www.gov.scot/cyberresilience

Scottish Government
Riaghaltas na h-Alba
gov.scot

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

THIRD SECTOR ACTION PLAN 2018-20

FOREWORD

THIRD SECTOR ACTION PLAN

Digital technology offers huge opportunities for Scotland as a modern, progressive nation.

Our ability to inform and interact with citizens is being transformed by the digital world, and Scotland's third sector is developing ambitious plans to embrace these opportunities.

But these opportunities also bring new threats and vulnerabilities that we must take decisive action to manage.

The cyber threat is growing. I regard it as vital to our ambitions as a modern, digital nation that our charities, large and small, understand that threat, and are supported to take steps to protect themselves.

No organisation, however large or small, is immune. Cyber attacks are as real a risk to the small, parent-run playgroup that holds a database of children's names and addresses as they are to larger charities delivering employability services to vulnerable adults.

This action plan sets out how we will work in partnership with Scotland's third sector to help tackle the cyber threat. Key to success will be the willingness of Scotland's charities, businesses and public sector organisations to work in partnership to raise fundamental levels of cyber resilience across Scotland.

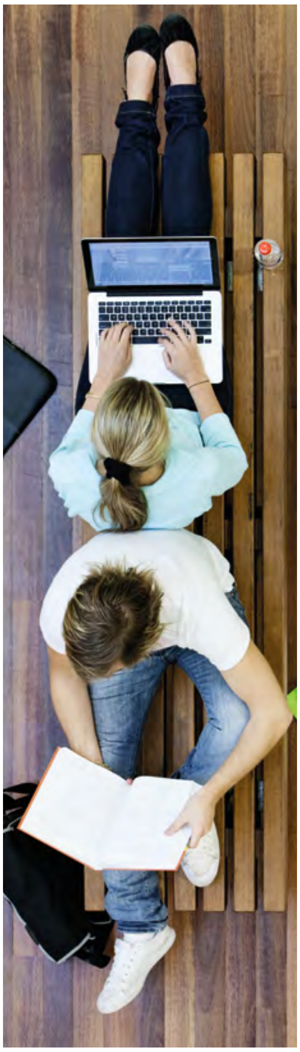
Alongside our action plans on Learning and Skills and Private and Public Sector Cyber Resilience, this plan represents an important step towards our ambition for Scotland to be a world-leading nation in cyber-resilience.

I look forward to working with Scotland's third sector, and our partners in the UK and internationally, to help make this a reality.

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

CONTENTS

EXECUTIVE SUMMARY



EXECUTIVE SUMMARY

1. The importance of cyber resilience in Scotland's third sector has never been greater. Digital technologies bring significant opportunities for our third sector organisations and our economy – but they also bring with them new threats and vulnerabilities that we must take decisive action to manage.

2. The cyber-threat is assessed as a Tier 1 threat to the UK's national security. The National Crime Agency describes it as a "major and growing threat" to UK organisations. Increasingly we have seen major cyber attacks affecting large numbers of organisations worldwide as a result of unintended consequences.

3. The National Cyber Security Centre notes that cybercriminals are becoming increasingly sophisticated, and are able to make judgements on "Return on Investment" when deciding who to target where – the harder the target, the smaller the ROI, the less incentive there is to invest time and money in an attack on those targets. Making Scotland overall, and individual sectors and organisations within Scotland, more cyber resilient may therefore help tip the balance around these judgements in the future, bringing economic advantage to Scottish organisations through an ability to continue operations unaffected by common cyber attacks. Being able to demonstrate that cyber security is taken seriously – that services and customer/client data are protected and resilient – will become increasingly important to an organisation's reputation, which in turn may impact on overall performance.

4. To combat the threat, and to ensure Scotland's overall preparedness and resilience, third sector organisations of all sizes must be supported to adopt a "when, not if" mindset in respect of future cyber attacks, and to take appropriate, proportionate preventative action.

5. This Third Sector Action Plan has been developed in partnership by the Scottish Government and the National Cyber Resilience Leaders Board (NCRLB). It has drawn heavily on the views and expertise of key third sector stakeholders, including representatives of small and medium sized third sector organisations. It sets out the key actions that the Scottish Government and key partners will take during 2018-20 to help make Scotland's third sector, and Scotland overall, more cyber resilient. It aims to realise the opportunities presented by Scotland's strong cyber resilience networks and communities of interest to position Scotland as a world leading nation in cyber resilience.

6. Delivery of the action plan will be coordinated and led by the Scottish Government's Cyber Resilience Unit, working in partnership with the NCRLB and Scottish third sector partners.

KEY ACTIONS

A. Developing a common approach to cyber resilience across the Scottish third sector

7. The Scottish Government and the National Cyber Resilience Leaders Board will work with the NCSC and key partners to consider options for developing a Third Sector Cyber Resilience Framework/Pathway by spring 2019. This would aim to provide a simple, structured way for organisations in Scotland – particularly small and medium sized third sector organisations – to assess the cyber threat to their operations and select an appropriate set of controls or guidance to help them work progressively towards strengthening their cyber resilience. As part of this work, consideration will be given to making clear how such a framework/pathway could align with the core common supply chain cyber security requirements of public and larger private and third sector organisations. This should help drive greater consistency in the demands placed on small and medium sized third sector organisations in supply chains. **(Key Action 1)**

B. Strengthening communications, awareness-raising and systems of advice and support

8. The Scottish Government will work with the National Cyber Resilience Leaders Board, the NCSC and key partners to strengthen the promotion of good cyber resilience practice at all levels in the third sector. This work will include the strengthening of systems of advice and support for the third sector (and other sectors) in Scotland, and activity aimed at communicating key messages and raising awareness of the operational and reputational importance of cyber resilience and effective ways of achieving it. An initial "target landscape" for advice and support will be identified with the goal of achieving this by spring 2019, and thereafter improved on an ongoing basis. **(Key Action 2)**

C. Strengthening partnership working, leadership, and knowledge sharing in Scotland's third sector

9. The Scottish Government will work in partnership with the NCSC, UK Government and key Scottish third sector organisations to help catalyse better cyber resilience practice across Scotland's third sector. From summer 2018, a cross-sectoral group of third sector cyber catalyst organisations will work with the Scottish Government and the NCSC to develop and support implementation of practical solutions to key challenges on an ongoing basis, with an initial focus on:

- strengthening leadership for, and helping drive greater awareness and uptake of good cyber resilient behaviours in, Scottish small and medium sized third sector organisations, including through the use of supply chain measures;
- strengthening coordination and knowledge sharing in respect of cyber resilience across key third sector organisations operating in Scotland; and
- supporting and promoting uptake of key educational initiatives in Scotland, including cyber security apprenticeships.

Appropriate support will be offered to the third sector cyber catalysts to help achieve desired outcomes. The Scottish Government will play a leading role in supporting and driving forward the work of the group, and identifying avenues for delivery. **(Key Action 3)**

D. Supply chain cyber security – leveraging requirements to improve the cyber resilience of Scotland's small and medium sized third sector organisations

10. The Scottish Government will work with third sector organisations and key partners to clarify the common core cyber resilience requirements that are currently placed on third party suppliers, and their relationship to wider standards and guidance. Thereafter, the potential for greater cross-sectoral alignment and cooperation in respect of common core supply chain requirements will be explored, with the goal of promoting greater coherence across Scotland's public, private and third sectors. A key aim of this alignment will be to improve the cyber resilience of Scotland's small and medium sized third sector organisations as part of the supply chain of larger public, private and third sector organisations. **(Key Action 4)**

E. Strengthening incentives to improve cyber resilience in Scotland's third sector

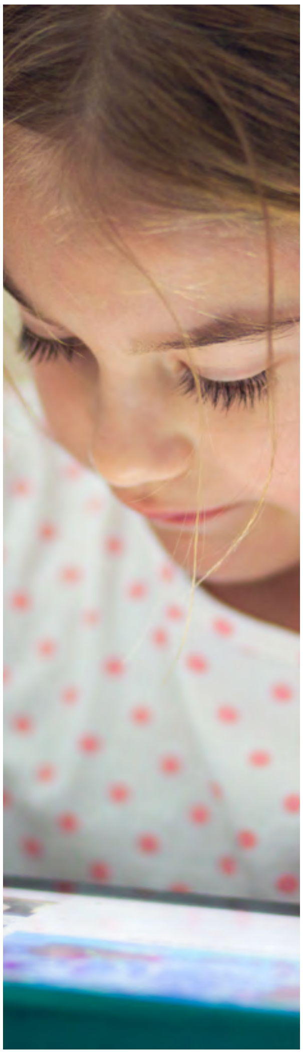
11. The Scottish Government and the National Cyber Resilience Leaders Board will work with the UK Government and key third sector stakeholders to consider how best to strengthen incentives to support the uptake of cyber security standards/accreditation, and the adoption of good cyber resilience practice more generally. This will include the continuation of a modified voucher scheme to support the achievement of Cyber Essentials or Cyber Essentials Plus by Scottish small and medium sized third sector organisations. On the basis of activity across all action plans, we aim to at least double the number of organisations across the public, private and third sectors holding Cyber Essentials or Cyber Essentials Plus certification in Scotland during Financial Year 18-19. **(Key Action 5)**

F. Benchmarking, Monitoring and Evaluation

12. The Scottish Government will work with the NCRLB, the NCSC, Regulatory Bodies and key partners to develop appropriate benchmarking, monitoring and evaluation arrangements for implementation by spring 2019. **(Key Action 6)**

A summary of these key actions, along with timelines, can be found at **Annex A** to this action plan.

INTRODUCTION AND BACKGROUND



1

1. INTRODUCTION AND BACKGROUND

1. **Safe, secure and prosperous: a cyber resilience strategy for Scotland**[1], was published in 2015. It set out the Scottish Government's vision for Cyber Resilience in Scotland:

Scotland can be a world leader in cyber resilience and be a nation that can claim, by 2020, to have achieved the following outcomes:

(i) Our people are informed and prepared to make the most of digital technologies safely.

(ii) Our businesses and organisations recognise the risks in the digital world and are well prepared to manage them.

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

(iv) We have a growing and renowned cyber resilience research community.

(v) We have a global reputation for being a secure place to live and learn, and to set up and invest in business.

(vi) We have an innovative cyber security, goods and services industry that can help meet global demand.

