Scottish Public-Sector Action Plan 2017–18:

Summary and compliance guidance

December 2017

Protect • Comply • Thrive

Scottish Public-Sector Action Plan 2017–18

Introduction

A Cyber Resilience Strategy for Scotland: Public Sector Action Plan 2017–18[1] was developed by the Scottish government and the National Cyber Resilience Leaders' Board (NCRLB) to enhance the cyber resilience of digital public services in Scotland by the end of 2018, in line with outcome (iii) of the Scottish government's strategy for cyber resilience: "We have confidence in, and trust, our digital public services."[2]

The action plan requires Scottish public bodies (listed in Appendix 2 to this paper) and their 'key partners' to take a number of 'key actions' to improve their resilience to cyber attacks. These are summarised below, with compliance guidance informed by the implementation toolkit[3] published by the Scottish government in November 2017, and useful background information where relevant.

The importance of cyber resilience to Scotland's public bodies

Cyber resilience encompasses cyber security and business resilience, and aims not only to defend against potential attacks but also to ensure organisations' survival following any successful attack.

Public services in Scotland are increasingly being provided online and the country also relies on networked technologies to run critical infrastructure. Protecting the public sector's digital networks and infrastructure, and ensuring they are resilient to cyber attacks is essential to Scotland's prosperity and reputation.

The Cyber Resilience Strategy for Scotland states that:

"The Scottish Government is committed to implementing cyber resilience arrangements within its own systems with the aim of building trust with citizens and businesses and working in partnership with the public sector, to develop cyber resilience across all our public services as part of a shared responsibility."

Key actions for public bodies

The key actions that the Scottish government, public bodies and key partners must take are:

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

Key action 1: Scottish public-sector cyber resilience framework
The Scottish government will work with the NCRLB, the National Cyber Security Centre (NCSC), the Scottish public-sector cyber catalysts (see key action 10, below) and other key partners to develop a cyber resilience framework for Scottish public bodies by the end of June 2018. (More information on the framework can be found below.)

B. Initial baseline cyber resilience requirements for Scottish public bodies

Key action 2: Governance
All Scottish public bodies must have minimum cyber risk governance arrangements in place by the end of June 2018.

These should include:

- A named board or senior management member who is responsible for organisational cyber resilience arrangements;
- Regular board or senior management consideration of cyber threats and the arrangements the organisation has in place to manage relevant risks; and
- Appropriate cyber resilience policies and processes.

Key action 3: CiSP membership

All Scottish public bodies that manage their own networks must become active members of the NCSC's Cyber Security Information Sharing Partnership (CiSP)[4] by the end of June 2018.

CiSP members receive cyber threat and vulnerability information, and can exchange information on threats and vulnerabilities as they occur. The platform is funded by the UK government through the National Cyber Security Programme.

CiSP has also set up a number of regional groups to help organisations share threat and vulnerability information locally. Scottish organisations are encouraged to join the Scottish Cyber Information Network (SCiNET)[5] on CiSP.

Key action 4: Appropriate independent assurance of critical controls (Cyber Essentials certification)

Cyber Essentials is a UK government-backed certification scheme that sets out five cyber security controls that all organisations can implement to establish a baseline of cyber security. There are two levels of certification available: Cyber Essentials or Cyber Essentials Plus. More information about the scheme can be found below.

All Scottish public bodies must undergo Cyber Essentials 'pre-assessments' by the end of March 2018, for which grants of up to £1,000 will be made available by the Scottish government.

Boards/senior management must decide whether to pursue certification to Cyber Essentials or Cyber Essentials Plus by the end of April 2018, and certification must be achieved by the end of October 2018.

In some instances, the Cyber Essentials scheme may not be an appropriate standard to work towards. Where Scottish public bodies believe this to be the case, they are asked to contact the Scottish government's Cyber Resilience Unit (CRU).

Key action 5: Active Cyber Defence (ACD) measures

All Scottish public bodies must implement the NCSC's four ACD measures[6] by the end of June 2018.

