www.gov.scot/cyberresilience

Scottish Government
Riaghaltas na h-Alba
gov.scot

# Cyber Resilience Toolkit

## Your go-to guide for all things cyber resilience


# Introduction:

## Getting the best out of the Cyber Resource Toolkit

This toolkit provides you with easy access to the growing number of helpful resources that can support individuals within the public, private and third sectors to address and improve organisational cyber resilience.

It signposts you to the most authorative guidance and support materials currently available. It should also be of value to those within your organisation who have little or no cyber security specialist knowledge, but who have roles in influencing change including leading, informing, training and educating or communicating to internal and external audiences.

This resource should be particularly useful to those who have an influencing role in external communications or managing customer relationships, where it could help to encourage a conversation around security, resilience and support to your customers.

The toolkit sections can be found on the left side bar, and they follow a logical progression path:

- Building Resilience
- Skills Development
- Communications
- Reporting, Response and Recovery
- Public Sector

# Overview:

## The Strategic Context

**The importance of cyber resilience in Scotland has never been greater. Digital technologies bring enormous opportunities but they also bring with them new threats and vulnerabilities that we must take action to manage.**

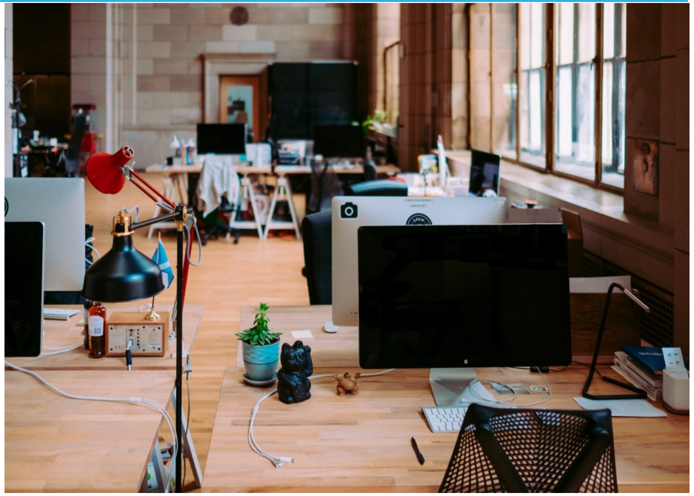
"Safe, Secure and Prosperous: A Cyber Resilience Strategy for Scotland" was published in 2015. It sets an ambition for Scotland to become a world leading nation in cyber resilience. The strategy is supported by a suite of action plans that have been developed and implemented to achieve our ambitions.

To support the strategy's aims, five action plans are in place:


- Economic Opportunity Action Plan: setting out actions to support Scotland's business, enterprise and academic communities to mature into a thriving, coherent cyber security cluster.
- Learning and Skills Action Plan: setting out actions to support the development of cyber resilient behaviours amongst our population, and to build a skilled and growing cyber security profession for Scotland.
- Public Sector Action Plan: setting out actions to ensure that Scotland's public bodies have in place a common baseline of good cyber resilience practice.
- Private Sector Action Plan: setting out a programme of work in partnership with Scotland's private sector to help raise fundamental levels of cyber resilience.
- Third Sector Action Plan: setting out a detailed programme of work in partnership with Scotland's Third sector to help raise fundamental levels of cyber resilience.

# Building resilience

## Understanding the risk to you and your organisation



We live in one of the most open digital societies in the world. This brings lots of opportunities, but it also makes us vulnerable to the ever-evolving cyber attacks that seek to defraud, extort, exploit, steal information, damage or disrupt businesses and organisations of all sizes and across all sectors.

Any organisation connected to the internet **is** vulnerable to cyber attacks. This can be either targeted or non-targeted attacks. It's a fact of digital life. Cyber attacks are simply one of the risks of doing business and communicating in a digital age. This risk should be managed in line with other organisational risks.

Getting the cyber basics right is relatively simple and can eliminate as much as 80% of the risk from non-targeted internet-borne threats. Doing business involves taking some informed risks but are you confident you are adequately informed about the cyber risk to your business?

**Why you should address the cyber risks to your organisation**

- Protecting your organisation from cyber attacks puts you in a stronger position to thrive. It can increase customer confidence and help secure and retain business and contracts.
- You may be putting your organisation at significant risk by underestimating the disruptive impact a cyber attack can have on your business, or the lasting damage to its reputation.
- Increasingly, organisations in the public and private sectors are asking suppliers to demonstrate their cyber security credentials.
- Protecting personal data is a legal requirement. Getting the cyber basics right will help you with this.
- Your customers and clients expect you to be managing the cyber risk and doing what is reasonably expected of every business.