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

2. "Safe, secure and prosperous" is closely aligned with the UK National Cyber Security Strategy[2], which sets out the UK Government's strategic approach to making the UK secure and resilient in cyberspace. Cyber security is a reserved matter, but it has strong implications for the resilience and security of Scotland as a whole. Scotland has unique partnerships and networks that support resilience across all sectors. As such, the Scottish Government works closely with key partners such as the UK National Cyber Security Centre to ensure appropriate alignment between work on cyber resilience at the UK and Scottish levels.

3. This action plan has been produced by the National Cyber Resilience Leaders Board (NCRLB) and its third sector representatives, in partnership with the Scottish Government. It has drawn heavily on the views and expertise of key third sector stakeholders. It sets out the key actions that the Scottish Government and key partners in the third sector will take during 2018-20, in order to make progress particularly towards outcomes (i) and (ii) above:

> ***Our people are informed and prepared to make the most of digital technologies safely.***
>
> ***Our businesses and organisations recognise the risks in the digital world and are well prepared to manage them.***

It aims to realise the opportunities presented by Scotland's strong cyber resilience networks and communities of interest to position Scotland as a world leading nation in cyber resilience.

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

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

The goals of this action plan and its relationship to wider work on cyber resilience in Scotland

4. The specific goals of this action plan are to move Scotland closer to the above outcomes, and to our vision of being a world leading nation in cyber resilience, by:

- Driving greater levels of **good cyber resilience practice** across Scotland's third sector, particularly amongst our **small to medium sized third sector organisations**, thus helping to raise overall fundamental levels of cyber resilience in the third sector.

  As part of this, there will be a particular focus on **raising awareness** and **increasing learning opportunities** for Scotland's third sector organisations in respect of cyber resilience; and

- Promoting **greater coherence and alignment** of work on cyber resilience across **the third sector and Scotland's public and private sectors**.

5. The Scottish Government and the NCRLB are developing and implementing complementary action plans for the **public and private sectors.** The first of these, the Public Sector Action Plan on Cyber Resilience, was published on 8th November 2017[3], and the Private Sector Action Plan is expected to be published alongside this Third Sector Action Plan. The aim is for all sectors in Scotland to adopt a common or aligned approach to cyber resilience where possible. As such, development of this Third Sector Action Plan has had regard to the public and private sector action plans.

The NCRLB is of the view that the Scottish and UK Governments should support Scotland's third, public and private sectors to work together as partners, ensuring strong leadership around cyber resilience and digital enablement for the benefit of all citizens and businesses. Many third and private sector organisations are both the supply chain and the purchasers of public sector services, thus increasing the importance of commonality and coherence. In simple terms, the more our citizens and organisations speak a "common language" around cyber resilience, the more likely it is that we will be able to work in partnership to make progress. Identifying common core cyber resilience requirements across more sectors, and encouraging sharing of good practice around cyber resilience, is also expected to help promote greater levels of cyber resilience and potentially reduce compliance burdens.

6. The Programme for Government 2017-18 also committed the Scottish Government and key partners to develop action plans in the following key areas:

- **Learning and Skills**, focused on how to ensure that (i) our citizens have the appropriate understanding, knowledge and behaviour to live and work safely and securely in the digital world; and (ii) our cyber specialist workforce have the appropriate skills. The success of this action plan, which was published on 7 March 2018, will be vital to establishing a genuine **culture of cyber resilience** in Scotland (including amongst third sector organisations), and to the longer term success of the third, public and private sector action plans.
- **Economic opportunity**, focused on how to seize fully the economic opportunities presented by the achievement of fundamental cyber resilience, and take a visible, global role in thought-leadership, research, development and innovation relating to cyber resilience. We expect this action plan to be published in Q3 2018.

[3] https://beta.gov.scot/policies/cyber-resilience/

7. To ensure efficiency and maintain momentum, these plans are being developed to differing timelines. Work to identify and take account of the strong interrelationships between the actions set out in this plan and other action plans is being undertaken on a regular basis by the Scottish Government and the NCRLB. In the future, our expectation is that this third sector action plan will be merged with other action plans to constitute a single action plan focused on Scotland's cyber resilience, as part of work on our overall security and resilience.

8. While the focus of this action plan is on cyber resilience, the actions set out in this plan will also help ensure that Scottish third sector organisations are meeting key requirements in respect of **protecting personal data**, which will be strengthened by the General Data Protection Regulation (GDPR)[4] from May 2018. The Information Commissioner has, for example, noted publicly that achieving Cyber Essentials accreditation can assist with preparing for GDPR. Third sector organisations should in general consider how work on cyber resilience aligns with wider work on GDPR compliance.

9. The action plan recognises that the third sector in Scotland is of considerable scale and complexity. Some organisations are of significant technical sophistication, or handle significant amounts of personal data, while others operate only very basic IT systems and may be concerned with delivery of services on a small scale. One of the biggest challenges in developing this action plan has been the need to take account of these significant differences in scale and risk profile. The NCRLB third sector steering group and other key third sector partners have offered advice to help ensure the action plan meets multiple needs.

The importance of cyber resilience to Scotland's third sector

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

11. The third sector in Scotland plays a huge role in delivering public services, with over one-third of funding[5] coming directly from the public sector, totalling almost £1.7bn per year. By the nature of the work they do, third sector organisations often deal with highly sensitive personal data (e.g. on health, employment etc.). However, evidence suggests that there is a need to build the capacity and resilience of third sector organisations to operate safely and securely in a digital world.

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

[5] https://scvo.org.uk/post/2016/01/02/briefing-public-sector-funding

12. The importance of ensuring cyber resilience in Scotland's third sector has never been greater. In the view of the NCRLB, there are compelling arguments for Scotland's third sector to work together to improve overall levels of cyber resilience now, supported by the Scottish Government. A number of factors make this so. They include:

(i) The scale and nature of the cyber threat to the digital systems upon which our economy and our public services increasingly rely, and the risks this presents to: our ambitions for Scotland's digital economy; our overall security and resilience; and the success of individual organisations in Scotland: Scotland's refreshed digital strategy[6] emphasises that the Scottish Government and its partners are fully committed to harnessing the benefits of digital technology across our economy and society, in order to deliver a step-change in productivity. Digital connectivity offers significant opportunities for innovation, inclusive economic growth and improved public services. However, with these opportunities come new threats and vulnerabilities, and it is imperative that we take these seriously and take action to address them and minimise their disruptive effects. Much of our prosperity now depends on our ability to secure our technology, data and networks from the threats we face. Yet cyber attacks are growing more frequent, sophisticated and damaging when they succeed.

The cyber threat to third sector organisations of all sizes is increasing, in common with the threat to the public and private sectors. This is outlined by the NCSC's February 2018 Cyber Threat assessment on the UK Charity sector[7]. Some charities are aware their data is sensitive, valuable and vulnerable to attack. However, the NCSC believes that many charities – particularly smaller ones – do not realise this and do not perceive themselves as targets.

The NCSC notes that the culture of openness in the sector makes charities particularly vulnerable to some types of cyber-criminal activity, such as cyber-enabled fraud and extortion. They also judge there is considerable variation in charities' understanding, approach to, and application of, cyber security.

Smaller charities may not consider it a priority to commit resources to cyber protection, perhaps in the belief that cyber security will be expensive and divert money away from frontline expenditure. Or it is possible they do not fully understand the threat.

The 2016 Lloyds Banking Group Digital Index identified that 49% of UK charities lack basic organisational digital skills and capability (compared with 38% of small businesses). This includes the ability to keep themselves 'safe' online, protecting their own data and that of their service users.

The cyber threat can be **targeted or indiscriminate**. Even where cybercriminals attempt to target specific organisations, the nature of the cyber threat is such that there can be significant unintended wider consequences. Third sector organisations of all sizes in Scotland need to understand the risks they face, and be confident they can take proportionate action to mitigate it. The nature of the cyber threat is such that this action is most likely to be effective if third sector organisations commit to **working together**, both within the third sector and across the public and private sectors, to mitigate the cyber threat across Scotland. The greater the "herd immunity" to the cyber threat in Scotland, the more secure all businesses are likely to be.

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

[7] https://www.ncsc.gov.uk/guidance/cyber-threat-assessment-uk-charity-sector

(ii) Legislative changes and their potential legal, financial and reputational impact: The new GDPR and the Security of Network and Information Systems (NIS) Directive both come into force in May 2018, and place new duties on third (GDPR only) and public and private sector organisations to ensure the protection of personal data and the continuity of essential services reliant on network and information systems, and to report personal data/cyber security breaches. Third sector organisations subject to these provisions could face significantly increased administrative fines of up to £17 million for data breaches or cyber security failures leading to service failure. These legislative changes should drive greater awareness of the importance of cyber resilience and the need to have appropriate technical protections for personal data in place. The actions set out in this plan are aimed at supporting organisations to understand how better to comply with the cyber aspects of such legislative duties.

(iii) Operational advantage: The flip side of these threats is that there is a significant operational advantage for Scottish third sector organisations, whether collectively or at an individual level, in working to become more cyber resilient. These opportunities include:

- **Avoidance of cost and disruption to business**: We cannot fully evaluate the likely impacts of a large, global scale attack across public, private and third sectors but it is widely anticipated that there will be an attempt to achieve this in the near future. Available evidence suggests there would be significant short and longer term disruption across critical digital infrastructure and, as a result, serious disturbance to business activity which would affect us all. The NCSC has indicated publicly that the UK is likely to face its first major "category one" cyber-incident in the next few years. (For the purposes of comparison, the WannaCry ransomware attack in May 2017 was a category two incident.) Lloyd's of London has reportedly assessed that a serious cyber-attack could cost the global economy more than £92bn, which is as much as catastrophic natural disasters such as Hurricanes Katrina and Sandy. This risk adds to the urgency with which all sectors need to review and address their security.

  Recent research by DCMS[8] found that one in five charities – surveyed for the first time in 2018 – identified a breach in the past 12 months. Among these, the most common were: staff receiving fraudulent emails (74%); others impersonating the organisation online (27%); and viruses and malware (24%). Small charities can face failure as a result of ransomware attacks, if they have not taken appropriate cyber security precautions. Insurers may also increase or reduce insurance costs depending on their assessment of an organisation's vulnerability to cyber-attack.

