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

IMPLEMENTATION TOOLKIT

Version 2 at MARCH 2018: Main updates to Annex C

This toolkit has been produced by the Scottish Government Cyber Resilience Unit to accompany the Public Sector Action Plan 2017/18

It is intended to be a live document and will be updated as new implementation guidance becomes available.

Please send all comments, questions or additions to cyberresilience@gov.scot

INTRODUCTION

1. This toolkit provides the key information that Scottish public sector organisations will need to implement the Scottish Public Sector Action Plan on Cyber Resilience. It attempts to make clear the steps that public bodies should take, and where they can find further expertise and advice, to ensure effective implementation.

2. **Annex A** provides information on the applicability of the action plan to public bodies and the wider public sector.

3. Public bodies with questions around implementation of the action plan that are not answered by the information set out in this toolkit should write to **cyberresilience@gov.scot** in the first instance, following which a member of one of the following areas will be in touch to discuss the issue:

    - the Scottish Government Cyber Resilience Unit;
    - the Scottish Government Digital Transformation Service;
    - the Scottish Government iTECS team;
    - Scottish Procurement; or
    - the National Cyber Security Centre (NCSC).

    Feedback is welcomed, and this toolkit will be updated regularly as required.

4. When public bodies have completed key actions, and have gained an understanding of process/challenges, etc. **the Cyber Resilience Unit would be very grateful if you could share any such learning with us**.

5. We will endeavour to support knowledge sharing with the wider public sector on the basis of any such feedback received, to help ensure the successful implementation of the plan. We have scheduled workshops, and will continue to host events, to address particular issues faced by public bodies when implementing the plan. We held an NCSC "Digital Loft" event in February 2018, which included workshops with technical experts, and will explore further partnership events with NCSC later in 2018. We will also explore whether more advanced public bodies can share expertise and advice with smaller public bodies as implementation progresses.

PREPARATORY ACTIONS

6. To assist with implementation and monitoring of the public sector action plan, all public bodies should send the following details to the Scottish Government Cyber Resilience Unit (cyberresilience@gov.scot) by **end November 2017**:

    - **Working level contacts** who will be responsible for day-to-day work to implement the action plan in your organisation and (if different) for **cyber incident response** issues, including receipt of early warning messages when public bodies are at risk of cyber-attack; and

    - A **Board/Senior Management-level contact** with overall responsibility for implementation of the action plan in your organisation.

KEY ACTION 1 Scottish Public Sector Cyber Resilience Framework

7. Key Action 1 commits the Scottish Government to working with key partners to develop and disseminate a **Cyber Resilience Framework** for Scottish public bodies by **end June 2018**.

8. **No immediate action** is required of Scottish public bodies in relation to this key action, other than the public sector cyber catalysts. The Scottish Government will work with the cyber catalysts to develop this framework by end June 2018.

9. Thereafter, the Scottish Government will write to Scottish public bodies to update them on any action required in respect of implementing the finalised framework.

KEY ACTION 2 Governance

10. Key Action 2 asks that public bodies ensure they have in place a **Board/Senior Management-level commitment** to manage the risks arising from the cyber threat. As part of this, they should ensure they have **minimum appropriate governance arrangements** in place by **end June 2018**. The action plan makes clear that this includes:

- 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 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.

11. More mature requirements around governance and risk management will be included in the finalised Scottish Public Sector Cyber Resilience Framework. Pending this, public bodies should strive to ensure that the effect of these governance arrangements is such that the Board/Senior Management of Scottish public bodies are enabled to answer the following key questions under the following themes[1]:

- **Protection of key information assets from cyber threats**

i. How confident are we that our organisation's most important information is being properly managed and is safe from cyber threats?
ii. Are we clear that the Board/Senior Management are likely to be key targets?
iii. Do we have a full and accurate picture of:

  - the impact on our organisation's reputation or existence if sensitive internal information (including citizens' information) held by us were to be lost or stolen?
  - the impact on our organisation if our online services were disrupted for a short or sustained period?

- **Exploring who might compromise our information and why**

iv. Do we receive regular intelligence from the Chief Information Officer/Head of Security/responsible individual on who may be targeting our organisation, their methods and their motivations?
v. Do we encourage our technical staff to enter into information-sharing exchanges with other public bodies in our sector and/or across the economy in order to benchmark, learn from others and help identify emerging threats? (NB: CiSP membership at Key Action 3 below).

- **Pro-active management of the cyber risk at Board/Senior Management level.** The cyber security risk impacts reputation, culture, staff, information, delivery of public services, technology, and finance. Are we confident that:

vi. we have identified our key information and IT assets and thoroughly assessed their vulnerability to cyber-attack?
vii. responsibility for the cyber risk has been allocated appropriately? Is it on the risk register?
viii. we have a written information security policy in place, which is championed by us and supported through regular staff training? Are we confident the entire workforce understands and follows it?

[1] Taken from "A Board Level Responsibility" under the 10 Steps to Cyber Security: https://www.ncsc.gov.uk/guidance/10-steps-board-level-responsibility

12. Public bodies can refer to the NCSC's risk management guidance collection or further insight on how to establish an effective risk management regime[2]. They may also wish to have reference to such resources as the IASME Governance standard self-assessment questionnaire when considering whether their risk management arrangements are appropriate.[3]

KEY ACTION 3 CiSP Membership

13. Key Action 3 asks that public bodies who are responsible for managing their own networks become active participants in the Cyber Security Information Sharing Partnership (CiSP) by **end June 2018**.

BACKGROUND

14. The cyber threat does not become a managed risk until it is understood. Good situational awareness is key to providing this understanding and managing this risk. CiSP is a joint industry and government scheme based in the National Cyber Security Centre (NCSC) designed to deliver situational awareness to its members and encourage the sharing of information on cyber risk to enable others to adopt appropriate mitigation.

15. CiSP is a secure social networking platform that enables its members to receive enriched cyber threat and vulnerability information and exchange information on threats and vulnerabilities as they occur in real time.

WHO IS CiSP FOR?

16. CiSP is funded by the UK Government through the National Cyber Security Programme and is offered as a free service and is primarily aimed at organisations who manage IT networks in the UK and individuals within the organisations who have some responsibility for managing threat or defending networks. Organisations should note that eligibility rules may exclude some regulatory bodies.

CiSP PRODUCTS

17. CiSP produces a wide range of products to cater for organisations at all levels of cyber maturity. These include, but are not limited to:

- Alerts and Advisories, including from national and international partners
- Best practice and guidance documents on common themes
- Quarterly Reports on threat trends
- Malware and phishing email analysis
- Incident Reporting.

CiSP BENEFITS

18. CiSP benefits include, but are not limited to:

- Engagement with industry and government counterparts in a secure environment
- Early warning of cyber threats
- Ability to learn from experiences, mistakes and successes of others and seek advice
- An improved ability to protect your organisation's network
- Access to subject or sector specific content - including vulnerabilities, latest incidents and exercising
- Access to free network reporting tools to help protect organisational security.
- Improved cyber situational awareness at no costs to your organisation.

SCOTTISH INFORMATION SHARING NETWORK (SCiNET GROUP)

19. CiSP has entered into a partnership with law enforcement agencies to set up regional groups for organisations to share threat and vulnerability information with other organisations in their region. The SCiNET has been set up as a community for Scottish Businesses to engage and share.

[2] https://www.ncsc.gov.uk/guidance/risk-management-collection

[3] https://www.iasme.co.uk/wp-content/uploads/2017/05/IASME-governance-and-Cyber-Essentials-questions-booklet-v10.6.pdf

APPLICATION PROCESS

20. The first applicant from a new organisation wishing to join the Cisp will require to be **sponsored** into this trust environment. Application is made online by visiting the NCSC website at https://www.ncsc.gov.uk/cisp and selecting 'Register your Organisation'. A simple online form is completed which will ask for the sponsor's details to be included. A check will be made with the sponsor that the organisation is known and meets the joining criteria. Thereafter all other members of the organisation make applications by selecting the 'Register yourself' option, which does not require sponsorship.