These are:

- **Protected DNS**
  Public bodies should register at https://nominet.service-now.com/csm.
- **DMARC anti-spoofing**
  Public bodies should email dmarc@ncsc.gov.uk for further details.
- **Web Check**
  Public bodies should register at www.webcheck.service.ncsc.gov.uk and quote the reference 'wbchk04/7'.
- **Phishing and malware mitigation**
  Public bodies should implement a process to forward suspicious emails and their attachments to scam@netcraft.com. Similarly, if a public body discovers a clone of one of its websites or online services, it should use the same email address to notify Netcraft of the URL of the offending site. Netcraft will take action to take down the offending sites in both instances.

Key action 6: Training and awareness raising

All Scottish public bodies must have appropriate cyber resilience training in place by the end of June 2018.

This must cover:

- Boards, senior executives and their support functions;
- Managers;
- Security-focused staff, including cyber security and front-of-house;
- Specialist staff, including IT, finance, legal and procurement;
- Privileged users; and
- All staff in policy and delivery roles.

Public bodies that are subject to the Scottish Public Finance Manual (SPFM) should already have such arrangements in place.

Key action 7: Incident response
All Scottish public bodies must have appropriate cyber incident response plans in place by the end of June 2018.

The Scottish government will develop and disseminate the following resources by the end of 2017:

- Guidance on central incident response coordination and reporting protocols that clarify how public bodies should report significant cyber threat incidents.
- A template incident response plan for public bodies.

Public bodies should ensure their plans align with the central incident reporting and coordination mechanisms.

C. Cyber security of supply chain and grant recipients

Key action 8
The Scottish government will seek industry guidance on, and draft a policy for, supply chain security that aligns with the General Data Protection Regulation (GDPR), which will be applied by public bodies as part of their procurement processes.

It will also develop guidance on the need for public grant funding recipients to have proportionate and risk-based cyber security arrangements in place.

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

Key action 9
The Scottish government will put in place a dynamic purchasing system for digital services[7] (including cyber security) by the end of October 2017.

E. Leadership and knowledge sharing

Key action 10
The Scottish government will coordinate a public-sector catalyst scheme by the end of June 2018, under which a number of bodies will commit to becoming 'cyber catalysts' – exemplars of cyber resilience – and sharing their knowledge with the wider public sector.

F. Monitoring and evaluation

Key action 11: Monitoring and evaluation
The Scottish government will put in place a monitoring and evaluation framework by the end of June 2018 to assess public bodies' compliance with the action plan.

The Scottish government will formally seek information from public bodies' boards/senior management in line with the following deadlines.

Deadlines for public bodies

Key action	Information required	Deadline
2	• Confirmation that your public body has minimum governance requirements in place.	End of June 2018
3	• Confirmation that your public body manages its own network and has become a member of CiSP; or • Confirmation that your public body does not manage its own network and therefore does not need to become a member of CiSP.	End of June 2018
4	• Confirmation that your public body has undergone a Cyber Essentials pre-assessment, that the report has been shared with the board/senior management, and that a decision has been made on whether to seek Cyber Essentials or Cyber Essentials Plus certification. • If you have opted for Cyber Essentials rather than Cyber Essentials Plus certification, confirmation of your reasons, with reference to existing accreditations that provide independent assurance. • Confirmation that certification to the Cyber Essentials scheme at either level has been achieved (or, if there are legitimate reasons for a delay, confirmation that plans are in place to achieve certification), with information on the scope of the certification and any plans for extending the scope in future.	End of June 2018 End of June 2018 End of October 2018
5	• Confirmation that you are aware of the NCSC's ACD programme, have assessed its relevance to your public body and are making appropriate use of it. If you are not using it, your reasons will be requested.	End of June 2018
6	• Confirmation that you have appropriate cyber resilience training and awareness-raising policies and processes in place, and details of what they are.	End of June 2018
7	• Confirmation that you have appropriate cyber incident response plans in place and that they align with central incident reporting and coordination mechanisms.	End of June 2018

Compliance obligations, including the GDPR and NIS Directive

Scottish public bodies must currently comply with a wide range of information security and cyber resilience requirements, and legislative changes are being introduced in the coming months that will complicate the already complex compliance environment even further.