  The NCSC notes that cybercriminals are becoming increasingly sophisticated, and are able to make judgements on "Return on Investment" when deciding who to target where – the harder the target, the smaller the ROI, the less incentive there is to invest time and money in an attack on those targets. Making Scotland overall, and individual sectors and organisations within Scotland, more cyber resilient may therefore help tip the balance around these judgements in the future. This may be expected to bring an operational advantage to Scottish organisations through an ability to continue operations unaffected by common cyber attacks.

[8] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018

- **The ability to meet supply chain cyber security requirements in the public, private and third sectors**: Many Scottish third sector organisations compete to deliver key contracts for public sector organisations (and some private and other third sector organisations). As these sectors strengthen their focus on cyber security in their supply chains, third sector organisations that can demonstrate appropriate levels of cyber resilience should find they are better placed to compete with other potential providers for such contracts.
- **Reputation**: As citizens' understanding of the cyber threat increases, and as the profile of cyber attacks and data breaches continues to rise, the importance that clients, funders, insurers and others place on cyber resilience is likely to increase. Being able to demonstrate that cyber security is taken seriously may become increasingly important to a third sector organisation's reputation, which in turn may impact on overall performance.

13. Against this background, the NCRLB has articulated its view that Scotland's third sector must make demonstrable progress towards establishing fundamental standards of cyber resilience that are in line with world-leading nations. Cyber resilience should be seen as just as fundamental to third sector organisations in Scotland as health and safety currently is.

14. The NCRLB emphasises that cyber resilience is as much a **cultural** issue as a technical one. They view it as vital that Scotland's third sector organisations understand and manage the cyber threat at **Board/senior committee level**, and take action to promote a culture of cyber security at all levels of the organisation (the Cyber Resilience **Learning and Skills Action Plan** sets out the actions we will take to achieve this transformational cultural change through our systems of formal and informal learning in Scotland). The NCRLB views it as being vitally important that small and medium sized third sector organisations are supported to understand and manage the threat in an appropriate and proportionate way – a one-size-fits-all approach to cyber resilience in Scotland's third sector is not desirable.

Current levels of cyber resilience in Scotland's third sector

15. In developing this action plan, the NCRLB and the Scottish Government have taken account of the diversity of the third sector in Scotland. There are approximately 24,000 registered charities and 20,000 voluntary groups. These range from local community groups run by volunteers to large housing associations and health and social care providers, with multi-million pound budgets and thousands of staff. The approaches to cyber resilience taken across these organisations will inevitably differ significantly according to size, risk profile, resources and capacity.

16. Currently, we do not have a comprehensive picture of the state of cyber resilience across the Scottish third sector. However, evidence suggests that there is a need to build the capacity and resilience of third sector organisations of all sizes to operate safely and securely in a digital world. Many lack an understanding of the issues around cyber resilience and the need to protect themselves. Key issues include: an expanding range of digital devices being used, without appropriate policies or protection; poor cyber hygiene and compliance; and legacy and unpatched systems. The need for a significant increase in **awareness and skills** around cyber resilience across the sector has been highlighted by NCRLB members.

17. To help create a more cyber resilient third sector, several pilot approaches have been trialled through senior-level engagement and an SCVO small grants programme to support small and medium sized charities to achieve Cyber Essentials certification. Grants of up to £1500 were made available to help cover the Cyber Essentials assessment fee and some of the associated IT support needed to achieve certification.

An evaluation of this funding pilot will be completed in May 2018. In addition, there has previously been financial encouragement (£1500 grants) through the Digital Scotland Business Excellence Partnership for 200 SMEs to become Cyber Essential certified – in 2016 Scotland was the only part of the UK providing this initiative. Key action 5 sets out proposals for this scheme to be continued and to include the third sector, drawing on learning from the initial phase and the SCVO pilot.

18. A number of mechanisms exist to encourage the sharing of threat intelligence across the Scottish and wider UK third sector. The NCSC has worked with industry to set up the Cyber Security Information Sharing Partnership (CiSP) to provide a secure environment in which to share cyber threat intelligence, increasing situational awareness and reducing the impact on organisations across Scotland and the rest of the UK. The Scottish Government has used National Cyber Security Programme funding to support a CiSP (and Cyber Essentials) coordinator role, located within Scottish Business Resilience Centre (SBRC), to promote membership of CiSP, including in the third sector. Since the coordinator was appointed in November 2016, active membership of SciNet (the Scotland-specific area of CiSP) has increased from 122 to 307, an increase of 152%. This makes SciNet the largest geographical group on CiSP within the UK. Activity to promote increased active Scottish third sector membership of CiSP, with a goal of ensuring our charities are better informed around the cyber threat, will be supported by this plan.

19. There is only limited information at present on the levels of cyber security accreditation achieved across different sectors in Scotland. Some larger third sector organisations are accredited to relatively sophisticated standards such as ISO 27001/2, although there is no publicly available central registry to make clear which organisations have achieved this, and to which parts of their networks such accreditation applies (companies holding such accreditation often choose to advertise their compliance for business/reputational purposes). Uptake of the NCSC-endorsed Cyber Essentials[9] scheme across Scotland is improving. At this time we do not have a breakdown by public, private and third sector.

Scottish public sector organisations do not currently require the adoption of certification such as Cyber Essentials by third and private sector organisations wishing to do business with them (the UK Government currently mandates this only if bidding for central government contracts which involve handling of sensitive and personal information and provision of certain technical products and services). The practice of third sector organisations with extensive supply chains in Scotland varies significantly, with no consistent approach currently in place (although there is effectively much commonality of approach). Implementation of the NIS Directive, and NCSC technical guidance in respect of supply chain security, may assist with developing greater consistency in some of the key sectors it covers (e.g. healthcare).

[9] The Cyber Essentials scheme offers a mechanism, endorsed by the National Cyber Security Centre, for organisations to demonstrate to customers, investors, insurers and others that they have adopted five critical network controls to guard against the most common forms of cyber-attack taken essential precautions. See: https://www.cyberaware.gov.uk/cyberessentials/files/scheme-summary.pdf for further details.

Both this plan and the Public Sector Action Plan on Cyber Resilience[10] propose work to help improve the uptake of appropriate cyber security accreditation/certification across Scotland's third sector, particularly in respect of Cyber Essentials and Cyber Essentials Plus. These include proposals to develop appropriate, proportionate, more aligned supply chain procurement policies in respect of cyber security accreditation/certification.

On the basis of all this activity, we aim to at least double the number of organisations across the public, private and third sectors holding Cyber Essentials or Cyber Essentials Plus certification in Scotland during financial year 18-19.

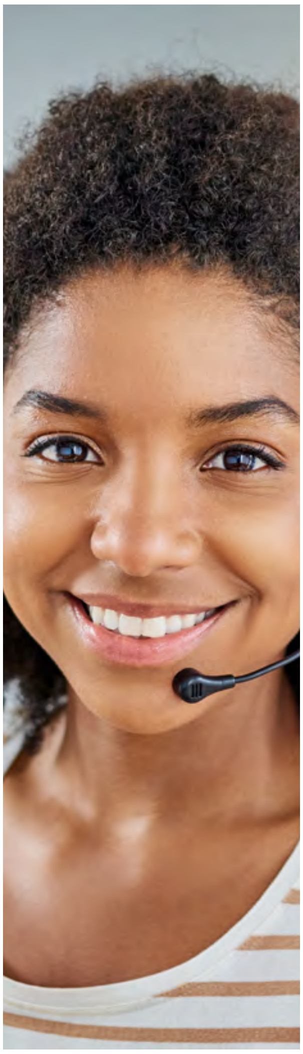
20. There is currently a lack of a clear **Framework/Pathway** for Scottish third (and public and private) sector organisations to work within and towards when managing the cyber risk, providing assurance and opportunities for benchmarking. Feedback suggests this is particularly problematic for small and medium sized third sector organisations, who lack the resources that large organisations have to make sense of the many different existing standards. Cyber Essentials and Cyber Essentials Plus offer a clear entrance point – however, even these may be beyond the initial reach of some smaller charities who have yet to achieve even a basic understanding of the cyber threat. Scottish third sector organisations have indicated that achieving greater clarity on a progressive cyber threat management model beyond Cyber Essentials, towards more sophisticated measures thereafter, would be helpful.

Such a Framework/Pathway would need to have a particular emphasis on supporting small and medium sized third sector organisations to understand the cyber risk and what options they have to manage it on a progressive basis. It must encompass standards or guidance that, at more sophisticated levels, ensure a robust, holistic, effective approach to cyber resilience, avoiding "checklists" and encouraging the management of cyber security with a multi-layered approach that encompasses people, processes and technology. It must also be adaptable to ensure it keeps up with fast-paced technological change and emerging threat. This action plan sets out proposals for the Scottish Government and the NCRLB to work with key third sector organisations, and key partners such as the NCSC, to explore the potential for the development and endorsement of such a Framework/Pathway, making it easier for our organisations (especially small and medium sized third sector organisations) to understand the cyber threat and work progressively towards more sophisticated ways of managing it. (See Key Action 1)