21. Graham Bye, Scottish CiSP Co-ordinator (graham.bye@sbrcentre.co.uk) and Keith McDevitt Scottish Government Cyber Resilience Unit (keith.mcdevitt@gov.scot) are moderators for the SCiNET group within Cisp and will act as organisational sponsors for the Scottish Public Sector. **Their names should therefore be provided in the application form at the appropriate section.**

22. Organisations wishing an overview of the CiSP and SCiNET are encouraged to contact Graham Bye at graham.bye@sbrcentre.co.uk.

KEY ACTION 4 Appropriate independent assurance of critical controls (Cyber Essentials certification)

23. Key Action 4 asks that public bodies ensure they have in place **appropriate independent assurance that five critical network controls are in place** by **end October 2018**. Specifically, the action plan asks that:

- Public bodies undertake a "pre-assessment" by **end March 2018** to help them prepare for Cyber Essentials/Plus certification – **funding** up to **£1,000** will be made available in support of this (**see below**).

- 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 related 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:

  - **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 alternative independent assurance is in place 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.

- In line with the decision made by the Board/senior management, public bodies should then go on to achieve either Cyber Essentials or Cyber Essentials Plus accreditation by **end October 2018**. In the event that this deadline cannot be met for legitimate reasons (e.g. a requirement for significant remediation work), Scottish public bodies should ensure they have in place **appropriate plans to achieve appropriate certification as soon as possible thereafter**.

24. The action plan makes clear that, in exceptional cases and for some particularly complex public bodies, the pre-assessment may make clear that Cyber Essentials or Cyber Essentials Plus is not an appropriate standard to work towards. It also takes account of the potential for wider issues or challenges in the operation of the scheme to be identified. Where public bodies believe this to be the case, they are asked in the first instance to contact the Scottish Government Cyber Resilience Unit.

25. Where public bodies rely solely on the **SCOTs network** for their core network, and only use SCOTS applications, the Scottish Government's Cyber Essentials Plus certification (currently being secured) should provide sufficient assurance for these bodies. Where organisations on the SCOTS network have other applications hosted on SCOTS, or accessible via SCOTS (e.g. in the cloud), they should consider achieving Cyber Essentials or Cyber Essentials Plus certification in respect of these additional elements.

26. The Scottish Business Resilience Centre has worked with Cyber Essentials Certifying Bodies based or operating in Scotland to help develop an agreed position upon which the following section of the toolkit draws. It is intended to help provide clarity with regard to:

    - the approach that Scottish public bodies can take to achieving Cyber Essentials/Plus; and

    - the approach that Scottish public bodies can expect Certifying Bodies based in Scotland to take when supporting them to do so, in line with the requirements of the scheme as set out by accrediting bodies and the technical authority NCSC.

IDENTIFYING A PROVIDER

27. There is a wide range of Cyber Essentials certifying and accredited practitioner bodies available throughout the UK. In broad terms, they undertake two types of key activity directly related to the scheme:

    - **"Pre-assessment":** Providers can work with public bodies to help them prepare for Cyber Essentials, producing a **report** or **gap analysis** identifying any key deficiencies that they need to address prior to seeking certification. This service may be provided either by specialist "Accredited Cyber Essentials Practitioners", who exist only to provide this type of support (i.e. they do not provide certification services) or by bodies that can also provide certification services (see below). Thus public bodies can seek pre-assessments from either type of provider.

    - **Certification**: Separately from the pre-assessment stage, providers can assess public bodies against the Cyber Essentials scheme and award a certificate of compliance if the relevant requirements are met. If public bodies use an "Accredited Cyber Essentials Practitioner" for the pre-assessment stage, they will need to submit for certification via a different Certifying Body or directly via an Accrediting Body, who will then assign the submission to a certified assessor.

    All Certifying Bodies and Accredited Practitioners must be **accredited** by one of the five existing accrediting bodies, which in turn have to comply with the scheme requirements as set down by the National Cyber Security Centre. The Accreditation Bodies are currently:

    - APMG[4]
    - CREST
    - IASME (Information Assurance for Small and Medium Enterprises Consortium)
    - IRM security
    - QG Management Standards (which runs the "Accredited Cyber Essentials Practitioners" scheme referenced above)

28. The Scottish Government **does not endorse any one supplier over another**, and it will be for Scottish public bodies to identify the suppliers they wish to work with. **Certifying Bodies**, **Accredited Practitioners** and **support for remedial action** may be identified in a range of ways. Public bodies will already have in place appropriate arrangements for procuring low value or low risk contracts (up to £50,000), and they are of course free to continue to use these routes to market. Other options to

[4] Note: do not currently accredit Cyber Essentials Plus certification.

identify appropriate support include the following routes, depending on public bodies' procurement requirements:

- **Certifying Bodies/Accredited Practitioners based or operating in Scotland** are listed on the Scottish Business Resilience Centre's website and can be accessed at: https://www.sbrcentre.co.uk/services/cyber-services/cisp-and-cyber-essentials/trusted-partners/.[5]

- The **UK Government's Cyberaware website** provides links to accrediting bodies, who can support public bodies to identify certifying bodies operating in Scotland: https://www.cyberaware.gov.uk/cyberessentials/get.html.

- The **Public Contracts Scotland Quick Quote** facility can be used for low value, low risk contracts where public bodies wish to obtain competitive quotations for the supply of services. The Quick Quote facility allows buyers to ask for competitive quotes for low value/low risk procurement exercises from suppliers who are registered on Public Contracts Scotland. A Quick Quote request is created online and sent to a selected list of suppliers. Only those suppliers selected to quote can access the details of the quote and submit a bid. Further details can be found at: http://www.gov.scot/Topics/Government/Procurement/Selling/SupplierJourney/identify-business-opps/quotations and https://www.publiccontractsscotland.gov.uk/sitehelp/help_guides.aspx.

- The **Digital Services Dynamic Purchasing System**, available to all public sector organisations, can be used to obtain general help and advice on cyber-related activities[6]. This may be most appropriate as a route to market where **remediation work** is required, rather than for low-cost pre-assessment and certification services. However, if pre-assessment, remediation work and certification services were bundles together in one procurement then the DPS can be a legitimate route to market. This service is expected to go live at the end of October 2017. Further details at this stage can be found here: http://www.gov.scot/Topics/Government/Procurement/directory/itms/DynamicPurchasingSystem.

29. When securing quotations, public bodies should discuss the **scope** of the certification they wish to achieve (see below), the **timelines** they are working to, and whether their initial expectation is to achieve **Cyber Essentials** or **Cyber Essentials Plus**.

30. If you are having difficulty in identifying an appropriate route to market, please contact the Cyber Resilience Unit on cyberresilience@gov.scot and we will liaise with Scottish Procurement colleagues to offer advice on an appropriate process.

Getting quotations – guideline pricing

31. Procurement of Cyber Essentials services should be carried out in line with public bodies' individual procurement policies. It is recommended that Scottish public bodies ensure they receive **more than 1 quotation** from different providers for relevant stages of work.

32. Cyber Essentials has been designed as a low-cost way of providing assurance in respect of basic cyber security controls. The cost of achieving Cyber Essentials/Plus will vary depending on the **complexity**[7] and **state of readiness** of an organisation. However, as a rough guideline, based on our understanding of the Scottish public body landscape, costs for public bodies should fall in the following ranges:

- For **a pre-assessment** – c. £750 to £1000. Public bodies can decide whether to opt for Cyber Essentials or Cyber Essentials Plus after completing this stage. **Funding** of up to £1,000 will be made available to all Scottish public bodies to complete this stage (see "process" below for further details).

[5] Any provider that is appropriately accredited and is operating in Scotland can request to be added to this list.

[6] If a specific supplier is not currently on the DPS they can apply to join at any time through the lifetime of the DPS. If the joining criteria are met, they will be rapidly added.

[7] "Complexity" can encompass the size of the organisation, the number of devices and sites, etc.

- For **Cyber Essentials certification** – between £300 to £1500[8]

- For **Cyber Essentials Plus certification** – between £1500 and £6000, depending on the complexity of the organisation. If opting for Cyber Essentials Plus, public bodies may wish to procure additional **CE+ "pre-audit" security testing**, ahead of certification, to give additional comfort that the test requirements will be met. This may cost an additional £750 to £1500.