The GDPR

Data protection law forms a significant part of those changes. If a public body processes personal data, it is currently subject to the UK Data Protection Act 1998 (DPA) and is liable for fines of up to £500,000 from the Information Commissioner's Office (ICO) for breaches of the law's eight data protection principles.

The EU GDPR will supersede the 1995 Data Protection Directive and all domestic legislation based on it, including the DPA, on 25 May 2018. The UK government will enact the GDPR's provisions as part of a new Data Protection Bill, which will apply in Scotland just as the current DPA does.

The GDPR marks a significant increase in responsibility for all Scottish public bodies that process personal data: it substantially extends the data rights of individuals, and requires data controllers and processors to implement appropriate and proportionate technical and organisational measures to protect personal data.

Moreover, the new law is backed by a regime of considerably higher penalties than the DPA – the greater of €20 million (£18 million) or 4% of annual global turnover – and grants aggrieved data subjects the right, under certain circumstances, to bring proceedings against organisations for failing to secure their personal data properly.

The NIS Directive

Another important law due to come into effect on 25 May 2018 is the EU's Directive on Security of Network and Information Systems (NIS Directive), which applies to digital service providers and operators of essential services in the energy, transport, banking, financial market infrastructures, health, water, and digital infrastructure sectors.

The NIS Directive requires organisations to implement appropriate and proportionate technical and organisational measures to mitigate the security risks their networks face, and carries a similar penalty regime to the GDPR.

The consultation on the UK government's plan to implement the NIS Directive closed on 30 September 2017.[8] The legislation that will enact the Directive in the UK is yet to be published.

Minimising the compliance burden

The action plan recognises that it is untenable to expect all Scottish bodies to comply with such a variety of complex requirements, so the Scottish government will work with the NCRLB, the NCSC, the Scottish public-sector catalysts (see key action 10, above) and others to minimise the burden by developing a cyber resilience framework for Scottish public bodies by the end of June 2018 in order to provide a common, effective, risk-based approach that Scottish public bodies can use to assess and approve their cyber resilience (see key action 1, above).

Scottish public-sector cyber resilience framework

The Scottish public-sector cyber resilience framework will align with the requirements of the NIS Directive and other measures, including the new Technology Security Standard that will be introduced by the UK government under the Security Policy Framework by the end of 2017 to establish a baseline of cyber security across UK government departments (see **Other relevant guidelines and standards**, below).

The framework will cover the four key domains of cyber resilience:

- **Identify (governance and risk management)**
  Appropriate organisational structures, policies and processes should be 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; and
    - Supply chain risk management.

  Key action 3 will apply.

- **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; and
    - Staff awareness and training.

  Key actions 4, 5 and 6 will apply.

- **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; and
    - Anomaly detection.

- **Respond and recover**
  Capabilities should be in place to minimise the impact 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.

  Key action 7 will apply.

Within these four domains, the framework proposes three progression stages, which all Scottish public bodies will be expected to work towards on a risk-based and proportionate basis:

- **Initial baseline**
  These will be the minimum requirements all Scottish public bodies will be expected to meet by the end of June 2018, or, in the case of Cyber Essentials certification or independent assurance of critical controls, October 2018.

  Key actions 2 to 7 set out how Scottish public bodies can progress towards meeting this stage.

- **Target**
  All Scottish public bodies will be expected to work towards meeting these requirements on a risk-based and proportionate basis. They will be aligned with the new Technology Security Standard and other existing standards and guidelines.

- **Advanced**
  These requirements will align with the NIS Directive and will apply automatically to public bodies in the health and water sectors. However, the Scottish government will also encourage other public bodies in the critical national infrastructure sector to work towards achieving them.

Until the framework is finalised – which will not be possible until the UK government publishes the legislation that will enact the NIS Directive in the UK – Scottish public bodies that are not working to advanced guidelines or standards can refer to the NCSC's 10 Steps to Cyber Security.

These guidelines and standards, including the 10 Steps to Cyber Security, are summarised below. The differences and overlap between them should show why there is a need for a single approach across the entire public sector in Scotland.