**This toolkit will provide you with the tools and guidance you need to improve your organisation's cyber resilience, reducing the likelihood that you will become a victim to cyber crime, or helping you to better handle a cyber attack—with as minimum negative impact as possible.**

# Getting The Basics Right

## First steps— What is it we want to protect?

Our digital devices are essential to our personal and working lives bringing speed, agility and efficiency to transform the way we do business, socialise and provide key services. This connectivity brings great opportunities, but it is not without risks. We need to take reasonable steps to reduce this risk.

Having an understanding of **what** we care about, and **why** it's important, should help to prioritise where to protect our organisation most—is it our identity, our privacy, our access to systems, our organisation, or indeed all of these things?

When we know what we need to protect, we need to understand **how** they might be at risk. Do your devices access the Internet? Are they standalone devices or are they connected with other devices (e.g. on a shared platform)? Does your data sit on the Cloud or on your organisation's network?

Once you know the answer to these questions, you can take some simple steps to better protect yourself and your organisation. The National Cyber Security Centre provides sound advice on the steps you can take to reduce your exposure to cyber risks;

Information for  the Self Employed and Sole Traders

Information for SME's and Charities

Information for Large Organisations

Information for the Public Sector

# Getting the basics right

## Where can I get further advice?

Here are some authoritative sources where you can get useful advice and guidance.

The National Cyber Security Service: the UK's authority on cyber threat, risk, prevention, awareness, reporting, response and recovery.

Cyber Aware : Cyber Aware is the UK Government's campaign to help individuals and smaller organisations protect themselves online.

Get Safe on Line: a free resource providing practical advice to individuals and businesses on how to protect themselves while online and using digital technologies.

My Gov: The Scottish Government's site with advice on how to keep your business safe online.

Gov.scot Scottish Government's policy on Cyber resilience.

Take Five to Stop Fraud: a UK awareness campaign led by FFA UK (part of UK Finance), and delivered with and through a range of partners in the UK payments industry, financial services firms, law enforcement agencies, telecommunication providers, commercial, public and third sector.

Police Scotland: responsible for the recording and investigation of crimes in Scotland. If you suspect you are the victim of cyber crime check out their website or call Police Scotland on **101.**

# Leadership

## Cyber Resilience is every leader's responsibility

Cyber risk for the Board is as important as financial risk and health and safety. The responsibility for data security can no longer be solely managed by the IT department. Leaders must actively review and approve data security policies. **Leaders don't need to be technical experts**, but they need to know enough about the threats and risks and be able to have a conversation with their experts about these, and understand the right questions to ask.

Protecting information assets is of critical importance to the sustainability and competitiveness of businesses. All organisations, regardless of size or sector, need to be on the front-foot in terms of their cyber preparedness. Cyber resilience is all too often thought of as an IT issue, rather than the strategic risk management issue it is.

Good cyber security is all about managing risks. The process for governing cyber security in your organisation will be similar to the process you use for other organisational risks.

It is a continuous, iterative process and comprises three overlapping components, summarised below:

1. Understand the risks you and your organisation face.

2. Use this information to understand and prioritise your risks.

3. Take steps to manage those risks.

**NCSC's Board Toolkit will provide you with the tools you need to have the necessary conversations with your IT team/supplier.**

If you're not sure where to start, NCSC suggests you start with the Introduction to Cyber Security for Board members and Embedding cyber security into your structure and objectives.

# Certification

## Demonstrating that your business takes security seriously

Crime is an unfortunate reality in society and we should not be surprised that it has evolved to exploit the digital environment in which we now operate. Demonstrating that you take digital security seriously is good for client/customer confidence and could be a differentiator between you and a competitor.

Getting the cyber basics right is therefore essential if operating your business online.

A good start is with the NCSC Small Business: Cyber Security and Small Charity Guide Each contains five quick and easy steps that could save time, money and even your business' reputation. This is a good first step but is not something that you can easily use to demonstrate to others that you take cyber security seriously.

Most cyber crime is not targeted. It simply takes advantage of the connectivity to cast a global net in the hope of hooking in a victim. Within this large untargeted market it is estimated that around 80% off attacks can be prevented by getting 5 critical controls in place.

Cyber Essentials is a simple but effective, Government-backed and industry-supported scheme that helps businesses protect themselves against the growing threat of cyber attacks. It provides a clear statement of the 5 basic controls organisations should have in place to protect them.