If public bodies receive quotations that are significantly above these guideline prices, they are encouraged to contact the Scottish Government Cyber Resilience Unit (CRU). The CRU liaises regularly with the NCSC on the effective operation of the scheme.

33. These costs **do not** include the costs of any **remediation** work that may be required if a public body is not currently meeting the five critical controls. See below for guidance on procuring remediation work from **separate suppliers**.

SCOPE

34. Public bodies should, as a first step, discuss the desired **scope** of Cyber Essentials certification with their selected provider. Assessment and certification can cover the whole of the applicant's IT infrastructure, or a sub-set. Either way, the boundary of the scope must be clearly defined in terms of the **business unit managing it**, the **network boundary** and **physical location**.[9]

35. The Scottish Government encourages public bodies **to avoid a restrictive approach** to scope. They should, in particular, be guided by their assessment of **risks to key assets** when deciding on the scope of certification. However, it can be appropriate (and entirely in line with the scheme's requirements) for complex organisations to consider securing certification on a **targeted or phased basis** – e.g. securing Cyber Essentials for the "core" or "central" part of an organisation, with subsidiary organisations or arms' length bodies excluded or tackled separately. This may, for example, be appropriate for local authorities in respect of their wider schools network, or for universities with a range of faculties who wish to assess their central management function as a priority. However, it should be noted that this is only possible if the "core" is separated from the rest of the network by design. It is sometimes possible to make simple network changes to achieve this, e.g. by changing firewall rules.

INTERPRETATION OF THE SCHEME

36. The NCSC sets out the technical requirements of the scheme, and all Accreditation and Certifying Bodies are required to adhere to these. The most up to date version of the technical requirements can be found here: https://www.cyberessentials.ncsc.gov.uk/requirements-for-it-infrastructure.html

37. Within the technical requirements, there are some criteria that require to be interpreted based on the **context** of the organisation undergoing certification – this is the same under other risk-based schemes. SBRC have confirmed with Certifying Bodies based or operating in Scotland that they apply an appropriate, pragmatic, risk-based approach to complex organisations, which takes account of the context in which they operate while still ensuring adherence to the five critical controls. Examples of where the need for a contextual approach may apply include:

- **Patching**: The scheme's technical guidance observes that all **critical** or **high-risk** security patches running on computers or network devices that are connected to or capable of connecting to the internet must be installed **within 14 days of release**. For security patches that are "medium" or "low" risk, public bodies should be able to demonstrate that they patch in a timely manner, and justify this with regard to risk and the complexity of the organisation.

- **Legacy systems**: Certifying Bodies recognise that some public bodies have to continue to operate legacy systems for some essential systems/services that have not yet been made available on

[8] Note: the CREST accreditation body has built in requirements for an external scan to the basic Cyber Essentials process – the higher price end of the range here reflects these requirements. These higher costs for Cyber Essentials certification are only expected to be applied by Certifying Bodies operating under CREST accreditation. Additionally, if the public body is applying a limited scope to certification, CREST requires Certifying Bodies to verify the segregation in place by means of additional scans, which may further increase costs.

[9] See: https://www.cyberessentials.ncsc.gov.uk/requirements-for-it-infrastructure.html

newer platforms. Where this is the case, Certifying Bodies will require public bodies to demonstrate that they are managing this risk appropriately (e.g. through network segregation), etc.

38. If, following discussions with certifying bodies, public bodies believe that the scheme is being interpreted by a Certifying Body in a way that is overly restrictive or not in keeping with the approach set out above, as well as discussing with the Certifying Body in question, they should contact the Scottish Government Cyber Resilience Unit (CRU), who can discuss issues with the NCSC to try and achieve greater clarity on any points of confusion.

39. If public bodies find that complying with the Cyber Essentials scheme's requirements is not possible due to justifiable constraints that are inherent to their current network or organisational design, they should contact the CRU. The CRU will endeavour to work to identify common solutions to issues requiring to be addressed across public sector organisations.

<u>Process (i) – Pre-assessment and Board/Senior Management decision on appropriate certification</u>

40. All public bodies are asked to secure and undergo a Cyber Essentials "pre-assessment" by **end March 2018**. The costs of this will be met under the UK Cyber Security Funding Programme in Scotland.

41. The Scottish Government will make available funding of up to £1,000 (inclusive of any irrecoverable VAT) for public bodies to undertake this work. It is proposed that this will be achieved by the following process:

    - The Scottish Government sent (in December 2017) to all public bodies a **provisional grant award letter**, detailing the terms of a grant award for the purposes of a Cyber Essentials pre-assessment.

    - Once individual public bodies have procured and paid for a Cyber Essentials pre-assessment in line with their own procurement rules, they can "claim back" the cost of doing so (up to £1,000, inclusive of any irrecoverable VAT) by **completing the grant award letter** and **returning it** to cyberresilience@gov.scot with **proof of the work having been undertaken**.

    - **Payment** will then be made by the Scottish Government Cyber Resilience to the individual public body in line with the terms of the grant letter.

42. The primary purposes of this pre-assessment are to help the public body to prepare for Cyber Essentials certification and identify any key issues that require to be addressed in order to secure certification. Evidence gathered under the Digital Scotland Business Excellence Partnership Cyber Resilience Voucher scheme run by Scottish Enterprise for small businesses suggests that this pre-assessment process can significantly improve the chances of securing Cyber Essentials certification. The pre-assessment process should also help identify any significant issues in terms of the way in which the scheme is being applied to Scottish public bodies.

43. Certifying Bodies will generally ask public bodies to complete a Cyber Essentials self-assessment in advance of the pre-assessment (some may offer telephone support, at a cost, to help complete this if required). The provider will then generally spend one day onsite with the public body, talking them through the scheme, seeking evidence against the assertions set out in the self-assessment, and helping the public body identify any areas of weakness. Public bodies should ensure they make available the key people needed to answer questions about the self-assessment.

44. The provider will generally then supply a **report/gap analysis/action plan** to the public body in question, identifying any areas for improvement. Public bodies should ensure that **executive Boards/Senior Management** are sighted on this report.

45. The **Board/Senior Management** of an individual public body should then make an informed decision on whether to seek CE or CE+ certification, based on the pre-assessment report received, their appetite for <u>independent assurance</u> that the five critical controls are being met, their assessment of the extent to which this is already being provided by alternative arrangements (e.g. broad-based PSN accreditation, other accreditations, etc.), and their assessment of costs and benefits.

46. If Boards/Senior Management are in any doubt as to whether they have independent assurance in place, they are encouraged to consider seeking Cyber Essentials Plus certification.

47. If Boards/Senior Management have concerns that the Cyber Essentials scheme is not appropriate for their organisation, or that the way in which the scheme is being applied is not in conformity with the pragmatic, risk-based approach to complex organisations outlined earlier in this toolkit, they are asked to contact the Scottish Government Cyber Resilience Unit (CRU). The CRU will raise any such concerns with the NCSC, and may work with the public body to identify alternatives to Cyber Essentials certification in exceptional cases.

48. NB: To ensure consistency of approach in terms of pre-assessment and certification, it may be desirable to use either the same organisation, or (if an Accredited Practitioner is used for the pre-assessment stage) an organisation operating under the same accreditation body, to undertake the pre-assessment and final Cyber Essentials certification stages of the process. However, if a requirement for **remediation work** is identified at the pre-assessment stage, public bodies should consider carefully the benefits of seeking **different suppliers** for this work, given the potential incentives for upselling that use of a single supplier throughout all stages of the process could create.

Process (ii) – Remediation work (if required)

49. Where **remediation work** is required in order to meet Cyber Essentials requirements, public bodies are required to carry this out within their existing budgets. Public bodies should make their own arrangements for any external advice or support required. They may wish to continue to seek advice from pre-assessment or certifying bodies with regard to the requirements for remediation work, and they may also wish to make use of the **Dynamic Purchasing System** to procure appropriate expertise. For bodies that already hold existing accreditations, the expectation is that remedial costs (if any) are likely to be minimal.

