Scottish Public Sector Supplier Cyber Security Guidance Note

Version 1.2 (December 2023)

This Scottish Public Sector Supplier Cyber Security Guidance Note has been produced by the Scottish Government Cyber Resilience Unit.

Public sector organisations with feedback or questions about the layout or implementation of this guidance note should contact cyberresilience@gov.scot for advice.

Scottish Government
Riaghaltas na h-Alba

Contents

Introduction

1. The Scottish Public Sector Action Plan on Cyber Resilience commits to developing a proportionate, risk-based policy about supply chain cyber security for Scottish public sector organisations "PSOs".

2. This guidance note forms part of the Scottish Public Sector Cyber Resilience Framework (the Framework). The Framework is embedded in several audit and compliance requirements that apply to different parts of the Scottish public sector.

3. The security of supply chains is increasingly important as we often see cyber incidents and attacks affect public sector bodies indirectly through their suppliers. It is vital that PSOs adopt an approach to supplier cyber security that best meets their risk profile/appetite. This guidance note promotes the adoption of a **consistent approach** across the Scottish public sector. For the purposes of this guidance note, Scottish Public Sector Organisations (PSOs) includes NDPBs, Non-Ministerial Departments, local authorities, health boards and universities and colleges.

4. The guidance is relevant to PSOs that rely on any suppliers to deliver goods or services as part of a supply chain. This could be through commercial OR non-commercial arrangements. PSOs should consider all circumstances where a cyber risk to their own security may be present through interactions with other organisations.

5. This guidance note incorporates advice from key partners in the Scottish public, private and third sectors, including public sector centres of procurement expertise. The Scottish Government works closely with the National Cyber Security Centre (NCSC), the UK-wide technical authority on cyber security, to ensure its work on cyber resilience is informed by appropriate technical expertise. As a result, the guidance aligns closely with NCSC supply chain guidance. Where appropriate, it also references guidance from the National Protective Security Authority (NPSA), the UK-wide authority which provides protective security advice to businesses and organisations across the UK national infrastructure.

6. Cyber security arrangements for systems processing personal data form a key aspect of compliance with the **General Data Protection Regulations (GDPR)**, which took effect on 25th May 2018. However, the data protection obligations placed on organisations and their supply chains by GDPR go wider than technical measures to protect personal data. Public sector organisations are asked to consider carefully how this guidance note can/should be embedded in wider measures to support compliance with GDPR.

7. **Cyber security can also be important in contexts not involving personal data**, such as arrangements involving sensitive official information, industrial control systems or the "Internet of Things" (where computing devices are embedded in everyday physical objects, which are then enabled to communicate, be controlled, etc. via the Internet).

The Importance Of Supplier Cyber Security

8. Most PSOs rely on suppliers or other partners to deliver products, systems, and services. Often these relationships form part of public sector organisations' supply chains. Supply chains can be large and complex, involving many suppliers doing many different things.

9. Securing suppliers and the supply chain against cyber-attacks can be difficult because vulnerabilities can be inherent in suppliers' systems, or introduced and exploited at any point in the supply chain. The NCSC notes that a vulnerable supply chain can cause significant damage and disruption to organisations.

10. PSOs must understand the cyber threat to their supply chain to take appropriate action to mitigate it. A series of high profile, damaging attacks on PSOs have demonstrated that attackers can, and will, exploit vulnerabilities in supply chain security.

The Key Aims Of This Guidance

11. The key aims of this Supplier Cyber Security Guidance Note are:

- To support PSOs to implement **consistent, proportionate, risk-based policies** that reduce the risk of damage or disruption to public services due to supplier cyber security issues;

- To **minimise any necessary additional burdens** on PSOs (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 from bidding for public sector contracts, by encouraging greater uniformity of the requirements placed on suppliers.

- To align requirements 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.

Scottish Public Sector Supplier Cyber Security – Guidance Note

1. This section describes the broad policy approach that Scottish public sector organisations are encouraged to take to supplier cyber security.