For organisations looking to develop beyond the basics of cyber resilience, there are a number of additional support routes, including:

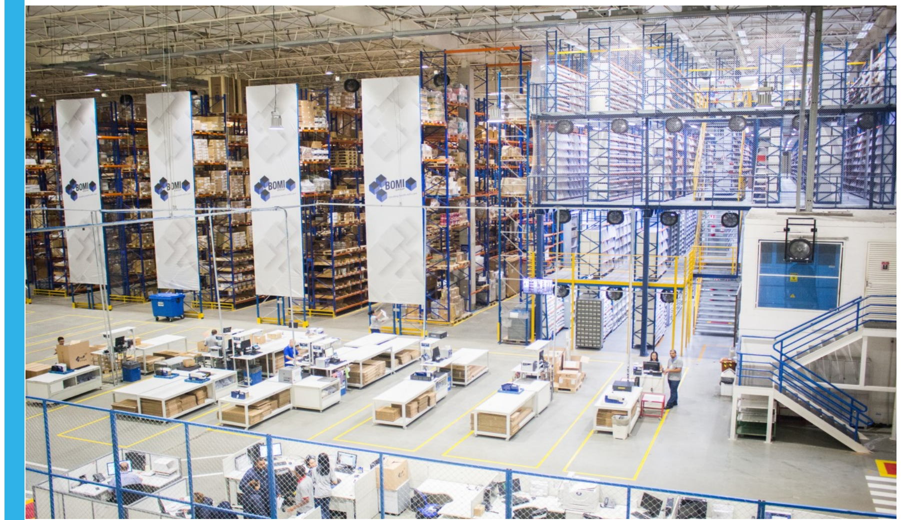
- NCSC Ten Steps to Cyber Security
- IASMI
- NCSC Cyber Assessment Framework
- ISO 27001 Information Security Management

# Supply Chain

## Improving the cyber resilience of your supply chain

**Most organisations rely upon suppliers to deliver products, systems, and services.**

Supply chains can be large and complex, involving many suppliers doing many different things. Effectively securing the supply chain can be difficult as vulnerabilities can be inherent, or can be introduced and exploited at any point in the supply chain. A vulnerable supply chain can cause severe damage and disruption. The **reputational and financial costs** of dealing with cyber attacks can be significant.



The NCSC has designed a set of [12 Principles] around supply chain security to help you gain and maintain the necessary level of control over your supply chain.

Implementing these recommendations will take time, but the investment will be worthwhile. It will improve your overall resilience, reduce the number of business disruptions you suffer and the damage they cause.

It will also help you demonstrate compliance with GDPR, the new Data Protection Act. Ultimately, these measures may help you win new contracts because of the trust you have gained in helping to secure your supply chain.

Introduction

Overview

Building Resilience

⇒ Getting the basics right

⇒ Leadership

⇒ Certification

⇒ Supply chain

⇒ Staff training

Skills Development

Communication

Response & Recovery, Reporting

Public Sector

# Supply Chain

## Securing the Public Sector supply chain

**Supply Chains for the Public Sector**

The cyber resilience of suppliers is increasingly important to the Scottish public sector. The number of cyber attacks targeting suppliers to the public sector has grown in recent years. Attacks can (intentionally or otherwise) disrupt and damage both suppliers' services and wider public services.

The Scottish public sector wants to ensure its suppliers have appropriate cyber security in place. That's because:

- It has a duty to prevent our public services from being disrupted by cyber attacks on suppliers; and
- It wants to support our suppliers to improve their cyber security, because it's good for the sustainability and resilience of our digital economy and society.

**Guidance and decision-making support tools**

To help improve supply chain cyber security, the Scottish public sector is being encouraged to adopt a more consistent approach to managing cyber risk in the supply chain. This will involve implementing:

- A guidance note, which has been produced for all Scottish public sector organisations, setting out best practice from the National Cyber Security Centre (the UK technical authority on cyber security).

- The Cyber Security Procurement Support Tool (CSPST) is a decision making support tool which all suppliers bidding for public sector contracts will be asked to use. Guidance on how to use the CSPST tool are available for public sector buyers **and** suppliers**.**

CSPST allows public sector buyers to risk-assess their contracts whilst developing their procurement strategy based on the sensitivity and handling of information and/or the access supplier may be granted to public sector systems and networks.

CSPST produces a risk profile and associated question set which potential suppliers can be invited to address as part of their tender. Suppliers can log onto CSPST and answer the questions and, in an effort to reduce burdens, will be able to reuse previous answers where applicable. Suppliers can also test their current cyber security and resilience through answering the questions and receiving a detailed report outlining any potential deficiencies with advice on how to further improve their cyber security.

# Staff Training

## Trained staff are vital to your organisation's cyber resilience

**People are often the first and strongest point of contact when it comes to security. It's important that you offer appropriate cyber resilience training and awareness raising arrangements for your workforce.**

There is so much cyber security advice available these days, many people find it hard to know where to start. This section aims to provide support businesses, charities and individuals with signposting and access to simple, free and trusted training resources and guidance to protect and keep themselves safe online at work and in their personal lives.

Some organisations struggle to explain **why** cyber security is something that all staff should care about. Even larger organisations (with dedicated training resources) find it difficult to explain the technical aspects of cyber security in ways that are **relevant** to their staff, so that they can help keep their organisations (and themselves) safe from cyber attack. Equally, many SMEs and charities, particularly very small organisations, may not have the resources to put any cyber security policies and training in place at all, leaving staff, their frontline defence, more vulnerable to cyber attacks.