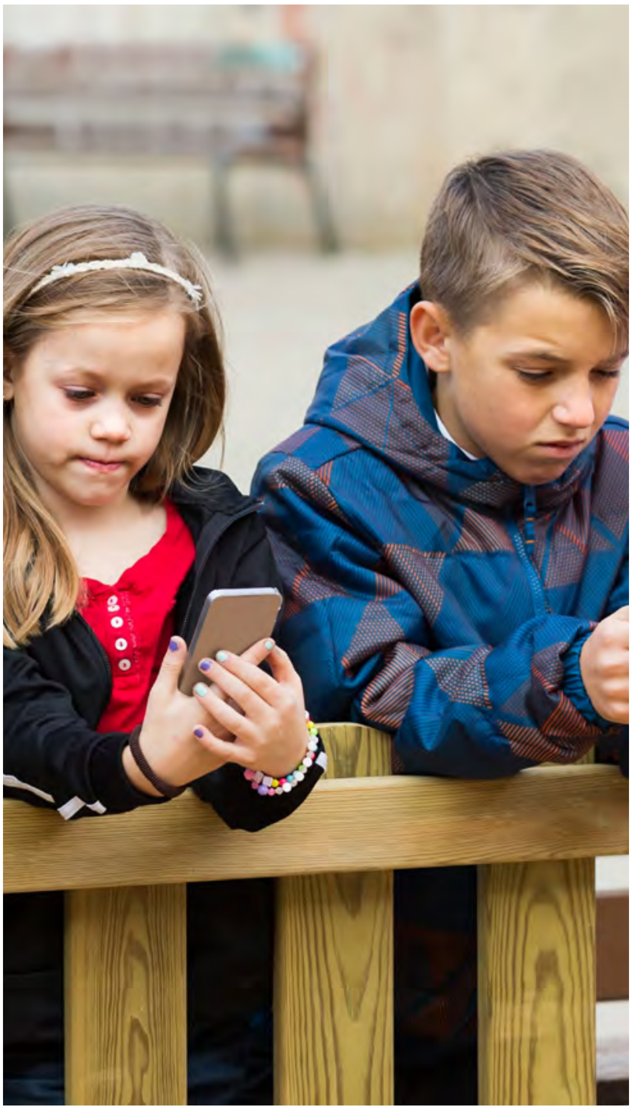
21. There is no clear monitoring framework in place to provide Government, Parliament and citizens with a sense for the progress being made towards the overall cyber resilience of Scotland's third sector (the public sector action plan sets out proposals to establish such a monitoring framework for public bodies). The development of the proposed Scottish Third Sector Cyber Resilience Framework/Pathway (Key Action 1) could help provide a consistent way of assessing the prevalence of good (accredited or certified) practice and perception of risk more widely across the third sector. Key Action 6 sets out a commitment to develop appropriate monitoring arrangements on the basis of existing and future information sources, to improve our understanding of the extent to which good cyber resilient behaviour is being adhered to across the Scottish third sector.

[10] See: https://beta.gov.scot/policies/cyber-resilience/cyber-resilience-action-plans/

KEY ACTIONS



2



2. KEY ACTIONS

Introduction

22. This section provides detail on the key actions that the Scottish Government and its partners will take during 2018-20 to help address these issues and ensure confidence in standards of cyber resilience in Scotland's third sector.

23. Delivery of the action plan will be coordinated and led by the Scottish Government's Cyber Resilience Unit, working as close partners with the NCRLB, the NCSC, the UK Government and key Scottish third sector partners.

24. The Scottish Government is clear that it cannot achieve a strong, cyber-resilient third sector in Scotland by taking action on its own. While the Scottish Government will offer targeted funding, support and direction where it is able to do so (as outlined in this action plan), achieving a world leading cyber resilient third sector will also require leadership, commitment and resource from third sector organisations of all sizes in Scotland. As work is taken forward to drive higher levels of cyber resilience in Scotland's public and private sectors, potential links or opportunities for cross-sectoral knowledge-sharing will also be identified.

25. Action to promote cyber resilience in Scotland's third sector will of course continue beyond 2018-20. This action plan will be refreshed at the end of this period, to take stock of progress to date and ensure continued progress.

Collaborative working, levers and influence

26. The Scottish Government's preferred approach to driving up levels of cyber resilience in Scotland's third sector is one of **collaborative working** with partners – to that end, this action plan sets out proposals to work in close partnership with the third sector, based on a shared understanding of the importance and benefits of strong cyber resilience across the sector.

27. There are, nevertheless, some areas in which more direct levers of influence may be used to influence third sector partners in different sectors and of different sizes to take action in respect of cyber resilience. These levers sit at different levels (UK, Scottish, local) and with different organisations. The key actions set out in this action plan seek to maximise use of these levers, which include:

- **Legislation and regulation**: Cyber security is a reserved issue. As part of the "Defend" strand of the National Cyber Security Strategy, the UK Government is working with international partners to make sure the right regulatory framework is in place in the UK and Europe – one that incentivises better cyber security but avoids unnecessary burdens on business. This work includes implementation of the **Security of Network and Information Systems (NIS) Directive** into UK law from May 2018, which will place requirements on Operators of Essential Services (OES), specifically in key areas of the private and public sectors, to improve certain aspects of cyber security. Scottish third sector organisations that form part of OES supply chains should expect to deal with an increased focus on their cyber resilience. The **General Data Protection Regulation** (GDPR) will also come into force from May 2018, and will apply to all third sector organisations handling personal data. Both pieces of law will effectively require third sector organisations to ensure they have appropriate cyber security arrangements in place, either to ensure continuity of essential services or to protect personal data. Significant **fines** will be able to be levied by the Information Commissioner or Competent Authorities in the event of breaches.

- **Existing regulatory and advisory practice**: Regulators, such as the Office of the Scottish Charity Regulator, support good management and governance. They can therefore play an important role in promoting security and resilience.

- **Supply chain requirements**: Whilst large organisations account for only a small percentage of total charity numbers, they represent a significant share of output, and they operate materiel, service and information supply chains that reach into Scottish and wider UK and international structures at all levels. Small and medium sized third sector organisations' supply chain scope is often smaller and there may not be as many chain partner relationships to manage, but they often form part of more complex business chain activity. The NCSC notes[11] that cyber criminals can identify the organisation with the weakest cyber security within the supply chain, and use the vulnerabilities present in their systems to gain access to other members of the supply chain, including large third sector organisations.

  Large organisations are both suppliers and contractors and there is an interdependency between the public and third sectors. The public sector in Scotland is a significant purchaser of third sector goods and services., while some larger Scottish third sector organisations have extensive supply chain arrangements, within and outside Scotland. By placing proportionate requirements on third sector organisations in respect of cyber security, both to ensure their own cyber security and to drive up overall levels of cyber resilience in Scotland, public sector organisations can potentially raise awareness of the importance of cyber resilience and wield significant influence over the uptake of good practice and accreditation, etc. not only in the third sector but also in the private sector. The Public Sector Action Plan on Cyber Resilience sets out a proposal to develop a policy on supply chain cyber security for the public sector, which is expected to align with NCSC guidance on supply chain security (including requirements in respect of Cyber Essentials certification, based on management of risk). This third sector action plan includes proposals on supply chain cyber security at Key Action 4.

- **Financial and other incentives**: While the public sector (in common with other sectors) at all levels is currently operating under significant resource constraints, there is the potential for targeted financial and other incentives to be offered to third sector operators (particularly small and medium sized third sector organisations) to drive a greater focus on cyber resilient behaviour. These could conceivably include, for example, subsidies for organisations achieving or seeking to achieve certain levels of cyber security accreditation.

28. In developing this action plan, the Scottish Government and the NCRLB have sought the views of the UK Government (including the NCSC) and key regulatory bodies. These partners will also play a vital role in the implementation of the plan, and arrangements will be put in place to ensure continued collaboration and coordination as the actions outlined in this plan are taken forward.

[11] https://www.ncsc.gov.uk/guidance/supply-chain-security

KEY ACTIONS

A: Develop a common approach to cyber resilience across the Scottish third sector

Key Action 1

The Scottish Government and the National Cyber Resilience Leaders Board will work with the NCSC and key partners to consider options for developing a Third Sector Cyber Resilience Framework/Pathway. This would aim to provide a simple, structured way for organisations in Scotland – particularly small and medium sized third sector organisations – to assess the cyber threat to their operations and select an appropriate set of controls or guidance to help them work progressively towards strengthening their cyber resilience.

As part of this work, consideration will be given to making clear how such a framework/pathway could align with the core common supply chain cyber security requirements of public and larger private and third sector organisations. This should help drive greater consistency in the demands placed on small and medium sized third sector organisations in supply chains.

Third sector organisations in Scotland – particularly small and medium sized third sector organisations – will then be encouraged, incentivised and supported to work towards implementing the most appropriate cyber resilience approach, based on the cyber threat to their operations. (Timing: by spring 2019, and thereafter on an ongoing basis dependent on confirmation of viability)

29. There exists a wide range of standards, guidance and accreditation schemes within the UK and internationally that can help provide assurance to third sector organisations and their customers with regard to managing the cyber threat. However, Scotland and the wider UK currently lack a clear, graduated hierarchy of such measures that can assist third sector organisations (particularly smaller or micro charities) to identify the most appropriate outcomes, standards or accreditations to work towards in order to manage progressively higher levels of cyber threat, and to offer a way of benchmarking against other third sector organisations.

30. Key third sector partners have indicated their support for the development of an easily recognisable Third Sector Cyber Resilience Framework/Pathway, with the aim of increasing awareness of the core common cyber resilience measures (via guidance, standards or accreditation schemes) that they should be considering implementing dependent on the cyber threat to their operations.

31. Feedback from third sector stakeholders has identified that any such Framework/ Pathway must be informed by:

- **Existing standards or guidance**, particularly those endorsed by the National Cyber Security Centre such as Cyber Essentials and the 10 Steps to Cyber Security. Unless particular gaps are identified in the landscape, there is no appetite to create fresh standards for the third sector – rather, the aim is to help make sense of existing ones;
- **Existing and planned practice in respect of supply chain cyber security** amongst larger public, private and third sector organisations – as set out later in this action plan, a key goal should be to promote greater awareness and alignment across different sectors in respect of the core common cyber security requirements they place on small and medium sized third sector suppliers, and to enhance understanding amongst small and medium sized third sector organisations of those core requirements (see Key Action 4); and
- **The views of Scottish small and medium sized third sector organisations** on the types of guidance or support that are most likely to help them begin and sustain their journey towards greater cyber resilience. On the basis of initial discussions, the Framework/Pathway should have a particular focus on supporting and influencing the third sector to have in place a **Board/Senior Management commitment** to understand and manage the risks arising from the cyber threat. There should also be a clear focus on **staff training and awareness**.

32. In undertaking this work, the Scottish Government, the NCRLB third sector steering group, the NCSC and key third sector partners (including the third sector cyber catalysts) will work together to:

- develop a stronger understanding of the **core cyber resilience requirements** that are currently encompassed by NCSC schemes and guidance, other common standards and key supply chain policies as they apply to the Scottish third sector (particularly small and medium sized third sector organisations), and how these relate to **progressively higher levels of cyber threat**;
- consider the development of **strengthened guidance** on the basis of this work where necessary, including in respect of public, private and third sector organisations' supply chain requirements (see Key Action 4), and the dissemination of such guidance appropriately via key partners, with a view to driving greater consistency in the messages going to third sector organisations (especially small and medium sized third sector organisations); and
- building on this work, consider options for the development of a **Third Sector Cyber Resilience Framework/Pathway**, with a particular focus on supporting small and medium sized third sector organisations to assess the cyber threat to their operations and select an appropriate set of core controls (via guidance, standards or accreditation schemes) to improve their cyber resilience.