50. Where significant remedial work is required, at significant costs, public bodies are encouraged to contact the Scottish Government Cyber Resilience Unit to discuss this. Where **common challenges** for the public sector in meeting the five critical controls are identified as a result of such feedback, the Scottish Government will work with public bodies to explore whether common solutions can be identified that would achieve economies of scale.

Process (iii) – Cyber Essentials (Plus) Certification

51. Public bodies should proceed to undergo Cyber Essentials or Cyber Essentials Plus certification following completion of steps (i) and (ii) above[10].

52. The speed at which this can be achieved will depend on the complexity of the organisation and any remedial work identified at step (i) above. However, public bodies are asked to ensure they have completed the process by **end October 2018**.

53. Where there are legitimate reasons for this deadline not being achievable (e.g. supply bottlenecks, significant remediation work required), public bodies will be asked to demonstrate that they have a plan in place to achieve certification as soon as possible thereafter.

54. If a public body opts to achieve the **Cyber Essentials certificate** (because they judge they have sufficient independent assurance from other accreditations held), they will be required only to submit their self-assessment to their selected Certifying Body[11]. That Certifying Body will then ensure that the self-assessment provided meets the requirements of the scheme. If it does, a **Cyber Essentials Badge** will be awarded. Public bodies opting to achieve the Cyber Essentials certificate will be asked by the SG Cyber Resilience Unit to give reasons for doing so (i.e. the existence of alternative independent assurance).

[10] Subject to the pre-assessment process providing confidence that the scheme is being appropriately applied to complex public sector organisations. In the event that it becomes clear this is not the case, the Scottish Government will raise any relevant issue s with the National Cyber Security Centre, and may consider alternatives to Cyber Essentials certification.

[11] Unless the certifying body selected is a CREST-accredited body, in which case a scan is required and built into the pricing.

55. If a public body opts to go on to achieve the **Cyber Essentials Plus certificate**, their Certifying Body will make clear what independent security testing (to confirm the Cyber Essentials self-assessment) under the process will entail, and what the public body should do to prepare. Some certifying bodies may require a public body to undertake CE+ security testing within **90 days** of submitting their CE self-assessment.

    A public body seeking CE+ may wish to undertake **Cyber Essentials Plus pre-audit security testing**, which involves a limited set of security scans to confirm any issues that remain to be addressed. This can offer additional comfort that the public body is likely to pass the final test.

    An assessor will then arrange a date to conduct the security tests. The costs attached to this will depend on the complexity of the public body, whether multi-site testing is required, etc. As noted above, costs should not generally exceed £6,000 even for more complex public bodies. Where they do, public bodies will be encouraged to contact the SG Cyber Resilience Unit for discussion. Once completed a **Cyber Essentials Plus Badge** will be awarded.

56. To ensure cost-effectiveness and reduce burdens, public bodies that undergo **PSN accreditation** may wish to consider requesting their annual IT Health Check suppliers to incorporate Cyber Essentials Plus certification into these assessments. This should lead to lower costs and reduced compliance burdens, but it may also affect timelines with regard to achievement of Cyber Essentials Plus. The Scottish Government has tested this proposal with a number of ITHC suppliers, who have indicated it should be feasible. Requirements in respect of ongoing Cyber Essentials/Plus accreditation will be clarified once the final Scottish Public Sector Cyber Resilience Framework is in place from end June 2018.

57. **Annex B** to this toolkit provides an overview of the process described above.

KEY ACTION 5 Active Cyber Defence Measures

58. Key Action 5 asks that public bodies be aware of, and implement appropriately, NCSC’s Active Cyber Defence (ACD) measures. Four of these measures are described in the action plan.

59. Public bodies should consider the extent to which they already have in place measures that replicate the ACD measures, and/or the extent to which their organisation would benefit from implementing the ACD measures.

60. Where public bodies already have in place paid-for measures that replicate the ACD measures, they may choose:

    - To discontinue their existing paid-for measures in line with contractual arrangements to take advantage of the free ACD measures;
    - If appropriate/feasible, to apply both their existing paid-for measures and the free ACD measures, to provide added assurance (e.g. if they feel that there is an imperfect overlap); or
    - Not to apply the ACD measures.

61. Once they have undertaken this initial analysis, public bodies should adopt the following procedures to take advantage of those ACD measures they wish to adopt:

    - To take advantage of **Protected DNS**, public bodies should register through the https://nominet.service-now.com/csm, select “Request an Account”, and supply the following details:

        - Organisation name and key contact details
        - Lead commercial contact responsible for choosing the DNS service in your organisation
        - Lead technical contact responsible for managing the DNS service in your organisation
        - What PSN domain your technical team manages for your organisation

  - What internet IP addresses you want to whitelist on the internet resolver

- To take advantage of **DMARC anti-spoofing**, Scottish public bodies should email dmarc@ncsc.gov.uk for further details.

- To take advantage of **WebCheck**, Scottish public bodies should register at www.webcheck.service.ncsc.gov.uk and quote the reference wbchk04/7.

- To maximise the effectiveness of the **phishing and malware mitigation Netcraft service**, public bodies should build into their processes a requirement for suspicious emails, along with any attachments, to be forwarded to scam@netcraft.com. Netcraft will then issue takedown notifications to the hosts of the mail and phishing sites. Similarly, if a department discovers a clone of their own site or online services, they should use the same email address to notify Netcraft of the URL of the offending site and they will initiate action for the site to be taken down.

KEY ACTION 6 Training and Awareness Raising

62. Key Action 6 asks that public bodies ensure they have in place appropriate training and awareness raising for the following staff:

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

63. Public bodies that are subject to the Scottish Public Finance Manual should already have such arrangements in place to comply with their obligations under the SPFM.

64. **Annex C** to this toolkit provides information on **existing training opportunities or providers** that public bodies may wish to make use of to ensure they have appropriate training arrangements in place. The **Digital Services Dynamic Purchasing System**, available to all public sector organisations, can also be used to identify and procure training services (see details under Key Action 4, above). **Annex D** provides some scenarios that Scottish public bodies can use to test their organisational resilience.

65. The Scottish Government is developing a significant **security behavioural change programme,** based on good practice in this area and building on many of the existing awareness raising resources highlighted in Annex C. This programme is being developed and implemented within the **Scottish Government** between 2018-20.[12]

66. The Scottish Government has committed to sharing learning materials that are relevant for the wider Scottish public sector. These materials will be made available in line with the timings of the Scottish Government programme, which are currently being finalised. Public bodies will be contacted as material becomes available. Public bodies should in the meantime make use of the existing resources identified at Annex C, or their own materials, to support staff training and awareness raising.

KEY ACTION 7 Incident Response

[12] An outline of this specific programme of work can be found at Annex D of the **action plan**.

67. Key Action 7 asks that public bodies ensure they have in place appropriate incident response arrangements that align with central coordinating and reporting protocols.

68. In December 2017, the Scottish Government disseminated the following key resources:

- Guidance on **central incident coordination and reporting protocols**, which make clear to Scottish public bodies how they should report significant cyber incidents; and
- A **template incident response plan**, providing material that public bodies may choose to adapt to suit their own organisations.

69. Public bodies should:

i. Ensure they have in place **appropriate organisational incident response plans**. They may wish to make use of the template plan provided by the Scottish Government, or they may wish to devise their own plans more suitable to their organisational structures. They should seek to incorporate these plans into their wider incident response arrangements.

Support for the **development and execution** of cyber incident response plans can be found via external providers. These can be accessed through:

- The **Digital Services Dynamic Purchasing System**, which any public sector organisation can access, and which offers a quick and easy route to market for cyber security services[13]. This is expected to go live at the end of October 2017. Further details at this stage can be found here: http://www.gov.scot/Topics/Government/Procurement/directory/itms/DynamicPurchasingSystem
- The **Crown Commercial Services Cyber Security Services 2 framework**, which is an EU compliant and regulated route to market for buyers from across central government and the wider public sector, to buy National Cyber Security Centre (NCSC) certified cyber security services. Lot 3 covers Cyber Incident Response: https://ccs-agreements.cabinetoffice.gov.uk/contracts/rm3764ii
- **The Cyber Security Incident Response scheme** - approved by CREST (Council of Registered Ethical Security Testers) – www.crest-approved.org - and focused on appropriate standards for incident response suited to industry, the wide public sector and academia. The scheme is administered by CREST and endorsed by NCSC and CPNI.

ii. Ensure by **end June 2018** that these plans align with **central incident reporting and coordination mechanisms**, as set out in the guidance that will be disseminated to public bodies by **end 2017**.