To help with this, NCSC Staff Cyber Training explains why cyber security is important and how attacks happen. This e-learning training package is free and takes less than 30 minutes to complete.

The four key areas covered:

- defending yourself against phishing
- using strong passwords
- securing your devices
- reporting incidents

The training is primarily aimed at SMEs, charities and the voluntary sector, but can be applied to any organisation, regardless of size or sector. It's been deliberately designed for a non-technical audience (who may have little or no knowledge of cyber security), with tips that complement any existing policies and procedures.

You can download Stay Safe Online Infographic here.

The NCSC has set out the following actions which should be carried out by staff responsible for implementing staff training and awareness.

# Staff Training

## Trained staff are vital to your organisation's cyber resilience

The Scottish Government Cyber Resilience Unit have produced an interactive staff Training Guide which complements the NCSC's training package, 'Stay Safe Online: Top Tips for Staff'. This training guide is aimed at those who lead on training in an organisation and helps them teach non-technical staff the cyber fundamentals, providing access to practical exercises to support training.

The guide includes:

- Cyber topics to teach your staff
- Resources and links to training available
- Awareness raising materials from trusted partners

**Learning programmes currently available through formal learning routes, online learning and commercial suppliers can be found at:**

- The Open University—Introduction to Cyber Security—Stay Safe Online
- Cybrary – Cyber Security Training
- Cyber Security for Small and Medium Enterprises: Identifying Threats and Preventing Attacks
- For further courses check out Future Learn and The Open University

**The Cyber Security Body Of Knowledge (CyBOK)**

A comprehensive Body of Knowledge to inform and underpin education and professional training for the cyber security sector.

The **CyBOK** project aims to bring cyber security into line with the more established sciences by distilling knowledge from major internationally-recognised experts to form a Cyber Security Body of Knowledge that will provide much-needed foundations for this emerging topic.

# Staff Training

## Trained staff are vital to your organisation's cyber resilience

Whether you are new to cyber security or you are an experienced security professional there are training and collaborative working opportunities available.

**Certified Training**

GCHQ Certificated Training

The GCHQ Certified Training (GCT) scheme provides a benchmark for cyber security training by assuring the quality of both content and its delivery. Whether you are new to cyber security or you are an experienced security professional looking to enhance your skills, GCT can help you or your organisation find the right training.

The GCT scheme certifies two levels of cyber security skills training:

**Awareness** level — giving newcomers a thorough foundation in cyber security

**Application** level — in-depth courses for professional development

GCT is designed to assure high quality cyber security training courses delivered by experienced training providers. You can access a range of cyber security training offered either in-house for your organisation, online or in the classroom. As a general guide, when selecting training materials, resources or courses check that it is currently approved by **GCHQ**. You can find certified courses listed on the APMG website.

Certified Professionals

The Certified Professional (CPP) scheme is a recognition of competence which is awarded to those who demonstrate their sustained ability to apply their skills, knowledge and expertise in real-world situations.

Industry 100

The NCSC is inviting organisations of all sizes to work with them to achieve a great understanding of the cyber security environment. Industry 100 brings together public and private sector talent to challenge thinking, test innovative ideas and enable greater understanding on cyber security.

Research Institutes

The NCSC, jointly with the Engineering and Physical Sciences Research Council (EPSRC) supports four UK academic Research Institutes to develop cyber security capability in strategically important areas.

# Skills Development

## Growing cyber security expertise

A Learning and Skills Action Plan was launched in March 2018. Its focus is to ensure Scotland's citizens are cyber aware and that we have a strong pipeline of cyber security talent ready to fill roles in our businesses and organisations, and to help Scotland become a global competitor in cyber security goods and services.

Cyber security skills are in increasing demand, with a skills gap that we need to address. We are doing this by embedding cyber security strategically as a key strand of digital skills development. Our skills agency, Skills Development Scotland (SDS), is leading important activity, including:

- promoting cyber security as a career, and providing guidance on how to get into cyber security
- refreshing the National Occupational Standards (NOS) for Information Security
- creating a baseline of evidence of what works in developing skills, and promoting and consolidating cyber security within apprenticeship programmes.

### Understand cyber security careers

The cyber security industry continues to grow rapidly with many new and exciting jobs emerging all the time.

SDS has produced an interactive career framework that sets out 15 key cyber security roles, providing information about what these roles involve, qualifications required and general salary levels for each.


Alongside the career framework is information about Scotland's coherent "ladder" of cyber security qualifications that are available in schools, colleges and universities. All the qualifications are linked to the Scottish Credit and Qualifications Framework (SCQF) and many of the computing science courses at both undergraduate and postgraduate level may also include cyber security modules.

The Digital World website includes an interactive map with a range of learning opportunities near you.

Find out more about NCSC-certified Bachelor's, Integrated Master's and Master's degrees in cyber security and closely related fields.