33. In view of the fact that many strategic organisations operating in Scotland will already be working to a range of UK and international regulatory requirements, it is expected that any such Framework/Pathway is most likely to be of use for smaller organisations (especially small and medium sized third sector organisations) in terms of assessing their own organisational cyber resilience. Such a framework, if appropriately aligned with common core supply chain requirements, could also drive benefits for larger organisations seeking to manage supply chain risk.

34. A **broad initial concept** for the development of a Third Sector Cyber Resilience Framework/Pathway is at **Annex B**. The potential for a pilot of this approach (or similar) is currently under discussion with the National Cyber Security Centre, the Scottish Council of Voluntary Organisations and other key partners.

One potentially key factor in securing greater awareness and take-up of any such Framework/Pathway will be an understanding of how **supply chain cyber security policies** in the public, private and third sectors broadly align with its contents. Key Action 4 in this action plan and Annex B set out how an understanding of the alignment of these policies could help ensure the success of any Framework/Pathway.

Developments in this area at the UK level, including in respect of NIS/NCSC guidance around supply chain cyber security, will be influential. The EU is also considering the development of a framework to govern European cybersecurity certification schemes, allowing schemes to be established and recognised across the EU in order to address market fragmentation. The current EU proposal outlines the minimum content of what would be required under such schemes. Ensuring alignment with this EU-level framework will be key.

35. The Scottish Public Sector Action Plan sets out a commitment to develop a Scottish Public Sector Cyber Resilience Framework. Alignment between this and any Third Sector Cyber Resilience Framework/Pathway will be carefully considered once both have been finalised.

36. The NCRLB emphasises that accreditation, while a helpful way of assessing and demonstrating good practice, does not offer a “silver bullet” to improving cyber security. Guidance will ensure that third sector organisations and their customers are aware that, ultimately, good cyber resilience is a **cultural issue**. Organisations should take care not to reduce cyber resilience to a “tick box” exercise.

B: Strengthening communications, awareness-raising and systems of advice and support

Key Action 2

The Scottish Government will work with the National Cyber Resilience Leaders Board, the NCSC and key third sector partners to strengthen the promotion of good cyber resilience practice at all levels in the third sector.

This work will include the strengthening of systems of advice and support for the third sector in Scotland. Communications activity will be aimed at raising awareness of the importance of cyber resilience and effective ways of achieving it. An initial "target landscape" for advice and support will be identified with the goal of achieving this by spring 2019, and thereafter improved on an ongoing basis.

37. It is vital that organisations across the Scottish third sector understand the importance of the cyber threat, know where to go to find trusted advice and support, and can take action to enhance their own cyber resilience.

38. The Scottish Government will work with the National Cyber Resilience Leaders Board, the NCSC and key third sector partners to support key messaging and to strengthen the promotion of good cyber resilience practice at all levels in the third sector.

39. The NCRLB have identified that there is a need to "declutter" and simplify the landscape in Scotland with respect to advice and support on cyber resilience for third sector organisations. Organisations of all sizes in Scotland should be able to discover the best official sources of advice and support in respect of cyber resilience, and be provided with high quality, consistent and easy-to-understand messages and advice products to support this. They should also understand where to go to find high quality, independent private sector expertise on cyber security.

40. To help achieve this, the Scottish Government and the NCRLB will work with Police Scotland and other key public and third sector partners to:

- finalise **analysis** on the cyber resilience advice and support landscape in Scotland, to identify the key strengths and weaknesses in current arrangements;
- develop and implement proposals to **promote easier access to trusted sources of advice and support on cyber security** for the third sector, with a focus on "decluttering" and simplifying the landscape; and
- build on this work to ensure third sector organisations are provided with **high quality, consistent, and easy-to-understand messages and advice products** through key partners to help raise awareness and support organisations' progress in respect of cyber resilience. These communications and awareness raising activities will be delivered through a range of key partners, including:
  - Third Sector representative organisations;
  - The Scottish Government, local authorities and other government bodies or agencies, including Skills Development Scotland and Business Gateway;
  - Regulatory bodies;
  - Third sector cyber catalyst organisations (see Key Action 3).
  - Specific charity bodies.

Awareness raising activities will have a particular focus on:

- Increasing **understanding of the cyber threat**, its importance to third sector organisations of all sizes, and the **business arguments** for adopting good practice.
- Raising awareness of the **Scottish Third Sector Cyber Resilience Framework/ Pathway** (if developed successfully – see Key Action 1), and the operational benefits of managing the cyber risk more effectively (including meeting the requirements of Scottish public sector procurement policies and those of third and private sector cyber catalysts).
- Providing/signposting best practice guidance on how to build cyber resilience effectively into **workplace learning**, and opportunities to benefit from **educational initiatives/apprenticeships** and **retraining and upskilling programmes**, in line with the **Learning and Skills action plan[12].**
- Publicising widely any **incentives** that exist or that have been developed (see Key Action 5) to support the achievement of standards/accreditation schemes.
- Promoting and encouraging uptake of **free, reputable services** aimed at strengthening cyber security in the third sector.
- Promoting and encouraging **active**[13] **membership of the Cybersecurity Information Sharing Partnership (CiSP)** by eligible organisations.
- Promoting and encouraging small and medium sized third sector organisations to **access key NCSC resources** available from the NCSC website, including Cyber Alerts and Advisory and Guidance reports, incident management guidance, etc.
- Supporting the third sector with the process and follow-up on confidently **reporting cyber incidents**, working with Police Scotland, NCSC and OSCR.

41. The role of the NCSC as a trusted source of advice is expected to be central to this work.

[12] https://beta.gov.scot/policies/cyber-resilience/learning-and-skills/

[13] Proportionate to the size and resources of the member organisation.

C: Strengthening partnership working, leadership and knowledge sharing in Scotland's third sector

Key Action 3

The Scottish Government will work in partnership with the NCSC, UK Government and key Scottish third sector organisations to help catalyse better cyber resilience practice across Scotland's third sector.

From June 2018, a cross-sectoral group of third sector cyber catalyst organisations will work with the Scottish Government and the NCSC to develop and implement practical solutions to key challenges on an ongoing basis, with an initial focus on:

- **strengthening leadership for, and helping drive greater awareness and uptake of good cyber resilient behaviours in, Scottish small and medium sized third sector organisations, including through the use of supply chain measures;**
- **strengthening coordination and knowledge sharing in respect of cyber resilience across key third sector organisations operating in Scotland; and**
- **supporting and promoting uptake of key educational initiatives in Scotland, including cyber security apprenticeships.**

42. Discussions with key Scottish third sector organisations have made clear that they fully understand the leadership role they can play in respect of cyber resilience in their sector. If we are to succeed in our shared goal of raising standards of cyber resilience across the whole of the Scottish third sector, it will be vital that influential Scottish third sector organisations commit to wielding their influence to encourage others to adopt good cyber resilience practice.

43. To help achieve this, from summer 2018 the Scottish Government will begin work in partnership with the NCSC, UK Government and a cross-sectoral group of **third sector cyber catalyst organisations** to develop and support implementation of practical solutions to key cyber resilience challenges in the Scottish third sector on an ongoing basis.

The Scottish Government will play a leading role in supporting and driving forward the work of the group, and identifying avenues for delivery.

Membership of this working group will be refreshed on a regular basis, in line with the key areas of focus that are identified through the ongoing work of the group. An up-to-date list of third sector cyber catalyst organisations will be placed on the Scottish Government Cyber Resilience website[14]. These organisations will commit at board level to working with the Scottish Government and the NCSC to undertake the following broad initial programme of work:

[14] https://beta.gov.scot/policies/cyber-resilience/

(i) Strengthening leadership for, and helping drive greater awareness and uptake of good cyber resilient behaviours in, Scottish small and medium sized third sector organisations, including by making use of supply chain levers.

Where appropriate, third sector cyber catalyst organisations will be asked and supported to:

- Support **public messaging** around the importance that should be attached to cyber resilience by all parts of the Scottish third sector, including by helping to develop and support a more consistent, joined-up programme of **awareness raising activities** aimed at small and medium sized third sector organisations and their customer and client community in Scotland (see Key Action 2); and
- Support work (set out in more detail at Key Action 4) to **enhance cross-sectoral understanding and alignment of supply chain policies**. A key aim of this work will be to examine whether more consistent "core" cyber resilience requirements can be identified in respect of the small and medium sized third sector organisations and the SME community that form part of influential organisations' supply chains, thus improving the ability of small and medium sized third sector organisations to anticipate the likely cyber resilience demands that will be placed on them if they wish to win contracts.

(ii) Strengthening coordination and knowledge sharing in respect of cyber resilience across key organisations operating in Scotland.

Where appropriate, third sector cyber catalyst organisations will be asked and supported to share best practice knowledge gained from their own organisational activity on cyber resilience **across sectors**, with a view to driving **greater cross-sectoral alignment and best practice**. This will include sharing learning with:

- one another, including in respect of any challenges or difficulties they have encountered, or any innovative solutions they have identified to overcome barriers and ensure an effective understanding of the cyber threat and implementation of effective cyber resilience measures;
- other Scottish third, public and private sector organisations – including, where appropriate, small and medium sized third sector organisations and SMEs – in order to help drive best practice in respect of cyber resilience, and develop a more coherent, aligned cross-sectoral approach across Scotland; and
- the UK NCSC and the UK Government Cabinet Office, to help inform the future development of standards and guidelines and other relevant requirements. Over time, the expectation is that these standards and guidelines will mature and improve to take account of experience in implementing them and technological developments.

Catalysts may be asked to facilitate wider engagement between government and key organisations in their sub-sector in appropriate circumstances.

(iii) Supporting and promoting uptake of key educational initiatives in Scotland, including cyber security apprenticeships.

Where appropriate, third sector cyber catalyst organisations will be asked and supported to:

- **make use of key educational initiatives in Scotland**, including cyber security apprenticeships, with a view to ensuring they have the right skills available to them to build organisational cyber resilience, and to support talent development in this area;
- **promote awareness** of these initiatives as part of wider work on public messaging; and
- **help inform the development of future initiatives**, to ensure they meet the needs of the Scottish third sector.

Further details of relevant initiatives and proposals in this area can be found in the **Learning and Skills action plan**.

