use of Active Cyber Defence
- Initial training and awareness arrangements
- Cyber incident response plans aligned with central arrangements

End Oct '18

All public bodies to provide written confirmation of achievement of Cyber Essentials or Cyber Essentials Plus certification (or, exceptionally, alternatives).

End Dec '18

Annex B. High-level concept for Scottish Public Sector Cyber Resilience Framework

1. This annex sets out a high level concept for the development of a Scottish Public Sector Cyber Resilience Framework.

2. The Scottish Government will work with the NCRLB, the NCSC, the Scottish public sector cyber catalysts[30] and other key partners to develop this concept by **end June 2018**, with a view to implementing it thereafter. It will be subject to change as UK Government plans for implementation of the NIS Directive become clearer in early 2018.

Aims

3. The Framework will aim to:

- Provide a **common, effective approach** for Scottish public bodies to **assess their levels of cyber resilience**, ensure they adhere to **minimum cyber resilience requirements**, and **progress** towards achieving higher levels of cyber resilience on a risk-based and proportionate basis.

- Align with the new **NIS Directive legislation and guidance** and **other key measures,[31]** to ensure consistency with forthcoming developments. Clarity on the key requirements of these initiatives is expected to have been achieved by **early in 2018**.

- Take account of **foreseeable technological developments**, such as a move to greater reliance on cloud systems and the further development of Smart City technologies and the Internet of Things.

- As far as possible, **minimise any additional burdens** on Scottish public bodies, including by making clear **how the Framework relates to existing standards or requirements**, and taking account of these when providing guidance on compliance. Wherever possible, the Scottish Government will work closely with the UK Government to promote rationalisation and alignment of different standards, although this will take time to achieve.

- Help to provide **clarity and assurance** to individual organisations, Ministers, Parliament and the public that appropriate levels of cyber resilience are in place across Scottish public bodies. Appropriate **monitoring and evaluation arrangements** will be put in place to align with the Framework (see Key Action 11). Consideration will be given to clarifying appropriate penetration testing and audit requirements under the framework, and aligning these with existing requirements such as PSN accreditation.

- Seek to align with a similar framework/hierarchy under development as part of the development of **private and third sector action plans on cyber resilience** by the Scottish Government and the NCRLB.

[30] See Key Action 10 in the action plan.

[31] Including the new Technology Security Standard under the Security Policy Framework and the GDPR.

Overview of key proposed features

4. The concept framework takes as its starting point the new **NIS Directive** legislation and guidance (which itself draws on existing frameworks such as the NIST Cyber Security Framework). Subject to the final shape of the NIS Directive legislation, it is expected that it will cover the following **4 key domains** of cyber resilience:

- **Identify (Governance and Risk Management)**: Appropriate organisational structures, policies and processes are in place to understand, assess and systematically manage risks to the network and information systems supporting essential services. Specific requirements will be set out in respect of:
  - Risk management
  - Asset management
  - Supply chain risk management
- **Protect**: Proportionate security measures should be in place to protect essential services and systems from cyber-attack, system failures, or unauthorised access. Specific requirements will be set out in respect of:
  - Service protection policies and processes
  - Identity access and control
  - Data security
  - System security
  - Resilient Networks and systems
  - Staff awareness and training
- **Detect**: Appropriate capabilities should be in place to ensure network and information system security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential services/public services. Specific requirements will be set out in respect of:
  - Security monitoring
  - Anomaly detection
- **Respond and recover**: Capabilities to minimise the impacts of a cyber security incident on the delivery of essential services/public services, including the restoration of those services where necessary.
  - Response and recovery planning
  - Improvements

5. Within and across these 4 key domains, the concept framework proposes clear **stages of progression** that Scottish public bodies can work towards. These will be as follows:

- **Initial baseline**: These will be the initial baseline requirements that all Scottish public bodies will be expected to meet as a minimum by **end June 2018** (or end October 2018 in the case of Cyber Essentials certification/independent assurance of critical controls). These requirements will aim to ensure that all Scottish public bodies have in place a common baseline of good cyber resilience practice in the short term.

  It is expected that the majority of Scottish public bodies will already in effect be meeting these requirements. However, the requirements set out under the initial baseline stage will provide clarity and assurance that this is the case.

  These initial baseline requirements form part of the public sector action plan. Key Actions 2 to 7 set out how Scottish public bodies will be asked to make progress towards meeting these initial baseline standards.

- **Target:** The requirements under this stage of progression will be those that all Scottish public bodies will be expected to work towards meeting, on a risk-based and proportionate basis. They are expected to be aligned with the new Security Policy Framework Technology Security Standard and other key existing standards and guidelines, and should, when met, help ensure that good practice in respect of cyber resilience is in place across Scottish public bodies.