# Skills Development

## Get involved in education and skills development

**Apprenticeships in Cyber Security**

Graduate Apprenticeships in Cyber Security are available at SCQF level 10 BEng (Hons) and SCQF level 11 BEng (Masters). Find out more information and how to apply for a vacancy.

Whether you're looking to improve your long-term talent pipeline or address skills gaps, the Scottish apprenticeship programme offers flexible options to suit your business needs. Employers can use apprenticeships to attract new talent or upskill existing staff.

**Get involved in education and skills development**

Cyber security professionals can add significant value to education and to the development of skills in a number of ways, for example by:

- providing careers talks in schools, colleges, universities and youth clubs
- mentoring students or offering work placements/internships—https://www.apprenticeships.scot/for-employers/
- co-delivering sessions on specific technical topics, for example as part of a qualification being delivered in a school or a college
- recruiting and mentoring apprentices
- providing tailored support for individuals with particular barriers, such as for autistic people, people returning to the workforce or changing careers
- providing input at events or courses, for example the Cyber Christmas Lectures or CyberFirst residential courses
- writing challenges for use in national competitions, for example the CyberFirst Girls Competition
- becoming a partner of the CyberFirst programme

If you would like to find out more about any opportunities to contribute to education and skills, please email: cyberresilience@gov.scot

# Communication

## The importance of communication

There is a wealth of well-intended advice and guidance available on cybercrime and cyber fraud, so much so that it can be very confusing. It is therefore important that cyber safe messages are communicated in the right way for different audiences and from an authoritative source. By communicating the cyber basics effectively, we can support the development of a culture of cyber resilience and, at the same time, create the necessary conditions to ensure Scotland achieves its ambition of becoming a world-leading cyber resilient nation.

### Communication Toolkit

The Communication Toolkit will support you in developing an effective communication strategy whether to your workforce or out to stakeholders. You will find out how to communicate effectively, provide cyber resilience messages and resources, and signpost existing campaigns and key contacts for further advice and guidance.

The Scottish Government is clear it cannot achieve a strong, cyber-resilient Scotland on its own. We absolutely need the help of those who are better placed to talk to target audiences about cyber resilience. By consistently communicating the simple, protective behaviours outlined, we will help bridge the gap between awareness, action and, importantly, encourage the reporting of crime.

**Blog feeds to follow:**

https://blogs.gov.scot/cyber-resilience/

https://www.ncsc.gov.uk/section/keep-up-to-date/all-blogs

**Who to follow on Twitter:**

Scottish Government Cyber Resilience Unit @CyberResScot

National Cyber Security Centre @NCSC

Police Scotland @policescotland

Get Safe Online @GetSafeOnline

Cyber Aware @cyberawaregov

Take Five @TakeFive

# Communication

## Signposting NCSC Resources

As an influencer, you should consider appropriate **signposting of NCSC guidance on an ongoing basis**, as part of wider communications and engagement activities.

**Some key NCSC resources that organisations should consider sharing with their stakeholders are:**

- Small Business **and** Small Charity Guides and associated materials (for smaller organisations)
- Small Business Guide: Response & Recovery Guidance that helps small to medium sized organisations prepare their response to and plan their recovery from a cyber incident.
- Board toolkit Resource to encourage cyber security discussions between the Board and their technical experts.
- Cyber Essentials standard—(for all organisations) - helps you to guard against the most common cyber threats.
- NCSC Exercise in a Box, to help organisations exercise their responses plans and identify weaknesses.
- Cybersecurity Information Sharing Partnership (CiSP) (to support organisations to share threat intelligence)
- Top Tips For Staff (for all organisations) e-learning training for staff
- NCSC and CPNI Supply Chain Guidance (relevant to all organisations that wish to manage supply chain risk)
- 10 Steps to Cyber Security (for large or small organisations dealing with more advanced cyber risks, and delivering medium risk contracts for public sector organisations)
- NIS Technical Guidance (for large or small organisations that form part of the critical infrastructure of Scotland/the UK. including those designated Operators of Essential Services under the NIS Directive)
- Reporting Cybercrime to Police Scotland

# Response & Recovery, Reporting

## Dealing with a cyber incident

The NCSC defines a cyber incident as unauthorised access (or attempted access) to an organisation's IT system/s. These may be malicious attacks such as denial of service attacks, malware infection, ransomware or more commonly phishing attacks.

**Have a plan to prevent, detect, respond and recover**

It is good practice to have a Cyber Incident Response Plan in place that sets out the steps your organisation should take to prevent, detect, respond and recover from cyber attacks. Your plan does not have to be complex but it should be clear on the roles and responsibilities of key individuals who can take action. This should not sit in isolation and should be woven into the wider resilience, business continuity and disaster recovery planning.