44. A Scottish public sector cyber catalyst group has already been instituted, and it is intended that a similar scheme be established for Scotland's private sector. The Scottish Government will work to support the sharing of knowledge and learning across all three sectoral cyber catalyst schemes, and to help drive greater alignment across all sectors.

D: Supply chain cyber security – leveraging requirements to improve the cyber resilience of Scotland's third sector

Key Action 4

The Scottish Government will work with third sector organisations and key partners to clarify the common core cyber resilience requirements that are currently placed on third party suppliers, and their relationship to wider standards and guidance, by spring 2019.

Thereafter, the potential for greater cross-sectoral alignment and cooperation in respect of common core supply chain requirements will be explored, with the goal of promoting greater coherence across Scotland's public, private and third sectors.

A key aim of this alignment will be to improve the cyber resilience of Scotland's small and medium sized third sector organisations as part of the supply chain of larger public, private and third sector organisations.

45. Supply chain cyber security is a vital part of organisational cyber resilience. Cyber criminals often attack the organisation with the weakest cyber security within the supply chain, and use the vulnerabilities present in their systems to gain access to other members of the supply chain, including large corporates.

46. Many large corporates in Scotland already require their supply chains – including third sector suppliers – to have appropriate cyber resilience measures in place, and make those requirements public. While the requirements they place on their supply chains are often similar, there is currently no agreed common practice or "core question set" either within or across sub-sectors (with the notable exception of the defence sector, where the Defence Cyber Protection Partnership have worked with industry to develop a Cyber Security Model for procurement[15]. This model is supported by an online tool called Octavian, which includes a short questionnaire to determine the Cyber Risk Profile for a contract or sub-contract).

Work is currently under way in the banking sector to explore the potential for greater alignment and cooperation between key organisations in respect of third party supply chain cyber security and assurance.

47. The NIS legislation and associated guidance will formalise requirements in respect of supply chain cyber security for private and public sector organisations who are subject to it – this may help ensure greater consistency in the approach taken across operators of essential services to the cyber security of third sector suppliers.

48. The Public Sector Action Plan commits the Scottish Government to working with key partners to develop a proportionate, risk-based policy in respect of supply chain cyber security, to be applied by public bodies in all relevant procurement processes. The views of Scottish third sector organisations will be sought on a draft policy early in 2018, with a view to implementation as part of the Scottish Public Sector Cyber Resilience Framework. This policy is expected to result in specific, proportionate, risk-based requirements being placed on private and third sector suppliers to the Scottish public sector in respect of cyber resilience.

The Scottish Government will make explicit how the public sector supply chain cyber security policy aligns with NIS requirements.

49. To help: (a) ensure the supply chain cyber security of any third sector organisations that form part of the critical infrastructure of Scotland, and (b) improve the cyber resilience of Scotland's small and medium sized third sector organisations, the Scottish Government will work with the NCSC and key third sector partners, including third sector cyber catalyst organisations, on the following programme of activity:

- Seeking views from the third sector to help **inform the development of the draft public sector supply chain cyber security policy** in 2018, so that it takes account of existing good practice in the third sector.
- Identifying the current **common core supply chain cyber resilience requirements** that are placed on small and medium sized third sector suppliers, with a view to **improving sectoral guidance** for the small and medium sized third sector organisations on what they need to do to strengthen their cyber resilience to position themselves to win contracts. This work should include a focus on progressive management of cyber threats and risks. Initial mapping of some key sector requirements should be undertaken by spring 2019.

[15] See: https://www.gov.uk/government/publications/defence-cyber-protection-partnership-cyber-risk-profiles

- Building on this analysis, considering the potential for **greater cross-sectoral alignment of core supply chain cyber resilience requirements** over time. Such alignment should have a particular focus on small and medium sized third (and private) sector suppliers, and be informed by regulatory requirements and existing practice in the public, private and third sectors. It may include a focus on alignment with NCSC-endorsed guidance or schemes (including Cyber Essentials, the 10 Steps to Cyber Security, NCSC Supply Chain Guidance) and other widely recognised standards (e.g. ISO and IASME), and help inform the development of the proposed Third Sector Cyber Resilience Framework/Pathway (see Key Action 1).
- Building on any such alignment work, exploring the potential for cross-sectoral **pooling or accessing of information** to support supply chain security across Scotland's third sector. This may include ways of accessing consistent information on which small and medium sized third sector supply chain organisations have been assessed as capable of managing different levels of cyber risk in line with a Third Sector Cyber Resilience Framework/Pathway. This work will aim to reduce the burdens placed on both purchasers and suppliers in managing cyber risk in the supply chain.

50. While there will inevitably be a requirement for individual large third (and private) sector organisations to include "bespoke" conditions around cyber security for specific contracts, identifying common core requirements should help provide a common starting point for consideration of the requirements that key third and private sector organisations (including the cyber catalyst organisations) will generally expect to see in place in their supply chains to manage the cyber risk in specific circumstances.

51. It is expected that this work will result in greater consistency in the incentives and requirements placed on Scotland's small and medium sized third sector organisations that form part of the public, private and third sector supply chain (or that wish to do so). That greater consistency of messaging, centred around a widely disseminated Third Sector Cyber Resilience Framework/Pathway, should help drive greater awareness in small and medium sized third sector organisations of what good practice in respect of cyber risk/threat management looks like. **Annex C** gives a visual representation of what this might look like.

52. Third sector organisations that make use of Cyber Essentials in their supply chain, either now or as a result of the alignment work described above, will also be encouraged to promote the use of a voucher scheme to support small and medium sized third sector organisations in their supply chains to achieve accreditation to Cyber Essentials or Cyber Essentials Plus level (see Key Action 5).

53. Of course, not all small and medium sized third sector organisations in Scotland form part of the supply chain of the public sector and larger private and third sector organisations. Wider awareness raising work will be required to ensure greater uptake of good cyber resilient behaviour. This is covered in Key Action 2.

E: Strengthening incentives to improve Cyber Resilience in Scotland's third sector

Key Action 5

The Scottish Government and the National Cyber Resilience Leaders Board will work with the UK Government and key third sector stakeholders to consider how best to strengthen incentives to support the uptake of cyber security standards/ accreditation, and the adoption of good cyber resilience practice more generally.

This will include the continuation of a modified voucher scheme to support the achievement of Cyber Essentials or Cyber Essentials Plus certification by Scottish small and medium sized third sector organisations. We aim to at least double the number of public, private and third sector organisations holding Cyber Essentials or Cyber Essentials Plus certification in total in Scotland during Financial Year 18-19.

54. Third sector partners have put forward arguments that **incentives** will be key to promoting the adoption of cyber security standards/accreditation and the adoption of good cyber resilience practice more generally.

55. The Scottish Government is particularly keen to support small and medium sized third sector organisations, who will often be starting from a relatively low base of knowledge or experience, to begin their journey towards greater cyber resilience. One way of doing so is to support uptake of Cyber Essentials/Plus certification. The Cyber Essentials scheme offers a mechanism, endorsed by the National Cyber Security Centre, for organisations to demonstrate to customers, investors, insurers and others that they have in place critical technical controls that protect against the most common internet-borne cyber attacks.

56. The Scottish Council of Voluntary Organisations (SCVO) supported a small pilot grants programme in October 2017. The programme provided funding of between £500 to £1500 for small and medium sized charities to achieve Cyber Essentials accreditation. An SCVO evaluation report to identify the barriers and enablers to achievement of Cyber Essentials certification in the third sector will be produced by May 2018. This will help to inform options for future initiatives to support achievement of Cyber Essentials or Cyber Essentials Plus certification by Scottish third sector organisations.

57. The Digital Scotland Business Excellence Partnership supported a voucher scheme that ran from summer 2016 until end 2017 to help Scottish SMEs achieve Cyber Essentials or Cyber Essentials Plus certification. The scheme provided funding to SMEs to allow them to secure the services of an industry expert to advise them on how to approach securing Cyber Essentials certification. The voucher was of the value of up to £1.5k per company. An evaluation of this scheme found that it had a positive effect on take-up and achievement of Cyber Essentials amongst SMEs.

58. The Scottish Government will build on the lessons of these two schemes by funding a modified voucher scheme to support Scottish small and medium sized third sector organisations (and private sector organisations) to achieve Cyber Essentials or Cyber Essentials Plus. This scheme is expected to be operational from autumn 2018. We aim to at least double the number of public, private and third sector organisations holding Cyber Essentials or Cyber Essentials Plus certification in total in Scotland during Financial Year 18-19.

59. Third sector organisations will be encouraged to publicise this scheme to their supply chain companies and customers/clients, in order to drive greater take up of Cyber Essentials and Cyber Essentials Plus. The scheme will also be publicised through key partners (including Third Sector Cyber Catalyst organisations) as part of the awareness raising activities set out under Key Action 2.

60. Beyond this, the Scottish Government, the NCRLB, the UK Government and key partners will work together to explore what additional incentives are already in place or could be developed further to promote good practice in the Scottish third sector in respect of cyber resilience. High level proposals on additional incentive schemes will be considered by the NCRLB by spring 2019, with decisions on subsequent action taken thereafter.

F: Benchmarking, Monitoring and Evaluation

Key Action 6

Key action 6: The Scottish Government will work with the NCRLB and key partners to develop appropriate benchmarking, monitoring and evaluation arrangements, for implementation by spring 2019.

61. In order to understand what progress is being made towards the vision of Scotland as a world leading nation in cyber resilience, it will be important to have in place arrangements to achieve a regularly refreshed picture of the extent of good cyber resilience practice in Scotland's third sector. The benefits of this are expected to include:

- The provision of greater assurance to **members of the public** with regard to the cyber resilience of Scotland's third sector as a whole and the cyber resilience of specific sub-sectors.
- The provision of useful **benchmarking information** for third sector organisations, to assist them in making judgements around what level of standards/accreditation they should be aiming to achieve in light of sectoral benchmarks.
- The provision of greater assurance to **Government, Parliament** and **Regulatory Bodies** with regard to levels of cyber resilience across key areas of Scotland's third sector.