Summary

2. Scottish PSOs are encouraged to consider **4 Key Points** when managing cyber risks in their supply chains:

i. **Key Point 1:** PSOs should follow the NCSC endorsed "12 principles of supply chain security".

ii. **Key Point 2:** In particular, public bodies should align their approach to **NCSC Principle 5** ("Set and communicate minimum security requirements for suppliers"). The "**Use Cases**" provided by the NCSC demonstrate how the principles can be applied in practical supply chain scenarios;

iii. **Key Point 3: PSOs** should embed an **appropriate and proportionate information/cyber security assurance process** within their procurement processes. This process will help public bodies assess levels of cyber risk when procuring and may take the form of a questionnaire or some other method to support local decision making. It may help to determine whether any personal data processing is involved as part of a contract or framework agreement, and the resulting technical protections that might be needed.

iv. **Key Point 4:** Cyber assurance processes may indicate that **accreditations and certification** such as Cyber Essentials, IASME, and/or ISO27001 **are needed to** provide additional independent assurance. This need should be judged on a case-by-case-basis, and supported by an information/cyber assurance process. PSOs should understand the **scope** and expiry date of any certification.

Annex A describes types of accreditations to help public bodies with this assessment.

An example Supplier Cyber Assurance Questionnaire is available to support decision-making and local information assurance processes used by public bodies. This may promote greater consistency of the application of this guidance across the Scottish public sector.

3. This guidance note advocates a **proportionate approach** to cyber security. It enables organisations to manage cyber risks while mitigating any unintended impacts, particularly on SME suppliers.

Applicability And Timelines

4. PSOs should apply this guidance note to new contracts and other relevant arrangements with suppliers and update their processes accordingly.

5. PSOs may wish to apply this guidance to existing contracts or supplier arrangements where appropriate. This could be done by undertaking a contract review process (where possible and appropriate to do so, based on relevant financial, legal and risk management advice). PSOs may wish to prioritise work based on **risk** and **criticality of services**, adopting a selective and/or phased approach to implementation. PSOs should assess the appropriate scope and timeframe for such review processes, based on their own circumstances and assessment of risk.

Key Point 1 – Adoption Of NCSC Supply Chain Principles

6. PSOs should incorporate the key elements of NCSC's 12 Principles of Supply Chain Security into their procurement processes and policies. This guidance note does not reproduce the principles in full and **Scottish public sector organisations should refer to the most up to date version of the NCSC Guidance.**

7. Some key practical points that public bodies may find helpful when implementing the principles are set out below. Please note that these practical points are intended to complement and promote practical implementation of the NCSC principles, not replace them.

Practical considerations for Scottish public sector organisations

1: Understand what needs to be protected and why

Think about the level of protection you need suppliers to give to your assets. You should consider the sensitivity and value of your information and assets that your suppliers will have access to. You should be clear about the products or services your suppliers will deliver to you as part of the contract.

Scottish PSOs should already have in place minimum cyber risk governance arrangements, and these should help to identify key assets/services that must be protected from cyber threats that may be introduced through supply chains.

Public sector organisations should consider how the supply chain cyber risk to these assets is reflected in corporate risk registers.

Adoption of proportionate information/cyber assurance processes can support application of this principle, particularly in the context of ensuring that suppliers understand what needs to be protected in specific circumstances and why.

2: Know who your suppliers are and build understanding of what their security looks like

You should know who your suppliers and sub-contractors are, as well as the maturity and effectiveness of their current security arrangements. You should consider the security protections you have asked your immediate suppliers to provide, and what they have asked any sub-contractors to do.

PSOs should:

- build clear central records to help understand who is supplying what goods or services to their organisations. It may be prudent to prioritise understanding which suppliers have access to personal data or sensitive information for which the organisation is responsible

- develop appropriate information/cyber assurance processes to understand suppliers' security arrangements in the context of specific contracts

- consider cyber assurance processes for suppliers and subcontractors where supplier arrangements involve access to personal data or sensitive information to ensure that minimum cyber security requirements are in place throughout the supply chain.

3: Understand the security risk posed by your supply chain

You should assess the risks these arrangements pose to your information or assets, to the products or services to be delivered, and to the wider supply chain. Use this assessment to decide the appropriate risk profile, and the protections you will expect suppliers across your supply chain to provide.

The NCSC guidance provides helpful links to relevant resources aimed at supporting consideration of risk, to strengthen governance arrangements.

4: Communicate your view of security needs to your suppliers

You should ensure that your suppliers understand their responsibility to provide appropriate protection for your contract information and contracted products and services.