**Reporting a cyber incident internally**

If you suspect that you have been the victim of a cyber attack, it is essential that you act quickly to minimise the risk and impact. Your actions will be critical to damage limitation. It is important that you know who within your organisation should be notified and how to notify them if you suspect you have been duped by a suspicious email, perhaps clicking on a suspicious link or visiting a suspicious website, or if your device is operating strangely. Exploiting email and browsing remains the most common method of launching cyber attacks and gaining access to organisational networks.

These attacks are designed to both exploit and dupe you into 'letting them in'. Anyone can fall for phishing attacks—it's why they are the primary first choice of cyber criminals. It is essential that you don't delay in reporting suspicious incidents. **Do not just switch off the device and/ or walk away** in the hope that it will all go away. Action is needed as quick as possible.

**Reporting a cyber incident externally**

Depending on the nature of attack you may require to report certain incidents externally whether that be to a regulator, to the Information Commissioner, the police or indeed your customer base if it is their data affected. You should know who within your organisation has this responsibility, as there should be an organisational plan in place to deal with a cyber attack. Cyber attacks are also crimes and as such consideration should be given to reporting the attacks to Police Scotland (dial 101). In addition, the National Cyber Security Centre (NCSC) can offer advice and guidance on handling incidents.

# Cyber response

## Creating a cyber response plan

All organisations understand the disruptive impact that loss of service can have on the business. Business Continuity plans are well understood to plan for the disruptive impact of extreme weather events, fire or technology failure.

National Cyber Security Centre
a part of GCHQ

Cyber attacks are an additional business risk for organisations and they should be planned for like any other risk to the business. Unlike a technical fault, a cyber attack can have immediate impact and far reaching consequences which may risk the integrity of the organisation. Naturally, you will want to identify and resolve the problem as quickly as possible so you can resume to a 'business as usual' state.

For these reasons, it is essential that organisations have a clearly defined plan to prevent, detect, respond and recover from cyber attacks, particularly the most common attacks.

The NCSC has created the **Small Business Guide to Response and Recovery**. It provides small to medium sized organisations with guidance on how to prepare their response, and plan their recovery to a cyber incident. It's a companion piece to the **Small Business: Cyber Security** and **Small Charity Guide**.

If you're a larger business, or face greater impact from a cyber incident, then the Incident Management section of the NCSC 10 Step Guide can further help your cyber response. Board members should refer to our guidance on **planning your response to cyber incidents**.

**Testing your response arrangements**
It is important to test your organisation's incident response plan, in the same way you test out your health and safety or fire drills.

**How cyber resilient is your organisation?**
Exercise in a Box (EiaB) is an NCSC online tool which helps organisations find out how resilient they are to cyber-attacks and to help them practice their response. The service provides exercises, based around the main cyber threats which your organisation can undertake at times suitable for you. It includes everything you need for setting up, planning, delivery and review.

Introduction

Overview

Building Resilience

Skills Development

Communication

Response &

Recovery,

Reporting

⇒ Cyber incident

⇒ Cyber response

⇒ Situational awareness

⇒ CISP

Public Sector

# Situational Awareness

## Understanding current cyber threats

*Situational awareness* is the art of listening, observing, understanding and considering the dynamics of any *situation*. In cyber security terms this means having an understanding of your environment and predicting and responding to potential problems that might occur.

Cyber threats whether targeted or un-targeted are primarily external and seek to achieve some form of advantage and gain by overcoming the security you have placed around your network. A threat becomes a managed risk when the likelihood and impact is understood. Having a good understanding of the known threats to your business is key to managing risk.

The NCSC provides access to a number of useful resources to support you to increase your situational awareness, these include

- Reports and Advisories
- Weekly Threat Reports
- Blogs

# CISP

## Cyber Security Information Sharing Partnership (CISP)

The Cyber Security Information Sharing Partnership (CiSP) is a joint industry and government initiative set up to exchange cyber threat information in real time, in a secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.

**Why should you become a member of CiSP?**

- engagement with industry and government counterparts in a secure environment
- early warning of cyber threats
- ability to learn from experiences, mistakes, successes of other users and seek advice
- an improved ability to protect their company network
- access to free network monitoring reports tailored to your organisations' requirements.

**What products does CiSP produce?**

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

**To become a registered CiSP member you must be:**

- a UK registered company or other legal entity which is responsible for the administration of an electronic communications network in the UK
- sponsored by either a government department, existing CiSP member or a regional Cyber PROTECT police officer or industry champion

**If your organisation is new to the CiSP and you are looking for a sponsor please contact the Cyber Resilience Unit at the Scottish Government at cyberresilience@gov.scot**

If you want further details or have a specific query about CiSP then please email cisp@ncsc.gov.uk.

# Public Sector

## Action Plan 2017—2018

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

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

The public sector action plan was published in November 2017 and encourages a consistent and proportionate approach to cyber resilience for 200+ public sector organisations in Scotland.