The Cyber Essentials scheme

All Scottish public bodies must achieve certification to the Cyber Essentials scheme by the end of October 2018. Cyber Essentials was developed by the UK government to provide five cyber security controls that all organisations can implement to achieve a baseline of cyber security.

The UK government estimates that these five controls can help prevent "around 80% of cyber attacks":

- **Secure configuration**
  This refers to security measures that are implemented when building and installing computers and network devices.

- **Boundary firewalls and Internet gateways**
  These provide a basic level of protection where a user connects to the Internet. Although antivirus software helps to protect the system against unwanted programs, a firewall helps to keep attackers or external threats from getting access to your system in the first place. The firewall monitors all network traffic and has the ability to identify and block unwanted traffic that could be harmful to your computer, systems and networks.

- **Access control**
  Protecting user accounts and helping prevent misuse of privileged accounts is essential. User accounts, particularly those with special access privileges (e.g. administrative accounts) should be assigned only to authorised individuals and managed effectively, and provide the minimum level of access to applications, computers and networks.

- **Malware protection**
  Protecting against a broad range of malware – including computer viruses, worms, spyware, botnet software and ransomware – will protect your machines, your privacy and your electronic records from attack.

- **Patch management**
  Cyber criminals can take advantage of known vulnerabilities in operating systems and third-party applications if they are not properly patched or updated. Patch management is about keeping software on computers and network devices up to date and capable of resisting low-level cyber attacks.

Cyber Essentials certification levels
There are two levels of certification to the scheme: Cyber Essentials and Cyber Essentials Plus.

- **Cyber Essentials**
  Cyber Essentials certification includes a self-assessment questionnaire (SAQ) and an external vulnerability scan that independently verifies your security status.

- **Cyber Essentials Plus**
  Cyber Essentials Plus certification includes all the assessments for the Cyber Essentials certification but

includes an additional internal scan and an on-site assessment.

More information about the scheme can be found on IT Governance's website.[9]

Other relevant guidelines and standards

Other relevant guidelines and standards include:

- **The Scottish Public Finance Manual (SPFM)**
  The SPFM provides guidance on the proper handling and reporting of public funds, and includes provisions on risk management, accountability, governance statements, certificates of assurance and internal control checklists, and best value, which should effectively mean that Scottish public bodies subject to the SPFM already meet robust standards for cyber resilience. The SPFM will be revised in due course to clarify how the requirements developed under the action plan apply to bodies subject to the SPFM. All such public bodies will then be required to provide assurance that they are adopting the practice set out in the action plan.

- **The Security Policy Framework**
  The Scottish government has so far aligned its approach to security with the UK government's Security Policy Framework (SPF). The UK government has indicated its intention to introduce a new mandatory Technology Security Standard under the SPF before the end of 2017. This new cyber security standard will, once implemented, establish a baseline level of cyber security across UK government departments.

- **International standards for cyber resilience**

  ISO/IEC 27001:2013
  The international standard for information security management, ISO/IEC 27001:2013 (ISO 27001), alongside its code of practice ISO/IEC 27002:2013 (ISO 27002), sets out the requirements of an information security management system (ISMS), an organisational approach to information security that encompasses people, processes and technology. Organisations can achieve independently audited certification to the Standard to demonstrate that they are following international best practice. In terms of cyber security maturity, ISO 27001 certification offers a greater level of assurance than Cyber Essentials certification.

  ISO 22301:2012
  The international standard for business continuity, ISO 22301:2012 (ISO 22301), sets out the requirements for a business continuity management system (BCMS), a comprehensive approach to organisational resilience that helps organisations update, control and deploy effective plans, taking into account organisational contingencies, capabilities and requirements.

  Integrated management system
  An integrated management system that combines an ISO 27001-compliant ISMS and an ISO 22301-compliant BCMS provides a best-practice approach to cyber resilience that is recognised the world over.

  Organisations can also integrate other standards as relevant, such as:

- **ISO/IEC 27031:2011** (ISO 27031), which describes the concepts and principles of information and communication technology (ICT) readiness for business continuity.