KEY ACTION 11 Monitoring and Evaluation

70. Key Action 11 sets out how public bodies will be asked to demonstrate that they are meeting the initial baseline progression stage of the Scottish Public Sector Cyber Resilience Framework.

71. Public bodies will ideally **proactively contact** the Scottish Government Cyber Resilience Unit (cyberresilience@gov.scot) at **working level** to update them on an ongoing and informal basis, and in any case in line with the deadlines set out in the document, when key actions have been completed.

72. The Scottish Government will **formally** seek information from the **Boards/Senior Management of public bodies** in line with the deadlines set out in the action plan. The details they will be asked to provide, and the timelines that will apply, are as follows:

[13] If a specific supplier is not currently on the DPS they can apply to join at any time through the lifetime of the DPS. If the joining criteria are met, they will be rapidly added.

ONE-OFF MONITORING INFORMATION REQUIREMENTS		
KEY ACTION	**INFORMATION REQUIRED**	**TIMELINES**
2	▪ Confirmation that your organisation has **minimum governance requirements** in place.	▪ End June 2018
3	▪ Confirmation that your public body manages its own network and has **become a member of CiSP**. ▪ Confirmation that your public body does not manage its own network and therefore does not require to join CiSP.	▪ End June 2018
4	▪ Confirmation that your organisation has undergone a **Cyber Essentials pre-assessment**, that the resulting report has been shared with your Board/Senior Management, and that a decision has been taken on whether to seek CE basic or CE+ certification (and what this decision is). *(Where, exceptionally, a judgement is made that neither certification is suitable for your organisation, please contact the SG Cyber Resilience Unit to discuss.)* ▪ If you have opted for CE "basic", confirmation of the Board/Senior Management's reasons for this, with particular reference to existing accreditations providing independent assurance. ▪ Confirmation that **CE or CE+ certification has been achieved** (or, where legitimate reasons for delay are supplied, that a plan is in place to achieve it), along with **information on scope of certification**, and any plans for extending the scope of certification in the future.	▪ End June 2018 ▪ End June 2018 ▪ End October 2018
5	▪ Confirmation that you are aware of the **Active Cyber Defence Programme**, have assessed its relevance to your organisation, and are making appropriate use of key elements. Details of reasoning where use is not made will be requested.	▪ End June 2018
6	▪ Confirmation that you have in place **appropriate training and awareness-raising** policies and processes, and details of what these are.	▪ End June 2018
7	▪ Confirmation that you have in place appropriate **cyber incident response plans** as part of wider response arrangements, and that these **align with central incident reporting and coordination mechanisms**.	▪ End June 2018

73. Thereafter, monitoring and evaluation arrangements will depend on the shape of the final Scottish Public Sector Cyber Resilience Framework and the development of any self-assessment tool that supports burden reductions. Further information will be supplied to public bodies in due course.

ANNEX A – APPLICABILITY OF ACTION PLAN TO SCOTTISH PUBLIC BODIES

This annex sets out a list of Scottish public sector organisations, and makes clear the applicability of the public sector action plan to different classes of organisation. It divides them into:

a) **"Scottish public bodies"**: These are Scottish public bodies the majority of which are subject to the Scottish Public Finance Manual[14] to ensure good practice. These public bodies will be expected or encouraged to align their approach to cyber resilience with this action plan in order to ensure compliance with the SPFM or other relevant requirements.[15]

Some of the organisations in this section have a special constitutional status that means their independence from Government, and the way in which a Government-sponsored action plan applies to them, must be particularly carefully considered. This is especially true of the Scottish Parliament and its Parliamentary Commissioners, and bodies such as Audit Scotland. Where bodies are denoted by an asterisk (*), this means that, while the action plan may not apply directly to their organisation, they have been made aware of its contents and invited to align their work on cyber resilience with other Scottish public bodies. Where such bodies have adopted the SPFM, this is also expected to influence their alignment with the action plan.

b) **"Wider Scottish Public Sector"**: Scottish public bodies and organisations where the Scottish Government will work closely with key central coordinating bodies to implement this action plan wherever possible, whilst recognising that certain bespoke arrangements may be required in view of sector-specific challenges – this applies to **local authorities** and the **colleges[16] and universities sector**.

a) Scottish public bodies

Executive agencies (7)

- Accountant in Bankruptcy
- Disclosure Scotland
- Education Scotland
- Scottish Prison Service
- Scottish Public Pensions Agency
- Student Awards Agency for Scotland
- Transport Scotland[17]

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 Service18
- Scottish Fiscal Commission

[14] See: http://www.gov.scot/Topics/Government/Finance/spfm/Intro for detailed information on the applicability of the SPFM.

[15] Note: For Health Boards and Scottish Water, it will be necessary to agree an aligned approach with the new NIS Competent Authority or Authorities when in place. Cyber resilience arrangements for Integration Joint Boards are reliant on Health Boards and Local Authorities, to whom this action plan applies as set out in this annex.

[16] Note: Since 2014, colleges have been classified as public, central government bodies with the sponsor relationship managed through the Scottish Funding Council. Universities are classified as charitable bodies, not public bodies. Both are included in the "wider public sector" class of bodies in view of the desirability of aligning their approaches.

[17] Note: Regional Transport Partnerships (RTPs), which are independent bodies corporate defined in the Transport (Scotland) Act 2005, will also be asked to align their approach to this action plan wherever possible. There are 7 RTPs: Shetland Transport Partnership (ZetTrans); Highlands and Islands Transport Partnership (HITRANS); North-East of Scotland Transport Partnership (NESTRANS); Tayside and Central Scotland Transport Partnership (TACTRAN); South-East of Scotland Transport Partnership (SESTRAN); Strathclyde Partnership for Transport (SPT); South-West of Scotland Transport Partnership (Swestrans).

[18] The Scottish Courts and Tribunals Service supports Tribunals in Scotland, with the exception of the Parole Board for Scotland, which operates independently of the SCTS.

- 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 Trust19
- 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)[20]

- Healthcare Improvement Scotland
- Mental Welfare Commission for Scotland

[19] The SFT has a separate, bespoke Management Statement and associated Financial Memorandum (MSFM) and is not subject to the SPFM.

[20] See footnote 15 above.

- 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

b) "Wider Scottish Public Sector Organisations"

Local authorities (32) [21]

- Aberdeen City Council
- Aberdeenshire Council
- Angus Council
- Argyll and Bute Council
- City of Edinburgh Council

[21] The Scottish Government has agreed to work closely with the Scottish Local Government Digital Office, who will lead on the development of a programme of cyber security activity for local authorities that is aligned with this action plan. £100,000 has been made available under the UK Cyber Security Programme to support the appointment of a Chief Information Security Officer (CISO) for these purposes.