The plan aims to ensure that Scotland's public bodies have in place a common baseline of good cyber resilience practice, and are working towards becoming exemplars of cyber resilience. This is vital to ensuring our digital public services are safe and secure.

**PSAP Key Actions**

The PSAP focuses on key areas of

- Governance (designated board member responsible for cyber, risk management processes in place)
- information sharing (NCSC CiSP membership and active sharing of intelligence)
- securing of critical technical controls, (Independent assurance of controls through CE+ or equivalent)
- active cyber defence measures, (Protected DNS, DMARC, Web check and Netcraft usage where eligible)
- staff training & awareness, (NCSC Top Tips for Staff) and
- incident response arrangements (Cyber Incident Response Plan, playbooks and exercising)

An Implementation Toolkit has been developed to help public bodies understand how to implement the PSAP.

**PSAP Monitoring**

Public sector bodies completed initial baseline surveys of their cyber resilience arrangements in 2018. These surveys highlighted key areas for improvement—cyber threat monitoring, staff training, incident response and exercising.

# Public Sector

## Cyber resilience framework

The **Scottish Public Sector Action** Plan on Cyber Resilience set out a commitment to develop a **Scottish Public Sector Cyber Resilience Framework**.

The key aim of this Framework is to:

- Provide a common, effective way for Scottish public sector organisations to assess their cyber resilience arrangements, identify areas of strength and weakness, gain reasonable confidence that they are adhering to minimum cyber resilience requirements, and take decisions on how/whether to achieve higher levels of cyber resilience on a risk-based and proportionate basis.

In doing so, the Framework seeks to:

- Align with key wider cyber-related requirements under the General Data Protection Regulation (GDPR), the Security of Network and Information Systems (NIS) Directive and other standards;

- As far as possible, minimise any additional burdens on Scottish public sector organisations, including by making clear how the Framework relates to existing standards or requirements, and taking account of these when providing guidance on compliance;

- Provide a clear basis for internal and external audit and inspection activity, promoting greater consistency in the areas and issues covered by audit and inspection bodies when assessing Scottish public sector organisations; and

- Help to provide clarity and assurance to individual organisations, Ministers, the Scottish Parliament and the public that appropriate levels of cyber resilience are in place across the Scottish public sector and its individual subsectors.