- **Advanced:** These requirements will align with the **NIS Directive legislation and guidance**. Scottish public bodies in the health and water sectors will automatically be subject to these requirements under relevant legislation. However, the Scottish Government will also encourage other public bodies that form part of critical infrastructure in Scotland to work towards achieving the requirements under this highest stage of progression.

6. The Scottish Government will work closely with key partners to ensure a clear understanding of the way in which **existing standards, requirements and guidelines** can contribute to assurance that requirements under the Framework's different domains and stages of progression are being met. In particular, in view of the landscape within which Scottish public bodies are currently operating, it will be made clear how the following standards, requirements and guidelines can offer guidance or assurance in respect of each domain and progression level:

- Cyber Essentials (Plus)
- Public Service Network (PSN) Information Assurance Obligations
- Public Service Network for Policing (PSNP) Information Assurance Obligations
- The NHSScotland Information Security Policy Framework
- The 10 Steps to Cyber Security
- The IASME Governance Standard
- ISO 27001
- The SANS Top 20 Critical Controls
- The NIS Directive Legislation requirements and guidelines

7. To support this, the Scottish Government will explore the potential for the development of **a self-assessment and reporting tool**, that, as well as supporting Scottish public sector organisations to assess and report on their organisational progress against the Scottish Public Sector Cyber Resilience Framework, could make clear the links between other standards, requirements or guidelines (including the Competent Authority NIS Assessment process), and assist in "translating" these into a self-assessment against the Framework (see also Annex C – Key monitoring and evaluation measures for Scottish public bodies).

8. The Scottish Government will also work with the NCRLB and key partners to make clear how the 4 domains and 3 stages of progression relate to similar hierarchies that are currently under development by the NCRLB in respect of the private and third sectors. The aims of this alignment will be to:

- assist with **benchmarking** and **example-setting** across different sectors; and to
- promote an **understanding of levels of cyber resilience across Scotland as a whole**.

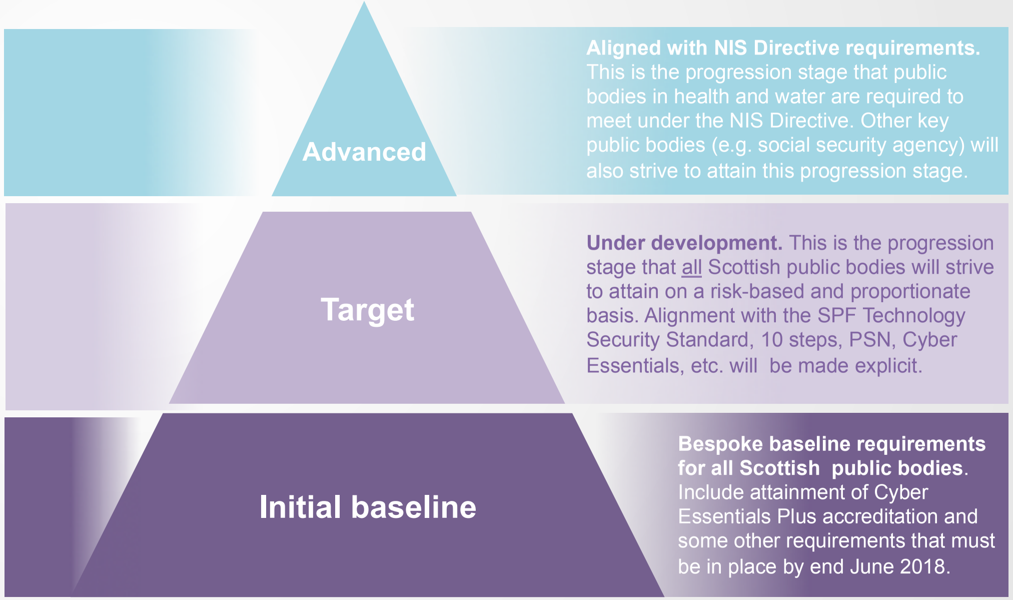
9. The following pages provide an early example of what the NCRLB and the Scottish Government aim to achieve in respect of the overarching framework.

Scottish Public Sector Cyber Resilience Framework (Indicative)

The Four Domains

Identify				Protect						Detect		Respond and Recover	
Governance	Risk Management	Asset Mgt	Supply chain	Service protection	ID access/control	Data secueity	System security	Resilient networks	Staff Training	Sec. Monitoring	Anomaly detection	Response planning	Improvements
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Under development													
✓	✓				✓		✓		✓	✓		✓	

The Three "Stages of Progression"



Aligned with NIS Directive requirements. This is the progression stage that public bodies in health and water are required to meet under the NIS Directive. Other key public bodies (e.g. social security agency) will also strive to attain this progression stage.