- 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

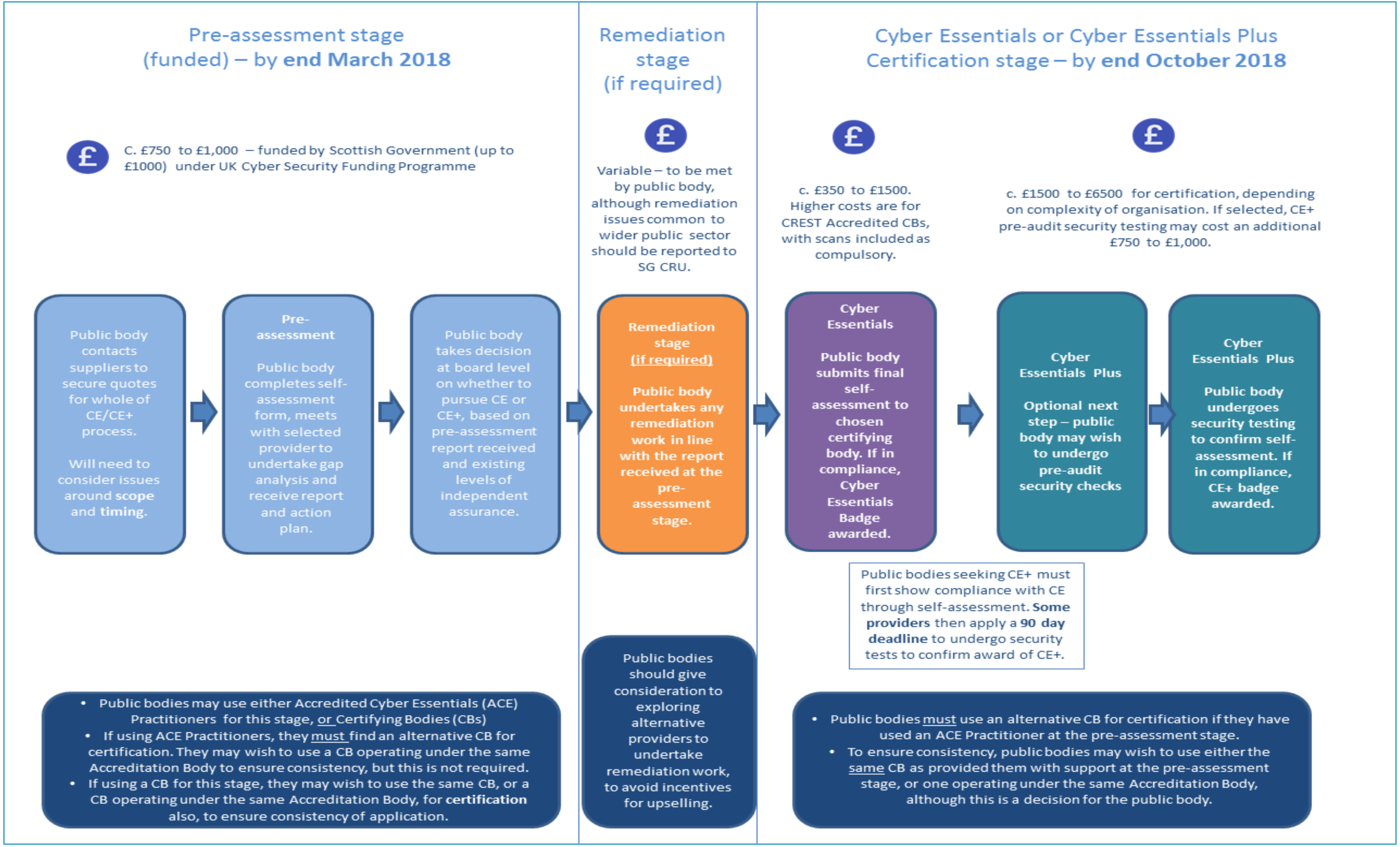
Scottish colleges and universities (43) [22]

- 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

[22] The Scottish Government will seek to work closely with key bodies including HEIDS (Higher Education Information Directors for Scotland) and Universities and Colleges Shared Services (UCSS) to align work in universities and colleges with this action plan wherever possible.

- 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

ANNEX B – OVERVIEW - CYBER ESSENTIALS CERTIFICATION PROCESS FOR SCOTTISH PUBLIC BODIES (ILLUSTRATIVE)



Pre-assessment stage (funded) – by **end March 2018**

£ C. £750 to £1,000 – funded by Scottish Government (up to £1000) under UK Cyber Security Funding Programme

Public body contacts suppliers to secure quotes for whole of CE/CE+ process.

Will need to consider issues around **scope** and **timing.**

Pre-assessment

Public body completes self-assessment form, meets with selected provider to undertake gap analysis and receive report and action plan.

Public body takes decision at board level on whether to pursue CE or CE+, based on pre-assessment report received and existing levels of independent assurance.

- Public bodies may use either Accredited Cyber Essentials (ACE) Practitioners for this stage, or Certifying Bodies (CBs)
- If using ACE Practitioners, they must find an alternative CB for certification. They may wish to use a CB operating under the same Accreditation Body to ensure consistency, but this is not required.
- If using a CB for this stage, they may wish to use the same CB, or a CB operating under the same Accreditation Body, for **certification** also, to ensure consistency of application.

Remediation stage (if required)

£ Variable – to be met by public body, although remediation issues common to wider public sector should be reported to SG CRU.

Remediation stage (if required)

Public body undertakes any remediation work in line with the report received at the pre-assessment stage.

Public bodies should give consideration to exploring alternative providers to undertake remediation work, to avoid incentives for upselling.

Cyber Essentials or Cyber Essentials Plus Certification stage – by **end October 2018**

£ c. £350 to £1500. Higher costs are for CREST Accredited CBs, with scans included as compulsory.

£ c. £1500 to £6500 for certification, depending on complexity of organisation. If selected, CE+ pre-audit security testing may cost an additional £750 to £1,000.

Cyber Essentials

Public body submits final self-assessment to chosen certifying body. If in compliance, Cyber Essentials Badge awarded.

Cyber Essentials Plus

Optional next step – public body may wish to undergo pre-audit security checks

Cyber Essentials Plus

Public body undergoes security testing to confirm self-assessment. If in compliance, CE+ badge awarded.

Public bodies seeking CE+ must first show compliance with CE through self-assessment. **Some providers** then apply a **90 day deadline** to undergo security tests to confirm award of CE+.

- Public bodies must use an alternative CB for certification if they have used an ACE Practitioner at the pre-assessment stage.
- To ensure consistency, public bodies may wish to use either the same CB as provided them with support at the pre-assessment stage, or one operating under the same Accreditation Body, although this is a decision for the public body.

ANNEX C – EXISTING AWARENESS RAISING AND TRAINING OPPORTUNITIES OR PROVIDERS (Updated March 2018)

74. This annex provides information on **existing awareness raising and training opportunities or providers** that Scottish public bodies can make use of to ensure they have appropriate training arrangements in place.

CYBER RESILIENCE STRATEGY – PILOT PROJECTS IN SCOTLAND ADDRESSING CYBER RESILIENCE WORKPLACE LEARNING NEEDS

75. The Scottish Government has been allocated funding in 2017/18 under the UK Cyber Security Funding Programme, to support initiatives in Scotland which will improve and build on Scotland's cyber resilience. Of the projects the Scottish Government is supporting in 2017, three of them are focussed on **workplace learning and skills development**. The following projects are all in the initial development stages (at October 2017). The Cyber Resilience Unit will share information and participation details about these programmes as they begin to be rolled out, or when there are course outlines and learning materials available which can be shared or adapted by public sector organisations.

i. **Scottish Union Learning**: Scottish Union Learning (SUL) are currently working on a project to build the capacity of organisations, unions, Union Learning Representatives and Scottish Union Learning itself to embed cyber resilience and security into their learning offer for workers. This will complement SUL's existing Digital Unions project. SUL will work in partnership with Craig Steele Digital Training to extend reach and help workers to cope with daily cyber security risks, by providing opportunities to improve their personal cyber security skills. Funding of £55,000 has been made available to support this project.

   For more information on this project please contact: Catherine Garvie, Scottish Union Learning: cgarvie@stuc.org.uk; Craig Steele Digital Training: cr@igsteele.com.

ii. **Napier University**: Napier University's Cyber Academy are working on a project to build national capability and resilience in identifying, managing and responding to cyber threats. They will be developing a series of training courses for Police Scotland and public sector staff to: increase the pool of trained cyber specialists across key organisations in Scotland; develop specific skills and capability in security operations and incident response; increase collaboration by sharing skills, information and knowledge across organisations; and increase the effectiveness of Scotland's public bodies in managing cyber threats. Funding of £35,000 has been made available to support this project. *For more information on this project please contact:* Basil Manoussos, The Cyber Academy: V.Manoussos@napier.ac.uk

Update at March 2018:

BOOKING - These workshops are being delivering in March 2018 in Edinburgh (at their new SOCLAB) Glasgow, Inverness, Aberdeen and Perth. They are also delivering some of their non-technical training online in order for people in remote areas to participate in some of the training.