The framework can be found here

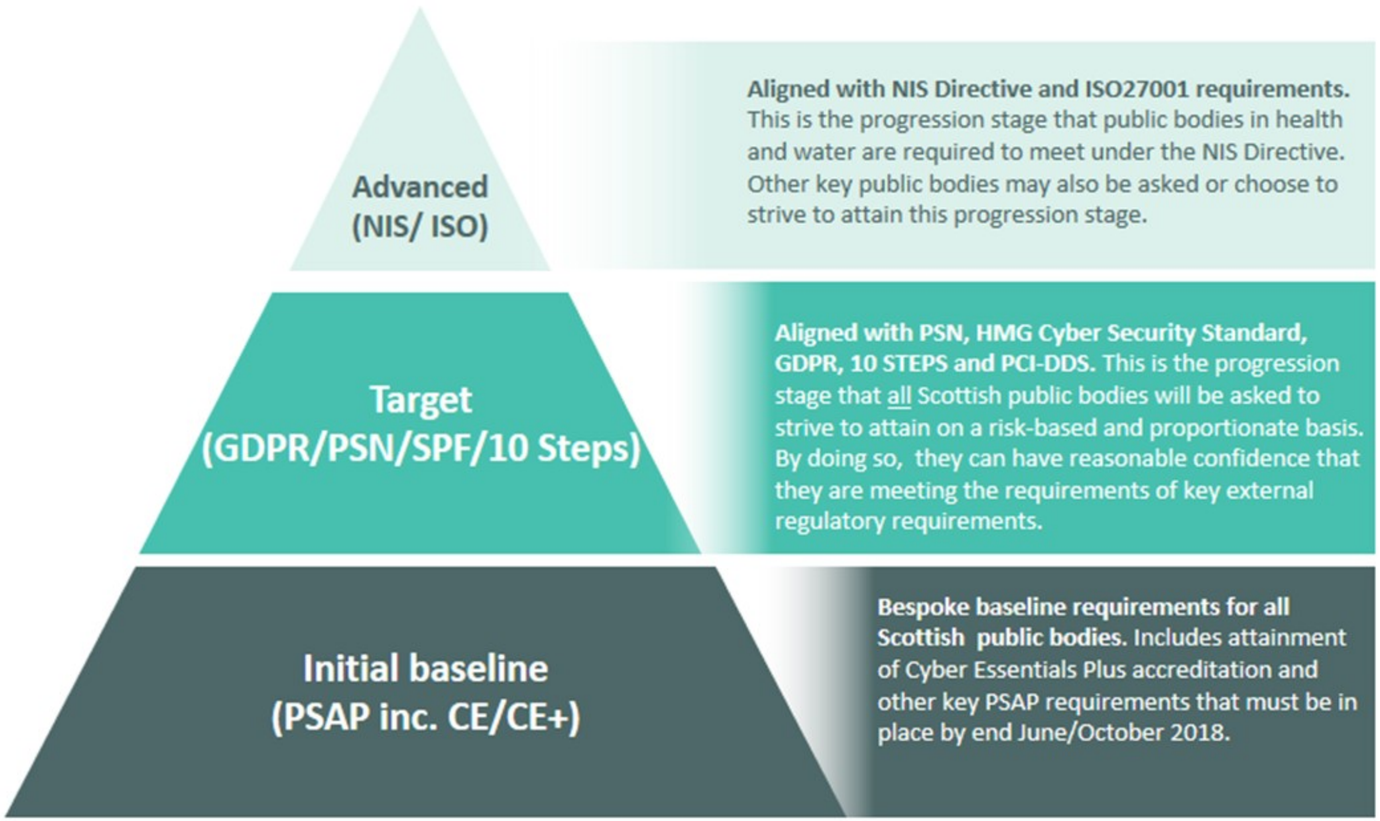
# Public Sector

## Cyber resilience framework

The framework outlines a natural hierarchy of the common cyber security standards, with PSAP/Cyber Essentials as the baseline and the Network and Information Systems Regulations at the advanced level.

The PSAP encouraged all public sector bodies to achieve the baseline by October 2018 and it is anticipated that the majority of public sector bodies will move to achieve the Target stage by the end of 2020.

Key Water and health sector organisations are already working towards the NIS regulations and the Scottish Government expects that a number of other bodies will align themselves with NIS as a sensible and pragmatic approach to managing their cyber risks and threats.



# Public Sector

## Supply chain

**Scottish Public Sector Supplier Cyber Security Guidance Note**
The Scottish Public Sector Action Plan on Cyber Resilience (PSAP) was published in November 2017 and set out a commitment to develop a proportionate, risk-based policy in respect of supply chain cyber security for Scottish public sector organisations. The Supplier Cyber Security Guidance Note has been developed to meet that commitment.

The key aims of the Supplier Cyber Security Guidance Note are:

- To support Scottish public sector organisations to put in place **consistent, proportionate, risk-based policies** that effectively reduce the risk of Scottish public services being damaged or disrupted by cyber threats as a result of supplier cyber security issues;

- To **minimise any necessary additional burdens** on Scottish public sector organisations (as purchasers) and private and third sector organisations (as suppliers), whilst ensuring the presence of proportionate cyber security controls in the public sector supply chain. This includes a requirement to avoid discouraging SMEs, in particular, from bidding for public sector contracts. This latter aim will be supported by ensuring greater uniformity of the requirements placed on suppliers (thus minimising the number of conflicting demands they face), and by providing a decision-making support tool to aid consistent, proportionate implementation by public sector organisations; and

- To ensure **alignment** where possible with key requirements in respect of supply chain cyber security that have implications for the Scottish public sector and its supply chains. These include the EU Security of Network and Information Systems (NIS) Directive as transposed into UK-wide legislation and guidance.

**Cyber Security Procurement Support Tool**
To support public sector organisations in implementing the Supply Chain Guidance Note, the Cyber Security Procurement Support Tool (CSPST) has been developed. CSPST has been integrated into the Procurement and Supplier journeys to assist the public sector in seeking consistent assurances from potential suppliers during procurement activities.

CSPST allows public sector buyers to risk assess their contract whilst developing their procurement strategy base on the sensitivity and handling of information and/or the access supplier may be granted to public sector systems and networks. CSPST produces a risk profile and associated question set which potential suppliers can be invited to address as part of their tender. Suppliers can log in to CSPST and answer the questions and , in an effort to reduce burdens, will be able to reuse previous answers where applicable.  Suppliers can also test their current cyber security and resilience through answering the questions and received a detailed report outlining any potential deficiencies and advice to improve their

# Public Sector

## Incident response

The public sector initial baseline surveys during 2018 highlighted that Cyber Incident was a key area for improvement across much of the public sector.

To address this, a significant research study was carried out in the first half of 2019 to review the cyber incident response arrangements of the Public Sector Cyber Catalysts, identify good practise and develop a generic incident response plan template and playbooks for key cyber threats.

**The Cyber Capability Toolkit** has been created to support Public Sector organisations to better manage their cyber incident response.

The Toolkit contains;

- A Model Incident Response Plan template
- A set of Playbooks covering Denial of Service, Malware, Data loss, Phishing and Ransomware attacks
- A Cyber Incident Assessment tool designed to provide high level insight into the organisations maturity across a range of related incident management controls

The Cyber Capability Toolkit will be subject to constant review and are to be regarded as live documents, building on good practise, lessons from exercises and incidents and feedback of public sector bodies.