- **ISO/IEC 27032:2012** (ISO 27032), which provides guidance for improving cyber security, with particular regard to information security, network security, Internet security and critical information infrastructure protection.

- **ISO/IEC 27035-1:2016** and **ISO/IEC 27035-2:2016** (ISO 27035), which provide guidance on information security incident management.

- **The Payment Card Industry Data Security Standard (PCI DSS)**
  All organisations that process card payments must comply with the PCI DSS – a set of 12 requirements for keeping cardholder data secure:

  1. Install and maintain a firewall configuration to protect cardholder data
  2. Do not use vendor-supplied defaults for system passwords and other security parameters
  3. Protect stored cardholder data
  4. Encrypt transmission of cardholder data across open, public networks
  5. Protect all systems against malware and regularly update anti-virus software or programs
  6. Develop and maintain secure systems and applications
  7. Restrict access to cardholder data by business need to know
  8. Identify and authenticate access to system components
  9. Restrict physical access to cardholder data
  10. Track and monitor all access to network resources and cardholder data
  11. Regularly test security systems and processes
  12. Maintain a policy that addresses information security for all personnel

- **20 Critical Security Controls**
  Published by the Center for Internet Security (CIS) and supported by the SANS Institute, the US government's CIS Critical Security Controls[10] provide "specific and actionable ways to stop today's most pervasive and dangerous attacks […] derived from the most common attack patterns highlighted in the leading threat reports and vetted across a broad community of government and industry practitioners".[11]

  The controls are:

  1. Inventory of Authorized and Unauthorized Devices
  2. Inventory of Authorized and Unauthorized Software
  3. Secure Configurations for Hardware and Software
  4. Continuous Vulnerability Assessment and Remediation
  5. Controlled Use of Administrative Privileges
  6. Maintenance, Monitoring, and Analysis of Audit Logs
  7. Email and Web Browser Protections
  8. Malware Defenses
  9. Limitation and Control of Network Ports
  10. Data Recovery Capability
  11. Secure Configurations for Network Devices
  12. Boundary Defense
  13. Data Protection
  14. Controlled Access Based on the Need to Know

15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment and Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

- **NCSC 10 Steps to Cyber Security**
  The NCSC's 10 Steps to Cyber Security[12] comprise an organisational risk management regime and nine steps that support it. They encompass, and expand on, the five controls of the Cyber Essentials scheme and are contained in the information security management system standard ISO 27001:2013.

  The ten steps are:

  - Risk management regime
  - Secure configuration
  - Network security
  - Managing user privileges
  - User education and awareness
  - Incident management
  - Malware prevention
  - Monitoring
  - Removable media controls
  - Home and mobile working

Complete cyber resilience solutions

IT Governance is an information security, governance, risk management and compliance specialist, with more than a decade's experience helping organisations of all sectors and sizes all over the world.

We provide a complete solution for attaining cyber resilience, including books, standards, documentation toolkits, software, training, consultancy and technical services.

We are a Lot 3 (Cyber Security Services) supplier under the Scottish government's Dynamic Purchasing System for Digital Services.[13]

Here are some of the ways we can help your public body increase its cyber resilience.

Cyber Essentials certification

IT Governance is the leading CREST-accredited Cyber Essentials certification body, and has certified hundreds of organisations to the scheme, including Vodafone, Airbus Defence and Space Ltd, Action for Children, NHS Professionals, and Lockheed Martin.

We can help with all aspects of your Cyber Essentials project, from initial scoping to pre-assessment:

- You can conduct the entire certification process online, without any expert cyber security knowledge, with our Cyber Essentials portal.
- We provide all the tools and resources you need to achieve CREST-accredited certification to either level of the Cyber Essentials scheme.
- Our experienced, CREST-accredited testers deliver all the technical tests and assessments: we do not outsource any of the services required to achieve certification.
- As we are a CREST-accredited certification body, you will benefit from the added level of independent verification of your cyber security status provided by an external vulnerability scan.
- We have six packaged solutions available to support companies with varying levels of experience through the Cyber Essentials or Cyber Essentials Plus certification process.
- We have led ISO 27001 implementations since the inception of the standard, and our strong global cyber security presence gives us the knowledge and insight to help progress beyond Cyber Essentials.