The link to register for these courses is: **https://www.eventbrite.co.uk/o/the-cyber-academy-16599551134**

Please book ASAP, or forward this link to any managers within your organisation you think would benefit from either technical or non-technical cyber incident response skills.

iii. **Perth College, University of Highlands and Islands – Accredited Cyber Resilience Management Project**: Perth College UHI are currently developing an online accredited Cyber Resilience Management Programme. The aims of this programme are to enable resilience practitioners to prepare their organisation for cyber risks, and to influence strategic direction within key responders to minimise impact on services and ensure a swift recovery from a cyber-related incident. The college are developing a module accredited at Scottish Credit and Qualifications Framework (SCQF) level 10 for resilience practitioners on **Managing Cyber Resilience**, to sit within a PG Certificate. They will also be making the module available as an online CPD. *For more information on this project please contact:* Jillian Elder, Sector Manager Business, Management and Computing: Jillian.Elder.perth@uhi.ac.uk or Suzanne Wilkie, Scottish Resilience Development Service: Suzanne.wilkie@gov.scot.

CYBER RESILIENCE AWARENESS RAISING PROGRAMMES AND CAMPAIGNS (UPDATE ADDED IN MARCH 2018)

The National Cyber Security Centre (NCSC) is intended to be the authoritative voice and centre of expertise on cyber security for the UK as a whole. It has a key role in managing significant national cyber security incidents. NCSC is a relatively new organisation – just over a year old – and continues to develop its advice and support offering.

CPNI has developed a series of security awareness campaigns, designed to provide organisations with a complete range of materials they need. Each campaign set has full guidance on how to run the campaign, and materials such as downloadable posters that can be customised to the organisation, wallets, flyers, videos and checklists (https://www.cpni.gov.uk/security-awareness-campaigns)

Protecting your device
Protecting your data
Protecting your business

Cyber Aware is a cross-government awareness and behaviour change campaign delivered by the Home Office in conjunction with Department of Culture, Media & Sport alongside the National Cyber Security Centre, and funded by the National Cyber Security Programme in the Cabinet Office (https://www.cyberaware.gov.uk/).

Cyber Aware has a wide range of communications and marketing campaigns which focus on three key pillars:

Take 5, a national awareness campaign led by FFA UK (part of UK Finance), backed by UK Government and delivered with and through a range of partners in the UK payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector, to help tackle financial fraud (https://takefive-stopfraud.org.uk/).

Get Safe Online (GSO) is a UK Government-funded free resource providing practical advice to individuals and businesses on how to protect themselves while on their computers and mobiles device and against fraud, identity theft, viruses and many other problems encountered online. Their website (https://www.getsafeonline.org/) contains a dense library of content that comes under the following headings:

Protecting your computer
Protecting yourself
Smartphone and Tablets
Shopping, banking and payments
Safeguarding children
Social networking
Business

LEARNING PROGRAMMES CURRENTLY AVAILABLE THROUGH FORMAL LEARNING ROUTES, ONLINE LEARNING AND COMMERCIAL SUPPLIERS

76. There is a broad range of learning programmes available through private training providers and higher and further education routes. Public bodies may wish to consider making use of these for their staff learning and development activities with regard to cyber resilience.

77. The **Digital Services Dynamic Purchasing System**, available to all public sector organisations, can also be used to identify and procure training services (see details under Key Action 4, above).

78. The Government Communications Headquarters (GCHQ) have developed a certification scheme to help individuals and organisations quickly identify high quality relevant cyber security training courses. The certified of courses cover a broad range of subjects from introductions to cyber security up to certified information systems security professionals. We have included links to a selection of those certified courses in the following table, but the full list of GCHQ Certified Training courses is available from https://apmg-international.com/product/gct

79. In addition to the GCHQ Certified Training courses mentioned above, we have also collated a selection of other learning opportunities identified through open source research. **Inclusion in this list does NOT constitute Scottish Government endorsement of the programme.** Providers who wish to be added to this list should contact the Scottish Government Cyber Resilience Unit (cyberresilience@gov.scot).

GENERAL AWARENESS OF CYBER RESILIENCE FOR ALL STAFF

Course title and content	Duration	Level (SCQF level if known)	Target audience	Cost
GCHQ Certified Training (GCT) courses for all staff awareness raising including board level There are a broad range of GCT courses which may suitable for general awareness raising for all staff or specific to boards and directors, these include: Introduction to Cyber Security (see	Dependent on course and supplier	Not known	some courses will be designed for general knowledge and all staff, some courses are specifically designed for specialist staff.	Dependent on course and supplier

below) Cyber Security for Boards Cyber Security for Non-Executive Directors, Trustees and Audit Committees The Insider Threat including Social Media Best Practice				
Open University –Future Learn, Introduction to Cyber Security This free online course will help you to understand online security and start to protect your digital life, whether at home or work. You will learn how to recognise the threats that could harm you online and the steps you can take to reduce the chances that they will happen to you. This GCHQ Certified Training course is also accredited by the Institute of Information Security Professionals (IISP)	3 hours per week over 8 weeks	Not known	The course does not assume any prior knowledge of computer security and can be enjoyed by anyone interested in improving the security of their digital information.	* Free *
HMG/National Archives – 'Responsible for Information' for SMEs free e-learning course aimed at staff in SMEs. It helps employees and business owners to understand information security and associated risks, and it provides good practice examples and an introduction to protection against fraud and cyber-crime. The course is divided into three modules, each module is tailored to the specific needs of the target audience and includes role-specific content. All modules conclude with an assessment to test the user's understanding.	It will take between 45 - 75 minutes to complete the course depending on the module you are taking	n/a	•General users •Information Asset and Information Risk Owners •Directors and Business Owners	* FREE *
NSPCC - Keeping children safe online course An online introductory safeguarding course for anyone who works with children •how children use the internet and technology •the risks they face from other people - both other children and adult offenders •behaviour by children that exposes them to greater risks online •what to do if children experience issues such as cyber bullying or grooming •how to make organisations safer places for children to go online •how to conduct an e-safety audit and create an acceptable use policy for your organisation.	3h	n/a	anyone who works with children or families in their paid or voluntary work	£20

Foursys Cyber Training Toolkit Toolkit for employers to upskills end users. Videos, posters, quizzes, email templates to send them out.	brief	n/a	Employees	* FREE *

SPECIFIC PROFESSIONS, e.g human resources, legal and procurement

Course title and content	Duration	Level (SCQF level if known)	Target audience	Cost
The Law Society - Cyber Security for Legal and Accountancy Professionals Designed for both lawyers and accountants this online course is designed to last for one hour and is structured into four modules. • Introduction to cyber security • Cyber security – your responsibilities • Managing the cyber risk • Scenarios	1h	n/a	Legal and Accounting Professionals	* FREE *
CIPS – Cyber Security e-learning for Procurement Professionals free online course which shows how employees and organisations can mitigate against cyber threats. It explains the relevance of cyber security in the procurement and supply chain function and why it is important to take it seriously. You can claim CPD points for completing it.	75 min	n/a	Procurement professionals	* FREE *
CIPD – Cyber Security for HR Professionals E-learning module about: what cyber security is, how it affects you and why you should care about it; The threats to how you do business and how they affect you as an individual; How attacks happen and terms such as 'phishing' and 'hacking'; The possible impacts of cyber attacks on you, your organisation, your employees and your customers; What you can do to mitigate these impacts.	75 min	n/a	HR Professionals	* FREE *