You may wish to take steps to ensure your suppliers adhere to their security responsibilities and include any associated security requirements in any sub-contracts they let.

5: Set and communicate minimum security requirement for your providers

Individual PSOs are responsible for ensuring minimum security requirements are in place.

You should make sure your requirements reflect your assessment of security risks, but also take account of the maturity of your suppliers' security arrangements and their ability to deliver the requirements you intend to set. Consider setting different protection requirements for different types of contracts, based on the associated risk profile.

PSOs should set minimum requirements through a cyber assurance process embedded within the wider procurement process. A good practice example questionnaire is also available to assist in the process of seeking assurances.

This principle is key to the effective application of the guidance note. The NCSC use cases provide examples of minimum security requirements that may be appropriate in different scenarios. This guidance note encourages public sector organisations to align their approach to minimum security requirements with the NCSC use cases where practical. A good practice example questionnaire is also available to assist in the process.

6: Build security consideration into your contracting processes and require that your suppliers do the same.

Require prospective suppliers to provide evidence of their approach to security and their ability to meet the minimum security requirements you have set at different stages of the contract competition. Develop appropriate supporting guidance, tools and processes to enable the effective management of the supply chain.

PSOs should consider cyber risk and minimum cyber security requirements as part of their procurement processes and seek proportionate information/cyber security assurances from potential suppliers.

Cyber assurance has been embedded within the Procurement Journey, the Supplier Journey and the model contractual terms and conditions made available by the Scottish Government to the wider public sector.

7: Meet your own security responsibilities as a supplier and consumer

You should provide upward reporting and pass security requirements down to sub-contractors. Tell customers about any issues you are encountering and work proactively with them to make improvements. Challenge your customers if guidance covering their security needs is not forthcoming, and seek assurance that they are they happy with the measures you are taking.

PSOs may wish to view this principle in the context of:

- their achievement of relevant certification, such as Cyber Essentials or Cyber Essentials Plus – demonstrating to stakeholders the importance they place on having basic technical controls in place; and

- their obligations when receiving data from other public sector organisations, taking care to demonstrate what controls are in place that can give the sharing organisation confidence that the data will be appropriately handled and protected.

8: Raise awareness of security within your own supply chain.

Explain security risks to your suppliers using language they can understand. Encourage them to ensure that key staff (e.g. procurement, security, marketing) are trained on, and understand these risks, as well as their responsibilities to help manage them. Share security information and education across your supply chain.

Your information/cyber assurance assessment process should help support communication of minimum security requirements in the context of specific contracts.

PSOs should encourage suppliers that manage their own networks to join the Cybersecurity Information Sharing Partnership (CiSP) to help raise their awareness of cyber threats.

9: Provide contractual expectations and available support for security incidents.

You should be prepared to provide support and assistance if necessary, where security incidents have the potential to affect your business or the wider supply chain. Contractual requirements should clarify supplier's responsibilities for advising you and the Information Commissioner's Office about such incidents.

Suppliers should have clear contractual obligations placed upon them to monitor and respond to cyber security incidents. The model terms and conditions made available by the Scottish Government for use by the wider public sector include requirements in this respect.

All Scottish public sector organisations should have and regularly test Cyber incident response plans, which should detail procedures when cyber incidents occur, including due to supplier arrangements.

10: Build assurance activities into your supply chain management.

These activities could include penetration testing, the right to audit, performance measurement, upward reporting, and good security behaviours. Advise or require your suppliers to do the same for any contracts that they have let that relate to your contract and your organisation.

Model terms and conditions (available here) include requirements around upward reporting and management of cyber incidents and the "right to audit".

Principle 5 of the NCSC supply chain guidance also covers recommended approaches to the use of certification that may require an element of independent testing and assurance (e.g. Cyber Essentials Plus).

11: Encourage the continuous improvement of security within your supply chain.

PSOs should encourage continuous improvement of security within their supply chain.

You may also wish to allow time for your suppliers to achieve security improvements which will help them meet security requirements in some cases. This avoids creating unnecessary barriers for suppliers and continuous improvement might enable suppliers to win future contracts within the sector.

12: Build trust with suppliers.

PSOs should build good relationships with suppliers, and to view cyber security as a shared concern throughout the supply chain.