62. To help achieve this, the Scottish Government will work with the NCRLB, the NCSC, Regulatory Bodies, key third sector partners and organisations providing accreditation, to develop appropriate benchmarking, monitoring and evaluation arrangements by spring 2019. Key measures that form part of these arrangements may include:

- Working with the NCSC to monitor and report on the number of third sector organisations achieving Cyber Essentials and Cyber Essentials Plus;
- Working with accreditation bodies and external audit companies to understand levels of take-up of private certification schemes in Scotland, where possible;
- Working with key partners to monitor and report on the uptake of free, reputable cyber security tools amongst Scotland's third sector (e.g. the Global Cyber Alliance's DMARC and Protected DNS services);
- Working with the NCSC to monitor and report on membership of the SciNet grouping on the CiSP; and
- Inclusion of appropriate questions focused on cyber resilience in Scottish-based surveys (e.g. the Scottish Crime and Justice Survey).

ANNEXES

A

Annex A. Key Actions and Timelines – Summary

Key action no.	Action required of:	Requirements	Deadline	Page no. action plan
1	SG, NCRLB, Third Sector partners	■ Consider options for developing a Third Sector Cyber Resilience Framework/Pathway, with a particular focus on small and medium sized third sector organisations. To include:	Spring 2019	P.19-21
	SG, NCRLB, Third Sector partners	– Work to develop a stronger understanding of core cyber resilience requirements currently encompassed by NCSC schemes and guidance, other common standards and key supply chain policies as they apply to the Scottish third sector (particularly small and medium sized third sector organisations), and how these relate to progressive levels of cyber risk.	Spring 2019	
2	SG, NCRLB, NCSC and key Third sector partners	■ Key communications messaging and awareness raising activities for the third sector. Undertake work to strengthen systems of advice and support – initial target landscape identified and achieved.	Ongoing & spring 2019	P.22-23
3	SG and NCRLB	■ Begin work with NCSC and key third sector partners in a Third Sector Cyber Catalyst Working Group, with initial focus on:	Summer 2018	P.24-26
	SG, NCRLB and Third sector cyber catalysts	– strengthening leadership for, and helping drive greater awareness and uptake of good cyber resilient behaviours in, small and medium sized third sector organisations, including through the use of supply chain measures.	Ongoing	
		– strengthening coordination and knowledge sharing in respect of cyber resilience across key third sector organisations in Scotland; and	Ongoing	
		supporting and promoting uptake of key educational initiatives in Scotland, including cyber security apprenticeships;	Ongoing	

Key action no.	Action required of:	Requirements	Deadline	Page no. action plan
4	SG, NCRLB and Third sector cyber catalysts	■ Seek views from the third sector to help inform the development of the draft public sector supply chain cyber security policy in 2018, so that it takes account of existing good practice in the third sector. ■ Identify current common core supply chain cyber resilience requirements that are placed on small and medium sized third sector suppliers, with a view to improving sectoral guidance for small and medium sized third sector organisations on what they need to do to strengthen their cyber resilience to position themselves to win contracts. ■ Building on this analysis, consider the potential for greater cross-sectoral alignment of core supply chain cyber resilience requirements over time. ■ Building on any such alignment work, explore the potential for cross-sectoral pooling or accessing of information to support supply chain security across Scotland's third sector organisations.	First half of 2018 Spring 2019 From spring 2019 From spring 2019	P.26-28
5	SG/SCVO/SE SG, NCRLB and key Third sector partners	■ Continuation of modified voucher scheme for Cyber Essentials ■ Explore greater use of incentives and put forward for consideration by NCRLB	Autumn 2018 By spring 2019	P.29-30
6	SG	■ Work with NCRLB, NCSC, Regulatory bodies and key partners to develop benchmarking, monitoring and evaluation arrangements.	By spring 2019	P.30-31

Annex B – Scottish Third Sector Cyber Resilience Framework/Pathway – Concept

1. This annex sets out a broad concept for the development of a Scottish Third Sector Cyber Resilience Framework or "Pathway".

2. The concept has been developed by the Scottish Government and members of the National Cyber Resilience Leaders Board, in consultation with the NCSC and key third sector partners.

In line with Key Action 1 in the action plan, work will be undertaken to finalise and pilot this Framework/Pathway (on the condition that further work confirms its feasibility) on the basis of initial analytical work to develop a stronger understanding of the **core cyber resilience requirements** that are currently encompassed by NCSC schemes and guidance, other common standards and key supply chain policies as they apply to the Scottish third sector (particularly small and medium sized third sector organisations), and how these relate to **progressive levels of cyber threat**.

Aims

3. The Framework/Pathway would aim to provide a **common point of departure** for Scottish third sector organisations to **assess the cyber threat** to their assets, and **identify the key measures** they should consider implementing to help manage these threats in view of the impact on their operations.

The Framework/Pathway could be used by small and medium sized third sector organisations to **benchmark** themselves against progressively more demanding or holistic approaches to cyber threat management. It would also provide a way for organisations in the early stages of their cyber resilience journey to identify key sources of guidance and assurance in order to **improve their capacity to manage progressively more targeted and sophisticated cyber threats**.

4. In view of the fact that many larger third sector organisations operating in Scotland will already be working to a range of UK and international regulatory requirements, it is expected that any such Framework/Pathway would most likely be of use for smaller organisations (especially small or medium sized third sector organisations). However, larger third sector organisations that are not currently subject to cyber security regulation may also find such a tool useful in identifying the levels of cyber resilience they should be aiming for based on the likely cyber threat to their assets.

5. Work would be undertaken to align any Framework/Pathway with similar frameworks under development as part of the **public and private sector action plans on cyber resilience** by the Scottish Government and the NCRLB.

Overview of key potential features

6. The starting point for any potential Framework/Pathway would be **an agreed common way of assessing the broad cyber threat to an organisation's networks and assets**, either in general or in the context of specific contracts or undertakings.

7. These cyber threat profiles should be organised in a **progressive hierarchy**, based on broadly defined increases in the expected targeting and sophistication of cyber threats. It should also take into account the likely organisational impact of breaches.

8. There should then be a clear **hierarchy of guidance, standards or controls** that is "mapped" directly to the relevant threat level, thus ensuring greater consistency of application of appropriate standards and controls.

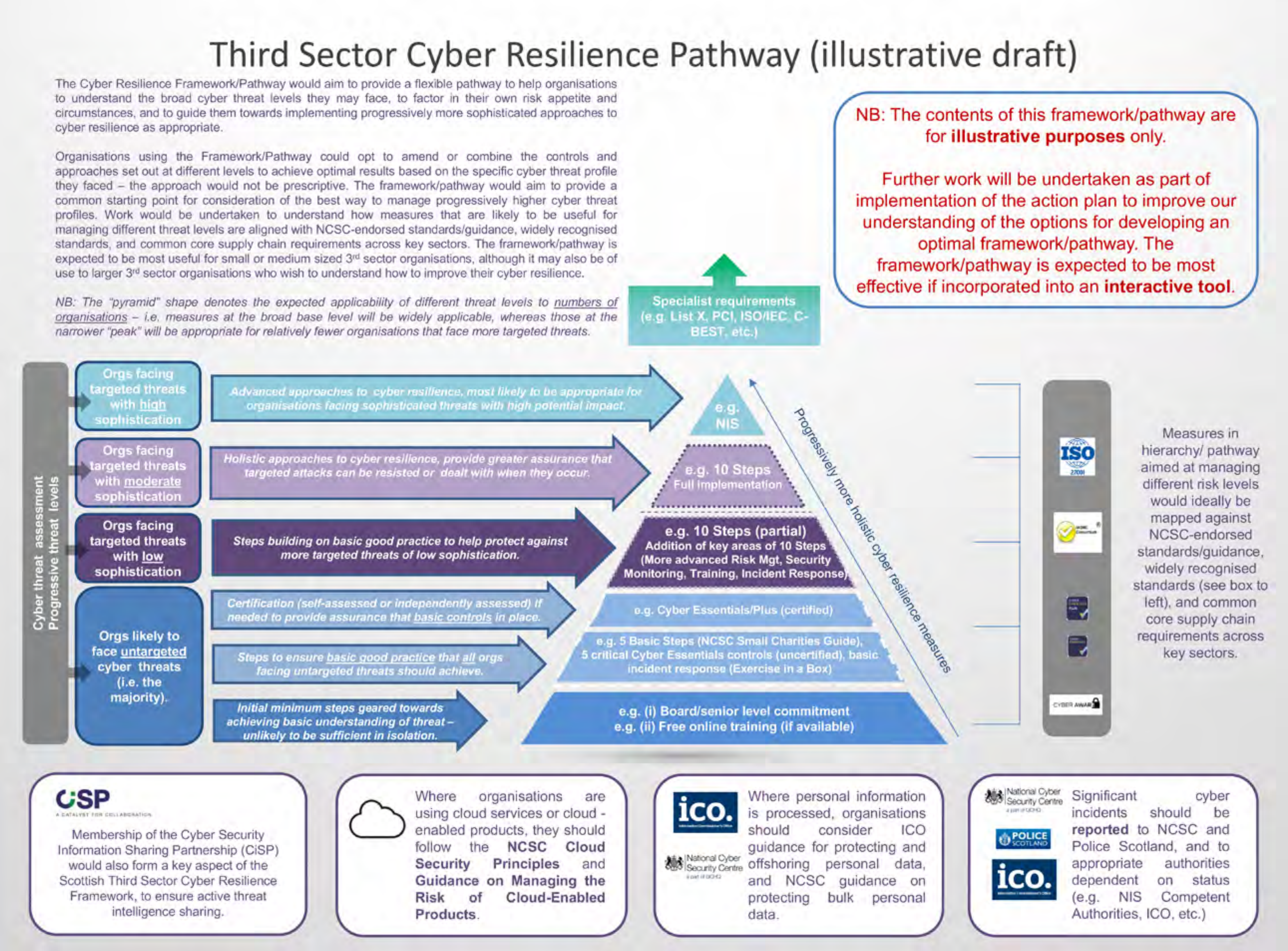
9. These cyber threat profiles and the hierarchy of standards or controls should, to the greatest extent possible, be aligned with or incorporate the following key existing or planned measures:

- **Existing standards, guidance or initiatives**, particularly those endorsed by the National Cyber Security Centre such as **Cyber Essentials**, the **10 Steps to Cyber Security**, **NIS Directive Technical Guidance**, **NCSC Supply Chain Guidance**, the **NCSC's cloud security principles**, the **NCSC's Cyber Security Information Sharing Partnership**, and **ICO guidance on protecting personal data**; and
- **Existing and planned practice in respect of supply chain cyber security** amongst larger public, private and third sector organisations.