Cyber resilience consultancy

Drawing on our unique blend of practical information security know-how and proven management system consultancy expertise, our team can help your public body implement an integrated management system that combines the international standards ISO 27001 and ISO 22301.

- **Cyber resilient management system**

  IT Governance's experienced consultants can help your organisation implement an effective cyber resilience posture, supported by the universally accepted international standards on information security management (ISO 27001) and business continuity

management (ISO 22301). Following a comprehensive approach to cyber resilience, our unique combination of technical expertise and solid track record in international management system standards means we can deliver a complete solution and manage the project from start to finish. View our cyber resilience information page for more.

- **Cyber Incident Response Management**
  Cyber incident response (CIR) management can help your organisation reduce the risk of information security incidents. The purpose of CIR is to manage and respond to unexpected, disruptive events with the objective of controlling the impact within acceptable levels. We are a leader in the field of providing CIR management action plans. Our CIR service is listed in the government's Digital Marketplace as official Crown Commercial Suppliers.

- **ISO 27001 consultancy**
  Backed by the management team that led the implementation of the world's first ISO 27001-compliant ISMS, we have helped more than 400 companies achieve certification to ISO 27001.

  In addition to our bespoke ISO 27001 consultancy service, we offer a range of fixed-price services to meet any of your implementation requirements. For organisations wishing to pursue accredited certification, we provide a 100% certification guarantee.

- **ISO 22301 consultancy**
  Our business continuity management team provides a comprehensive solution to implementing an effective BCMS based on the international standard ISO 22301.

  Our experts will save you hours of uncertainty, and trial and error, by providing you with the core competence and skills you need in order to implement business continuity best practice as cost-effectively as possible.

Documentation toolkits

Creating documentation for your management system is never easy, and can run to hundreds of pages. IT Governance's documentation toolkits contain fully customisable templates that have been written by our consultants to comply with international standards:

- **Cyber Resilience Documentation Toolkit**
  The Cyber Resilience Documentation Toolkit provides you with a comprehensive set of pre-written information security and business continuity policies, procedures, tools and templates that comply with leading international standards ISO 27001 and ISO 22301. The toolkit includes expert guidance and helpful project tools and resources to deploy a management system optimised for cyber resilience, including scope statements, implementation checklists, a management dashboard, a project management plan, a task manager and more.

Training

IT Governance's training programme is built on the foundations of our extensive practical experience designing and implementing management systems. Our training courses offer a structured learning path from Foundation to Advanced level for IT practitioners and lead implementers, and help to develop the skills needed to deliver best practice and compliance in any organisation.

- The Cyber Resilience Training Course provides a comprehensive approach to implementing an integrated cyber resilience management system that helps protect, respond and recover from cyber attacks.

- The ISO 27001 learning pathway will equip you with the knowledge and skills required to plan, implement, maintain and audit a best-practice ISMS in your organisation.

- The ISO 22301 learning pathway provides you with the knowledge and skills to implement and audit an ISO 22301-compliant BCMS.

- The Incident Response Management Foundation Training Course helps you manage and respond to a disruptive incident and take appropriate steps to limit the damage of a disruption to network availability and information security.

Attendees who pass the examinations will be awarded international qualifications accredited by GASQ and the International Board for IT Governance Qualifications (IBITGQ).

Penetration testing

Penetration testing is the most effective way of demonstrating that exploitable vulnerabilities in your company's Internet-facing applications and infrastructure have been identified, allowing appropriate mitigation to be applied.

IT Governance is a CREST member company, meaning that clients can rest assured that our penetration tests will be carried out to the highest standards by qualified and knowledgeable individuals.

International standards

- **Cyber Resilience Core Standards Kit**

  This kit includes the critical standards for cyber resilience:
- **ISO/IEC 27001:2013**
  The international standard for an ISMS.

- **ISO/IEC 27002:2013**
  Guidance on implementing an ISO 27001-compliant ISMS.

- **ISO 22301:2012**
  The international standard for a BCMS.

- **ISO 22313:2012**
  Guidance on implementing a BCMS.