Key Point 2 – Alignment Of Minimum Security Requirements (Principle 5) With NCSC Use Cases

1. **Principle 5** of the NCSC's Supply Chain Cyber Security Principles requires organisations to "Set and communicate minimum security requirements for suppliers". The NCSC provides a set of "Use Cases" that offer examples of appropriate minimum security requirements for different circumstances. PSOs should incorporate these requirements into organisational information/cyber assurance assessment processes.

2. PSOs should consider these "use cases" as their starting point for minimum security controls. They cover four scenarios:

   - Protecting information shared with suppliers (Use case A)
   - Specifying security requirements to a supplier who is delivering something to you (Use case B)
   - Connecting a supplier's systems (Use case C)
   - National security cases (Use case D)

Key Point 3 – Implementing The Principles: Information/Cyber Assurance Processes

3. PSOs should undertake an **information/cyber assurance assessment as part of the procurement process**. This will help them understand the levels of cyber risk present in specific contractual or other arrangements with suppliers. They can also identify the appropriate minimum cyber security requirements to address that risk.

4. Information/cyber assurance processes will generally involve a **questionnaire** or other local process to support decision making and determine whether there is likely to be a cyber risk to a specific contract, and how significant the level of risk is. The outcome of that initial assessment should inform the cyber security requirements that are placed on suppliers. This will allow suppliers to demonstrate they can appropriately mitigate risk.

5. The Procurement Journey and Supplier Journey, which facilitate best practice and consistency in procurement activity across the Scottish public sector, have been updated to reflect this guidance note and to prompt public sector buyers and suppliers to ensure consideration of cyber risks.

6. PSOs should **incorporate their own information/cyber assurance processes into existing procurement processes if they secure goods or services from suppliers**.

7. For example, **Scottish Government procurement processes** have been updated so that they promote **consultation with expert cyber colleagues** and include information/cyber risk assessments at the **strategy development stage** for individual procurements. This process aims to:

   i. help identify and understand what cyber risks may be present;
   ii. determine clear, proportionate and relevant minimum cyber security requirements for the proposed contract
   iii. allow for management of cyber risks in a proportionate way - this may include requiring suppliers to achieve compliance with minimum security requirements over a certain timeframe as a condition of contract award.

8. Where such cyber expertise is not available internally, and the cyber risks associated with a procurement appear significant, public bodies may wish to consider procuring external cyber security advice in appropriate circumstances (for example, via Lot 4 of the Dynamic Purchasing System);

Key Point 4 – Proportionate Use Of Certification And Accreditation

9. Some of the NCSC Use Cases propose the use of certification or accreditation as evidence of compliance with cyber security requirements. Certification can provide greater assurance around a supplier's cyber security, and can provide independent assurance of a supplier's information/cyber security maturity.

10. Scottish public sector organisations should:

    - judge the need for accreditation or certification as part of their **information/cyber security assurance process**. Judgements should be made on a **case-by-case-basis**, in view of the organisation's need for **independent assurance** that appropriate cyber security controls are in place.

    - Take steps to review and understand the **scope** and **expiry date** of relevant certification, and to ensure **ongoing good practice** in line with the certifications.

11. Certification/accreditation should be viewed as one way of achieving independent assurance that cyber security requirements are in place but should not be used in isolation.

12. The use of certification/accreditation can impose costs on both suppliers and purchasers and this means that **cost effectiveness and proportionality** must always be considered. However, certification/accreditation can also offer benefits to both suppliers and purchasers. For example, it can reduce the number of times suppliers and purchasers have to ask and answer detailed questions around compliance as they may be able to rely on their certification for multiple procurements. It may also provide reputational benefits.

13. Public sector bodies are encouraged to consider accepting assurances from a supplier that they will **work towards achieving any certification/accreditation by an agreed date**.

14. Public sector bodies should also be willing to accept equivalent evidence that demonstrates a level of cyber security that equates to or exceeds the requirements of certification/accreditation

15. **Annex A** provides further information on the likely benefits of certification and accreditation.

Other Important Issues

Requirement To Ensure Proportionality

16. Scottish public sector organisations are encouraged to take a **proportionate approach** to the application of security controls in line with this guidance note. Where a cyber risk has been identified, any decisions about minimum cyber security requirements should be risk-based and proportionate to your organisation's risk appetite. This is to avoid an overly prescriptive approach to cyber security.