10. The potential for development of a **freely accessible online tool** to support small or medium sized third sector organisations, in particular, to undertake a cyber threat assessment against the Framework/Pathway, and be directed to appropriate guidance or standards, would likely be key to the success of this work.

11. A basic visual representation of this proposed approach is set out on the following page. **It should be noted that the contents of this proposed Framework/Pathway will be subject to further work and discussion, and are included only for illustrative purposes at this stage.**

Annex B – Scottish Third Sector Cyber Resilience Framework/Pathway – Basic Concept (indicative draft only)



Third Sector Cyber Resilience Pathway (illustrative draft)

The Cyber Resilience Framework/Pathway would aim to provide a flexible pathway to help organisations to understand the broad cyber threat levels they may face, to factor in their own risk appetite and circumstances, and to guide them towards implementing progressively more sophisticated approaches to cyber resilience as appropriate.

Organisations using the Framework/Pathway could opt to amend or combine the controls and approaches set out at different levels to achieve optimal results based on the specific cyber threat profile they faced – the approach would not be prescriptive. The framework/pathway would aim to provide a common starting point for consideration of the best way to manage progressively higher cyber threat profiles. Work would be undertaken to understand how measures that are likely to be useful for managing different threat levels are aligned with NCSC-endorsed standards/guidance, widely recognised standards, and common core supply chain requirements across key sectors. The framework/pathway is expected to be most useful for small or medium sized 3rd sector organisations, although it may also be of use to larger 3rd sector organisations who wish to understand how to improve their cyber resilience.

NB: The "pyramid" shape denotes the expected applicability of different threat levels to numbers of organisations – i.e. measures at the broad base level will be widely applicable, whereas those at the narrower "peak" will be appropriate for relatively fewer organisations that face more targeted threats.

NB: The contents of this framework/pathway are for **illustrative purposes** only.

Further work will be undertaken as part of implementation of the action plan to improve our understanding of the options for developing an optimal framework/pathway. The framework/pathway is expected to be most effective if incorporated into an **interactive tool**.

Specialist requirements (e.g. List X, PCI, ISO/IEC, C-BEST, etc.)

Cyber threat assessment
Progressive threat levels

Orgs facing targeted threats with high sophistication

Advanced approaches to cyber resilience, most likely to be appropriate for organisations facing sophisticated threats with high potential impact.

e.g. NIS

Orgs facing targeted threats with moderate sophistication

Holistic approaches to cyber resilience, provide greater assurance that targeted attacks can be resisted or dealt with when they occur.

e.g. 10 Steps
Full implementation

Orgs facing targeted threats with low sophistication

Steps building on basic good practice to help protect against more targeted threats of low sophistication.

e.g. 10 Steps (partial)
Addition of key areas of 10 Steps
(More advanced Risk Mgt, Security Monitoring, Training, Incident Response)

Orgs likely to face untargeted cyber threats (i.e. the majority).

Certification (self-assessed or independently assessed) if needed to provide assurance that basic controls in place.

e.g. Cyber Essentials/Plus (certified)

Steps to ensure basic good practice that all orgs facing untargeted threats should achieve.

e.g. 5 Basic Steps (NCSC Small Charities Guide), 5 critical Cyber Essentials controls (uncertified), basic incident response (Exercise in a Box)

Initial minimum steps geared towards achieving basic understanding of threat – unlikely to be sufficient in isolation.

e.g. (i) Board/senior level commitment
e.g. (ii) Free online training (if available)

Progressively more holistic cyber resilience measures

Measures in hierarchy/ pathway aimed at managing different risk levels would ideally be mapped against NCSC-endorsed standards/guidance, widely recognised standards (see box to left), and common core supply chain requirements across key sectors.

CiSP
A CATALYST FOR COLLABORATION

Membership of the Cyber Security Information Sharing Partnership (CiSP) would also form a key aspect of the Scottish Third Sector Cyber Resilience Framework, to ensure active threat intelligence sharing.

Where organisations are using cloud services or cloud - enabled products, they should follow the **NCSC Cloud Security Principles** and **Guidance on Managing the Risk of Cloud-Enabled Products**.

ico.
National Cyber Security Centre

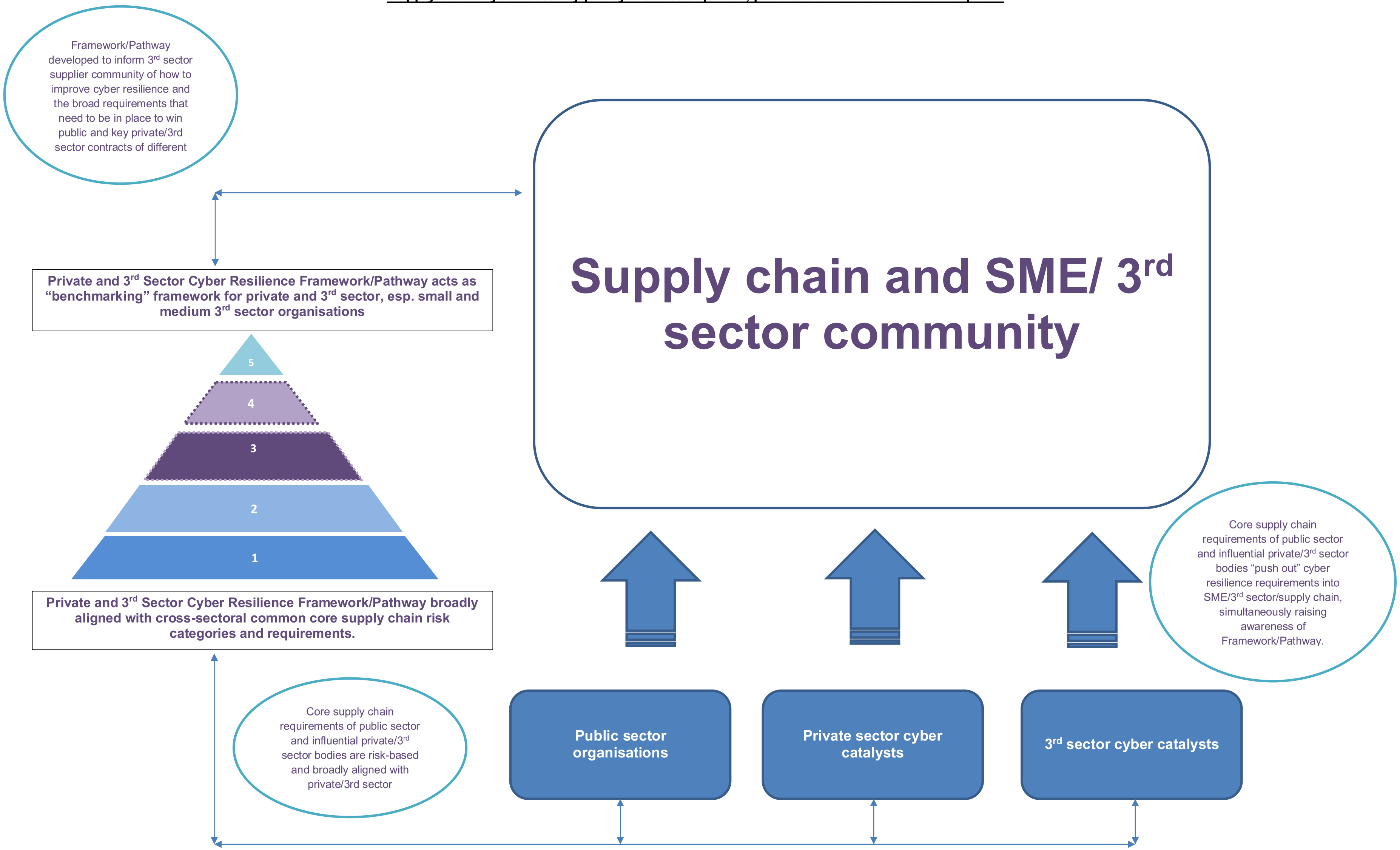
Where personal information is processed, organisations should consider ICO guidance for protecting and offshoring personal data, and NCSC guidance on protecting bulk personal data.

National Cyber Security Centre
POLICE SCOTLAND
ico.

Significant cyber incidents should be **reported** to NCSC and Police Scotland, and to appropriate authorities dependent on status (e.g. NIS Competent Authorities, ICO, etc.)

Annex C – Supply chain cyber security policies – driving good practice through Scotland's small and medium sized third sector organisations (concept)

Supply chain cyber security policy – effect of public, private and third sector action plans



Framework/Pathway developed to inform 3rd sector supplier community of how to improve cyber resilience and the broad requirements that need to be in place to win public and key private/3rd sector contracts of different

Private and 3rd Sector Cyber Resilience Framework/Pathway acts as "benchmarking" framework for private and 3rd sector, esp. small and medium 3rd sector organisations

Private and 3rd Sector Cyber Resilience Framework/Pathway broadly aligned with cross-sectoral common core supply chain risk categories and requirements.

Core supply chain requirements of public sector and influential private/3rd sector bodies are risk-based and broadly aligned with private/3rd sector

Supply chain and SME/ 3rd sector community

Public sector organisations

Private sector cyber catalysts

3rd sector cyber catalysts

Core supply chain requirements of public sector and influential private/3rd sector bodies "push out" cyber resilience requirements into SME/3rd sector/supply chain, simultaneously raising awareness of Framework/Pathway.

ANNEX D – NCRLB Third Sector Steering Group Membership

- Scottish Council of Voluntary Organisations (SCVO)
- Scottish Government Cyber Resilience Unit
- Health and Social Care Alliance Scotland (the ALLIANCE)
- Cornerstone
- The Wise Group
- Association of Chief Officers of Scottish Voluntary Organisations (ACOSVO)
- Information Commissioners Office (ICO)
- Learning Link Scotland
- Coalition of Care and Support Providers in Scotland (CCPS)
- National Cyber Security Centre (NCSC)
- Institute of Fundraising
- Office of the Scottish Charity Regulator (OSCR)
- Scottish Federation of Housing Associations (SFHA)
- Scottish Care

Scottish Government
Riaghaltas na h-Alba
gov.scot

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at
The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-78781-038-9

Published by The Scottish Government, June 2018

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS421426 (06/18)