Contact us: +44 (0)333 800 7000

www.itgovernance.co.uk servicecentre@itgovernance.co.uk

Appendix 1: Deadlines for public bodies, ordered by date

End of March 2018	• Undergo Cyber Essentials pre-assessment.
End of April 2018	• Decide whether to pursue certification to Cyber Essentials or Cyber Essentials Plus.
End of June 2018	• Have minimum cyber risk governance arrangements in place. • Become an active member of the NCSC's CiSP (only public bodies that manage their own networks – those that do not should confirm they do not). • Confirm a Cyber Essentials pre-assessment has taken place, that the report has been shared with senior management and that a decision has been made about whether to pursue certification to Cyber Essentials or Cyber Essentials Plus. Reasons for the decision to pursue Cyber Essentials rather than Cyber Essentials Plus must be provided. • Implement the NCSC's ACD programme or provide reasons if it is inappropriate to use it. • Have appropriate cyber resilience training in place. • Have appropriate cyber incident response plans in place.
End of October 2018	• Achieve certification to Cyber Essentials or Cyber Essentials Plus.

Appendix 2: Scottish public bodies and wider Scottish public-sector organisations

Scottish public bodies

The following public bodies are expected to align their approach to cyber resilience with the action plan.

Executive agencies (7):

- Accountant in Bankruptcy
- Disclosure Scotland
- Education Scotland
- Scottish Prison Service
- Scottish Public Pensions Agency
- Student Awards Agency for Scotland
- Transport Scotland

Non-ministerial departments (8):

- Food Standards Scotland
- National Records of Scotland
- Office of the Scottish Charity Regulator
- Registers of Scotland
- Revenue Scotland
- Scottish Courts and Tribunals Service
- Scottish Fiscal Commission
- Scottish Housing Regulator

Public corporations (5):

- Caledonian Maritime Assets Ltd
- Glasgow Prestwick Airport
- Scottish Canals
- Scottish Water
- The Crown Estate Scotland – Interim Management

Executive NDPBs (38):

- Accounts Commission for Scotland
- Architecture and Design Scotland
- Bòrd na Gàidhlig
- Cairngorms National Park Authority
- Care Inspectorate
- Children's Hearings Scotland
- Community Justice Scotland
- Creative Scotland
- Crofting Commission
- David MacBrayne Ltd
- Highlands and Islands Airports Ltd
- Highlands and Islands Enterprise
- Historic Environment Scotland
- Loch Lomond and The Trossachs National Park Authority
- National Galleries of Scotland
- National Library of Scotland
- National Museums of Scotland
- Police Investigations and Review Commissioner
- Quality Meat Scotland

- Risk Management Authority
- Royal Botanic Garden, Edinburgh
- Scottish Agricultural Wages Board
- Scottish Children's Reporter Administration
- Scottish Criminal Cases Review Commission
- Scottish Enterprise
- Scottish Environment Protection Agency
- Scottish Funding Council
- Scottish Futures Trust
- Scottish Land Commission
- Scottish Legal Aid Board
- Scottish Legal Complaints Commission
- Scottish Natural Heritage
- Scottish Qualifications Authority
- Scottish Social Services Council
- Skills Development Scotland
- Sportscotland
- VisitScotland
- Water Industry Commission for Scotland

Health bodies (23):

- Healthcare Improvement Scotland
- Mental Welfare Commission for Scotland
- NHS 24
- NHS boards (14 bodies)
- NHS Education for Scotland
- NHS Health Scotland Board
- NHS National Services Scotland
- National Waiting Times Centre Board
- Scottish Ambulance Service Board
- State Hospital Board for Scotland

Advisory NDPBs (5):

- Judicial Appointments Board for Scotland
- Local Government Boundary Commission for Scotland
- Mobility and Access Committee for Scotland
- Scottish Advisory Committee on Distinction Awards
- Scottish Law Commission

The Scottish Parliament

Parliamentary Commissioners and Ombudsmen (6):

- Children & Young Peoples Commissioner Scotland
- Commissioner for Ethical Standards in Public Life in Scotland
- Scottish Human Rights Commission
- Scottish Information Commissioner
- Scottish Public Services Ombudsman
- Standards Commission for Scotland