Under development. This is the progression stage that all Scottish public bodies will strive to attain on a risk-based and proportionate basis. Alignment with the SPF Technology Security Standard, 10 steps, PSN, Cyber Essentials, etc. will be made explicit.

Bespoke baseline requirements for all Scottish public bodies. Include attainment of Cyber Essentials Plus accreditation and some other requirements that must be in place by end June 2018.

Annex C. Key monitoring and evaluation measures for Scottish public bodies

1. This annex outlines the monitoring and evaluation arrangements that will be put in place to provide assurance that Scottish public bodies are making progress towards the initial baseline, target and advanced stages of progression under the Scottish Public Sector Cyber Resilience Framework.

A. One-off monitoring and evaluation arrangements against initial baseline progression stage

2. On a one-off basis, all Scottish public bodies will be asked to provide information to the Scottish Government (and, if appropriate and upon agreement, NIS Competent Authority/ies) with regard to progress against key actions under the **initial baseline progression stage** of the Scottish Public Sector Cyber Resilience Framework. The wider public sector, including local authorities and the colleges and universities sector, will also be encouraged to participate in these monitoring arrangements wherever possible, although coordination of these wider monitoring and evaluation arrangements may be entrusted to other key partners.

3. There will be **informal contact** between the Scottish Government and public bodies at working level throughout the period of implementation of this action plan, to gauge progress and offer support where required. A **formal request** will be made at Board/Senior Management level to all Scottish public bodies at **end June 2018** to provide **one-off written updates,** setting out progress on implementing the following key requirements under this action plan:

- Confirmation of (i) having undergone a Cyber Essentials pre-assessment, (ii) having taken a decision on whether to seek Cyber Essentials or Cyber Essentials Plus, and (iii) the expected timelines for achieving this.[32]
- Board/Senior Management – level commitment and basic governance arrangements in place.
- CiSP membership in place.
- Appropriate implementation of Active Cyber Defence measures in place.
- Appropriate training and awareness raising processes in place.
- Cyber incident response protocols in place, aligned with central mechanisms.

4. A **further formal request** will be made at Board/Senior Management level to all Scottish public bodies at **end October 2018** to provide confirmation that **Cyber Essentials or Cyber Essentials Plus certification** has been achieved.

[32] As noted in the action plan, it is possible that, in exceptional cases and for some particularly complex public bodies, the pre-assessment will make clear that Cyber Essentials or Cyber Essentials Plus is not an appropriate standard to work towards. It is also possible that, as the process of undergoing Cyber Essentials/Plus pre-assessments or certification for public bodies proceeds, wider issues or challenges in the operation of the scheme will be identified. Where this is the case, public bodies will be encouraged to raise this with the Scottish Government Cyber Resilience Unit who will draw these issues to the attention of the NCSC, and alternatives to Cyber Essentials may be considered.

5. Appropriate information on progress will be made available to the public, Ministers, Parliament and the NCRLB, with due regard to cyber security considerations.

B. Development of ongoing monitoring and evaluation arrangements for target and advanced stages under Scottish Public Sector Cyber Resilience Framework

6. Monitoring and evaluation processes to support the implementation of the Scottish Public Sector Cyber Resilience Framework will be developed in tandem with the Framework. They will be designed to take account of, and align with, the requirements of the new competent authority or competent authorities that will be introduced to oversee compliance with the requirements of the EU NIS Directive, as well as those of Scottish Ministers and the National Cyber Resilience Leaders' Board. They will also ensure alignment with, and support for, existing arrangements in respect of Critical Infrastructure.

7. There will be an initial focus on evaluating how the **Public Sector Cyber Catalysts** are progressing towards the target and advanced progression levels of cyber resilience against this framework. However, the Scottish Government will also explore the potential for the development of a **self-assessment and reporting tool** that could assist all Scottish public sector organisations to assess and report against the Framework. The aim of this tool would be to:

- Assist Scottish public sector organisations to **self-assess** their progress against the initial baseline, target and advanced progression stages under the Framework in a standardised way, including against a simplified RAG status.
- **Minimise additional reporting and compliance burdens** by making clear the links between other standards, requirements or guidelines, and assisting in "translating" these into a self-assessment against the Framework. For example, where public bodies hold Cyber Essentials Plus, it may be assumed that this would provide a "green" RAG status in respect of certain criteria set out in the framework. Where public bodies are on the SCOTs[33] or other shared networks, it would be assumed that the standards achieved by providers of those networks apply to those connected to them.
- Produce **standardised reports** for submission to the Competent Authority/Authorities and Scottish Ministers on a mandatory (in the case of NIS operators of essential services) or voluntary (for all other organisations) basis.