ICT AND INFORMATION SECURITY STAFF QUALIFICATIONS AND PROFESSIONAL DEVELOPMENT

Course title and content	Duration	Level (SCQF level if known)	Target audience	Cost
GCHQ Certified Training (GCT) courses for ICT and information security staff There are a broad range of GCT courses which are suitable for developing professional skills in this	Dependent on course and supplier	Not known	Some courses will be designed for general knowledge and all staff, some courses are	Dependent on course and supplier

area, from awareness to application level. These include: Cyber Security Awareness Delivering Information Assurance Training System and Network Security Introduction Penetration testing and ethical hacking Information Risk Management			specifically designed for ICT and information security staff.	
Edinburgh Napier University - MSc Advanced Security and Cybercrime The Masters degree in Advanced Security and Cybercrime focuses on extending your knowledge into leading-edge issues related to network and computer security technologies and processes, both generally and with a particular focus on the growing threats from cybercrime. Fully GCHQ certified	18 months, 180 SCQF credits	11	designed for professionals already employed in the area of computing who wish to develop their skills into the areas of computer security and cybercrime.	£3,750
Open University –Future Learn, Cyber Security: Safety at Home, Online, in Life This three-week online course explores practical cyber security including privacy online, payment safety and security at home. The course is presented by researchers and practitioners from Newcastle University's School of Computing, an acknowledged Academic Centre of Excellence in Cyber Security Research (ACE-CSR).	3 hours per week over 3 weeks	Not known	The course is suitable for people who have some knowledge of cyber security, some IT background and an interest in finding out the state of practice in cyber security as well as future research directions.	* Free *
BCS/ECDL - IT Security 2.0 This module sets out concepts relating to the secure use of ICT in daily life and skills used to maintain a secure network connection, use the Internet safely and securely, and manage data and information appropriately.	37 SCQF credits	SCQF level 5	Designed specifically for those who wish to gain a qualification in computing to enable them to develop their IT skills and enhance their career prospects.	£130 £155 advanced

ANNEX D – SCENARIOS TO EXPLORE ORGANISATIONAL CYBER RESILIENCE

1. This annex provides some basic scenarios to enable senior teams to consider their organisation's cyber resilience procedures and identify lessons to take forward. These scenarios are based on real life incidents that have taken place.

2. You may wish to use and adapt these scenarios to explore your own organisation's preparedness and response to a cyber incident, as well as your links and relationships with other bodies and reporting organisations such as Police Scotland and the Information Commissioner's Office.

RUNNING (AND LEARNING FROM) AN EXERCISE

3. These scenarios are designed to be conducted as a 'talk through' workshop, where participants can safely explore their understanding of your organisation's current cyber resilience arrangements.

4. It would be beneficial if you are able to access an experienced **facilitator** within your own organisation to run these scenarios with your senior teams, and a person tasked to note any learning points identified throughout the workshop.

5. Experience suggests there will be lots of lessons identified when talking through these scenarios. The senior team should take ownership of the lessons process to ensure that any actions required to improve the organisation's cyber resilience are undertaken. Lessons reports should consider:

   - Exactly what happened, at what times?
   - How well did staff and management perform in dealing with the incident/scenario? Were the documented procedures followed? Were they adequate?
   - What information was needed sooner?
   - Were any steps or actions taken that might have inhibited the recovery?
   - What would staff and management do differently the next time a similar incident occurs?
   - How could information sharing and coordination with other organisations have been improved?
   - What corrective actions can prevent similar incidents in the future?
   - What precursors or indicators should be watched for in the future to detect similar incidents?
   - What additional tools or resources are needed to detect, analyse and mitigate future incidents?

6. We suggest that you repeat these exercises once you have identified and acted on any lessons from the first run through.

7. You can run these scenarios independently of each other, or link them to suggest an escalating and targeted attack on your organisation or sector.

EXERCISE PARTICIPANTS

8. These scenarios and questions are designed to be discussed by an organisation's **senior leadership teams**. We suggest that you also include representatives from relevant departments such as ICT, communications, resilience, emergency planning or business continuity, personnel security, and any others that you may call upon during these type of incidents.

SCENARIOS

These scenarios can be run sequentially to replicate an escalating cyber threat. Please feel free to adapt them to your own organisation.

Scenario 1 – Website defacement
Monday 8 pm:
Media reports claim that a high profile hacker group intend to attack key national information assets due to political issues in Scotland. There is no evidence of specific targets.

- *How might you know about this?*
- *Would you receive any threat intelligence?*
- *How might you respond if at all?*

Tuesday 12 noon:

The Hacker Group claim to have defaced a number of websites in both the public and private sectors. Police Scotland confirm they have been called in to investigate a number of high profile website defacements.

- *Would you be aware of this?*
- *What would you be thinking about?*
- *What would you be doing, if anything?*

Scenario 2 – Distributed Denial of Service attack
Wednesday 9am:
Your IT department reports that your main website is down as a result of a Distributed Denial of Service attack.

- *What would you be thinking about?*
- *What would you be doing?*
- *Do you have incident response plans for Cyber as part of Business Continuity?*
- *Would you have media lines prepared?*

Thursday 9am:
The DDOS attack has ended and your website is up and running. The Media are running a story of unhappy end users who could not transact due to the DDOS attack.

Your organisation is asked to comment, as the media are linking this attack to the claims from hacker groups earlier in the week.

- *What would you be thinking about*
- *What would you be doing?*
- *Who would you be consulting?*
- *Would you review your response arrangements?*

Scenario 3 – Ransomware with potential data theft
Friday, 9 am (1 week on from Scenarios 1 & 2):
Your IT team are now dealing with a Zero Day attack on your network enabling a Ransomware attack to take effect. This also happens to be a key transactional day when payments are due.

- *What are your immediate considerations?*
- *Who else may be involved?*
- *Would the Police be informed?*
- *Is there a policy on ransomware (pay/not pay)?*

Friday 12 noon:

Your IT team now report that the attack has deployed malware which has wormed through the network and is encrypting data as it finds vulnerabilities in patching.

- *What are your immediate considerations?*
- *At what level is this attack being contained / managed?*
- *Does your organisation have the capacity and capability to deal with this attack?*

Friday 2pm:
Your IT team recommend taking the network down as it requires to be isolated to contain the spread and allow them to assess the damage. Staff will not be able to use the network, customers will not be able to transact with the website.

- *Do you have a holding web page?*
- *How do you communicate the issues?*
- *Are your IT team on the CiSP Extranet where solutions could be discussed?*

Friday 4pm:
The Scottish Government gives notice of seeing an identical impact on its network. You are identified as the potential source of infection. At the same time your corporate social media account has been hacked and inaccurate information is being distributed.

- *How do you respond to this?*
- *Ministers are demanding assurances , how do you respond?*
- *How would you seek to reassure your own Board/Senior Management and users?*

Friday 5pm:
The hacker group claim to have significantly disrupted nationally significant services, including that of your organisation, and to have control of your website, network and social media account, claiming security was lax.

- *What are your considerations now?*
- *How to you manage the media?*
- *BBC asks for an interview, who gives it?*

Following week:
You have regained control of your network, website and social media account. The NCSC are reporting that malware is under control, there is no further spread.

- *How would you review the handling of the incident?*
- *Who else may be involved?*
- *Who takes the lead?*
- *Would you share the lessons learned?*

ADDITIONAL QUESTIONS FOR ANY SCENARIO

9. We have included a few questions to ask during the scenarios above. Here are some other suggest lines of question that your facilitator may find useful.

General questions

- How would this scenario be played out?
- Who is involved?
- Who coordinates?
- Who leads?

Reporting/Sharing

- Who would know about this situation and who should know?
- Would you share information about this incident?
- Who would you inform? Senior teams, Police, Government, Information Commissioner etc
- How would you communicate with you staff and stakeholders?

Incident Response

- What incident response plans do you have for this type of event?
- Do you have out of hours procedures for ICT, Comms etc?

Communications

- How, and what, do you communicate with your staff and stakeholders?
- Do you have a media plan or ‘lines to take’?

Solutions

- Who would you contact for specialist advice, support, fixing the problem (e.g. digital forensics, data recovery, etc.)?
- How might you have avoided this incident?
- What staff training measures do you have in place?
- Do you have out of hours monitoring of your systems?

Scottish Government
Riaghaltas na h-Alba
gov.scot

© Crown copyright 2017

This toolkit has been produced by the Scottish Government Cyber Resilience Unit to accompany the Public Sector Action Plan 2017/18

It is intended to be a live document and will be updated as new implementation guidance becomes available.

Please send all comments, questions or additions to cyberresilience@gov.scot