    The Scottish Government supports and encourages the use of **Cyber Improvement Plans** for suppliers who do not, at the time of bidding, meet minimum cyber security requirements.

Responsibility For Cyber Risk Management

17. It is for individual Scottish public sector organisations (with appropriate independent oversight from audit and competent authorities where applicable) to ensure they are working to identify cyber security risks in their supplier arrangements (or requiring suppliers to do so) and to interpret and implement the guidance set out in this document and elsewhere accordingly.

18. This guidance note and associated tools/documents are not intended to replace formal assessment processes or expert advice where this may be required. It is ultimately the responsibility of the individual public sector organisation to satisfy themselves that cyber risk has been adequately assessed and mitigated, and that where appropriate they seek expert advice from IT/information/cyber security/data protection professional colleagues or external consultants.

19. This responsibility includes assessing how best to incorporate the 12 NCSC principles into existing third party/supply chain/procurement policies and processes in a proportionate, effective way.

Methods To Support Decision Making

20. The Scottish Government has produced a spreadsheet that can help PSOs determine their risk profile, and to ensure that appropriate cyber assurance procedures are in place throughout their supply chains. The Cyber Security Procurement Support Tool (CSPST) is no longer available. The new support document will be developed based on user feedback, and we encourage users to send any feedback to cyberresilience@gov.scot.

NCSC's Early Warning Service

21. The NCSC's "Early Warning" is a free service designed to inform your organisation of potential cyber attacks on your network, as soon as possible. The service enhances your organisation's security by increasing your awareness of the low-grade incidents which could become much bigger issues, so you can act on them earlier. Early Warning filters millions of events that the NCSC receives every day and,

using the IP and domain names you provide, informs you of any that are relevant to your organisation. You can find more information, including how to sign up, by visiting the NCSC's website.

Annex A – Certification And Accreditation

1. Key Point 4 of this guidance note encourages the appropriate, proportionate use of certification and accreditation to evidence compliance with minimum cyber security requirements. This annex provides further information on the expected costs and benefits of adopting this approach.

Certification And Accreditation

2. The following certification/accreditation schemes may be appropriate to demonstrate compliance with minimum cyber security requirements, depending on the specific risk profile of a contract.

Cyber Essentials (Self Assessment)

Cyber Essentials is a simple but effective UK Government-backed scheme that helps organisations, whatever their size, to protect against a range of the most common cyber attacks.

At the entry level, Cyber Essentials offers a "self-assessment" option, which involves answering questions about your critical cyber security arrangements and submitting these to a certification body, which will verify that the answers provided meet the requirements of the scheme.

Note that where small or medium firms do not have their own on-premise IT networks, they may be unable to achieve Cyber Essentials. In these circumstances, those organisations' own supplier cyber security arrangements are an important area of focus.

Further information can be found at the Cyber Essentials website.

Cyber Essentials Plus

Cyber Essentials Plus still has the same protections as Cyber Essentials. However, this time the verification of an organisation's cyber security is carried out independently by a Certification Body.

Further information can be found at the Cyber Essentials website.

IASME (Information Assurance for SMEs) Governance Standard (Audited):

IASME provides both a Level 1 and Level 2 Cyber Assurance Scheme, which considers the following controls:

- Risk Assessment & Risk Management

- Operational / People / Change Management
- Monitoring & Backups
- Data Protection (GDPR)
- Incident Management & Business Continuity

Level 1 is a self-certification, and Level 2 involves an independent audit. “Cyber Essentials” certification is a requirement of going for either level of IASME Cyber Assurance. The IASME Cyber Assurance Scheme was created to offer SMEs an affordable and achievable alternative to the international standard, ISO 27001. The IASME Governance standard maps closely to several widely recognised cyber security and assurance standards and guides. This means it can be used to demonstrate compliance to many of these standards, however it must be annually renewed.

Further information can be found at the IASME website.

ISO 27001

This is a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation’s information risk management processes. It includes details for documentation, management responsibility, internal audits, continual improvement and corrective and preventive action. The ISO standard requires co-operation by all parts of an organisation and is independently audited and accredited.

Further information can be found at the BSI website.

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: 978-1-83521-829-7 (web only)

Published by The Scottish Government, December 2023

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS1400534 (12/23)

w w w . g o v . s c o t