Other significant bodies (18):

- Scottish Fire and Rescue Service
- Scottish Police Authority
- Independent Living Fund Scotland

- Audit Scotland
- Convener of School Closure Review Panels
- Court of Lord Lyon
- Drinking Water Quality Regulator
- HM Inspector of Constabulary in Scotland
- HM Chief Inspector of Prisons in Scotland
- HM Chief Inspector of Prosecution in Scotland
- Justices of the Peace Advisory Committee (6 bodies)
- Office of the Queens Printer for Scotland
- Scottish Road Works Commissioner

Wider Scottish public-sector organisations

The Scottish government will work with central coordinating bodies to help the following organisations implement the action plan where possible, recognising that certain bespoke arrangements may be needed to meet specific sectoral challenges.

Local authorities (32):

- Aberdeen City Council
- Aberdeenshire Council
- Angus Council
- Argyll and Bute Council
- City of Edinburgh Council
- Clackmannanshire Council
- Comhairle nan Eilean Siar
- Dumfries and Galloway Council
- Dundee City Council
- East Ayrshire Council
- East Dunbartonshire Council
- East Lothian Council
- East Renfrewshire Council
- Falkirk Council
- Fife Council
- Glasgow City Council
- Inverclyde Council
- Midlothian Council
- North Ayrshire Council
- North Lanarkshire Council
- Orkney Islands Council
- Perth and Kinross Council
- Renfrewshire Council
- Scottish Borders Council
- Shetland Islands Council
- South Ayrshire Council
- South Lanarkshire Council
- Stirling Council
- The Highland Council
- The Moray Council
- West Dunbartonshire Council
- West Lothian Council

Scottish colleges and universities (43):

- Argyll College
- Ayrshire College

- Borders College
- City of Glasgow College
- Dumfries and Galloway College
- Dundee and Angus College
- Edinburgh College
- Fife College
- Forth Valley College
- Glasgow Clyde College
- Glasgow Kelvin College
- Inverness College
- Lews Castle College UHI
- Moray College UHI
- New College Lanarkshire
- Newbattle Abbey College
- North East Scotland College
- North Highland College UHI
- Orkney College UHI
- Perth College UHI
- Sabhal Mor Ostaig UHI
- Shetland College UHI
- South Lanarkshire College
- Scotland's Rural College
- West College Scotland
- West Highland College UHI
- West Lothian College
- Abertay University
- Edinburgh Napier University
- Glasgow School of Art
- Heriot-Watt University
- Open University in Scotland
- Queen Margaret University Edinburgh
- Robert Gordon University
- Royal Conservatoire of Scotland
- University of Aberdeen
- University of Edinburgh
- University of Glasgow
- University of the Highlands and Islands
- University of St Andrews
- University of Stirling
- University of Strathclyde
- University of the West of Scotland

References

[1] https://beta.gov.scot/publications/cyber-resilience-strategy-scotland-public-sector-action-plan-2017-18/documents/00527399.pdf?inline=true
[2] http://www.gov.scot/Resource/0048/00489206.pdf
[3] https://beta.gov.scot/publications/cyber-resilience-public-sector-toolkit/Cyber%20Res%20-%20Implementation%20Toolkit.pdf?inline=true
[4] https://www.ncsc.gov.uk/cisp

[5] http://sbcc.neighbourhoodalert.co.uk/pages/3668/1/SCiNET.html
[6] https://www.ncsc.gov.uk/blog-post/active-cyber-defence-tackling-cyber-attacks-uk
[7] http://www.gov.scot/Topics/Government/Procurement/directory/itms/DynamicPurchasingSystem
[8] https://www.gov.uk/government/consultations/consultation-on-the-security-of-network-and-information-systems-directive
[9] https://www.itgovernance.co.uk/cyber-essentials-scheme
[10] https://www.cisecurity.org/controls/
[11] https://www.sans.org/critical-security-controls/
[12] https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
[13] http://www.gov.scot/Topics/Government/Procurement/directory/itms/DynamicPurchasingSystem