8. In considering the feasibility of this self-assessment tool, the Scottish Government will work closely with the NCSC to build on a proposed Cyber Assessment Framework currently in development to support the NIS requirements. Subject to the successful development of the tool, consideration will be given to extending the requirement to report progress against the Framework to all Scottish public bodies in due course.

9. An indicative version of a monitoring and evaluation framework for the target and advanced stages of the Framework is set out below. This will be updated as the Framework is finalised and details of the NIS requirements become clear.

[33] The SCOTS network is the Scottish Government's IT network. A range of non-core Scottish Government Scottish public bodies also connect to the network.

Draft Monitoring and Evaluation Framework for Scottish Public Sector Cyber Resilience Framework (Official Sensitive when completed) (indicative)

Legend
▨ Status unknown/ no information available/not applicable
🟥 No significant progress made towards progression stage
🟨 Work underway/ some progress made towards progression stage
🟩 Progression stage achieved (and confirmed by audit or independent accreditation)

Organisation Working to progression stage: 🟦 = Advanced 🟪 = Target 🟪 = Init. baseline	Governance	Risk management	Asset Management	Supply Chain	Service protection policies and processes	Identity Access and Control	Data security	System security	Resilient Networks and Systems	Staff training and awareness	Security monitoring	Anomaly detection	Response and recovery planning	Improvements	Overall
	IDENTIFY				PROTECT						DETECT		RESPOND AND RECOVER		
1. AN Other (example)	🟨	🟨	🟨	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟥	▨
2. TBC	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
3. TBC	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
4. TBC	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
5. TBC	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
6. TBC	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
7. TBC	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
8. TBC	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
9. TBC	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
10. TBC	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨

Annex D. Outline of Scottish Government Security Awareness, Training and Education Programme

1. This annex sets out details of the Scottish Government's Security Awareness, Training and Education Programme. Products developed under this programme will be adapted and made available for general use by the wider Scottish public sector.

2. The Scottish Government is in the process of developing a new Corporate Security Awareness, Training and Education programme – "Security Action for Everyone" (SAFE) – which will improve all aspects of security behaviours by engaging with staff to develop a culture of security awareness which will reduce the likelihood of a successful physical or online attack.

3. The scope of the SAFE programme has evolved from a purely cyber awareness, training and education programme to a broader security behavioural change programme that now includes cyber, IT, physical, personnel and counter terrorism. This change in focus follows conversations with exemplar organisations. As the Centre for the Protection of National Infrastructure states: *"Effective protective security requires the integration of physical, personnel and people, and cyber security measures."*

4. The main objectives of the SAFE Programme are:

- Compliance with data protection regulations, Code of Conduct, IT Security Policy.
- Ensure employees understand and comply with policies, processes, and procedures.
- Identify top seven human risks to the Scottish Government and reduce those risks.
- Improve incident response by enabling employees to identify and report an incident.
- Implement metrics activities to track and report on the impact of the programme.

5. The SAFE programme will focus on **7 themes**, with clearly defined key messages using a range of activities including primary online training and reinforcement activities such as events, webcasts, screensavers, corporate communications and phishing exercises. These themes are:

- Access – Passwords and Passes
- Phishing and Social Engineering
- You're a target!
- Clear workspace
- Remote working
- Privacy
- Report it!

6. The SG Security ATE Programme begins content development in Autumn 2017 and roll-out of the programme in 2018/19.

7. *For more information on this project please contact:* SG Cyber Resilience Unit: cyberresilience@gov.scot

Annex E. List of Scottish Public Sector Cyber Catalysts

The following organisations have agreed to participate in the Public Sector Cyber Catalyst scheme.

- Aberdeenshire Council
- City of Edinburgh Council
- Disclosure Scotland
- Dumfries and Galloway Council
- Fife College
- Forth Valley College
- Independent Living Fund Scotland
- NHS Lanarkshire
- NHS Lothian
- Police Scotland
- Revenue Scotland
- Scottish Ambulance Service
- Scottish Canals
- Scottish Enterprise/ Skills Development Scotland/Highlands and Islands Enterprise
- Scottish Environment Protection Agency
- Scottish Fire and Rescue Service
- Scottish Government
- Scottish Public Pensions Agency
- Scottish Water
- Student Awards Agency Scotland
- Transport Scotland
- University of Aberdeen
- University of Edinburgh
- University of St Andrews
- VisitScotland
- West Lothian Council

Membership of the Cyber Catalyst scheme may be expanded or amended in the future as work progresses.

Scottish Government
Riaghaltas na h-Alba
gov.scot

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: 978-1-78851-400-2

Published by The Scottish Government, November 2017

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS315426 (11/17)