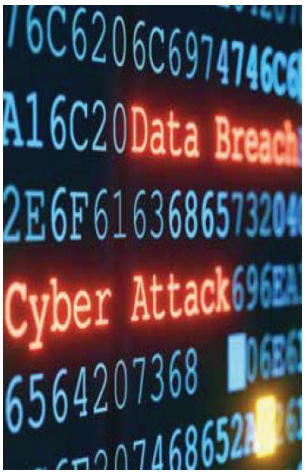
SAFE, SECURE AND PROSPEROUS:
A CYBER RESILIENCE STRATEGY
FOR SCOTLAND

PUBLIC SECTOR
ACTION PLAN



SCOTTISH PUBLIC SECTOR SUPPLIER CYBER SECURITY GUIDANCE NOTE

Version 1.1

This Scottish Public Sector Supplier Cyber Security Guidance Note has been produced by the Scottish Government Cyber Resilience Unit to accompany the Public Sector Action Plan 2017/18.

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

Scottish Government
Riaghaltas na h-Alba
gov.scot

CONTENTS

INTRODUCTION

1. 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. This Supplier Cyber Security Guidance Note has been developed to meet that commitment.

2. This guidance note forms part of the Scottish Public Sector Cyber Resilience Framework. It is intended for use by public sector organisations that are implementing the PSAP[1] and the Framework. The Framework is expected to be embedded in a number of audit and compliance requirements that apply to different parts of the Scottish public sector including the Scottish Public Finance Manual and Certificates of Assurance processes, with the aim of improving consistency and trust across the Scottish public sector.

3. In line with previous discussions and agreements between Scottish Ministers and key public sector partners, while it is ultimately for individual public sector organisations to decide on and adopt an approach to supplier cyber security that best meets their risk profile/appetite, wherever possible the adoption of a **consistent approach** to this issue is encouraged across the Scottish public sector. For the purposes of this guidance note, the Scottish public sector is broadly defined, and includes NDPBs, Non-Ministerial Departments, local authorities, health boards and universities and colleges.

4. This guidance note has benefited from 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 authority on cyber security, to ensure its work on cyber resilience is informed by appropriate technical expertise. As a result, the note aligns closely with NCSC supply chain guidance. Where appropriate, it also references guidance from the Centre for the Protection of National Infrastructure (CPNI), the UK-wide authority which provides protective security advice to businesses and organisations across the UK national infrastructure.

5. Cyber security arrangements for systems processing personal data form a key aspect of compliance with the new **General Data Protection Regulation (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

[1] Further information on the applicability of the Public Sector Action Plan and its associated requirements (including the Scottish Public Sector Cyber Resilience Framework that this guidance note will form part of) can be found at Annex A of the Action Plan Implementation Toolkit. Note that we expect the Scottish Public Finance Manual to be updated for FY 2020-21 to reflect the requirements of the PSAP and the Framework.

compliance with GDPR. The decision-making support tool described at Key Point 4 of this guidance note (The Cyber Security Procurement Support Tool or "CSPST"), has been designed to encompass GDPR requirements in respect of technical protections for personal data.

6. It must be clearly understood that **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

7. Most Scottish public sector organisations rely on suppliers or other partners to deliver products, systems, and services and require exchange of information to deliver those services effectively. 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.

8. Effectively 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. Examples of supply chain attacks can be found here.

9. A series of high profile, very damaging attacks has demonstrated that attackers have both the intent and ability to exploit vulnerabilities in supply chain security. This trend is real and growing. There is a clear need for Scottish public sector organisations to understand the cyber threat to supply chain security and to take appropriate, proportionate action to mitigate it.

THE KEY AIMS OF THIS GUIDANCE

10. The key aims of this 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[2].

QUESTIONS AND FEEDBACK

11. Public sector organisations with questions around implementation of this guidance note should write to cyberresilience@gov.scot for advice. Feedback is welcomed, and this guidance note will be updated on an ad hoc basis as required.

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. In summary, Scottish public sector organisations are encouraged to adhere to **4 Key Points** when managing cyber risks in their supply chains:

i. **Key Point 1:** They should follow the cyber security principles (the 12 Principles of Supply Chain Security) endorsed by the NCSC;

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

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

[2] See: https://www.ncsc.gov.uk/guidance/a4-supply-chain

iv. **Key Point 4:** In some circumstances, an information/cyber assurance process may indicate that **accreditations and certification** such as Cyber Essentials, IASME and ISO27001 (allowing also for equivalent standards) may be appropriate to provide additional assurance. The need for accreditations/certifications should continue to be judged on a case-by-case-basis by public bodies, with judgements as to proportionality supported by the information/cyber assurance process. Understanding the **scope** (and expiry date) of any certification is important.

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

> The **decision-making support, Cyber Security Procurement Support Tool** is being made available to support local information assurance processes used by public bodies, and to help promote greater consistency of application of this guidance note across the Scottish public sector.
>
> Any public sector organisation can make use of the tool to support their decision-making on supplier cyber security where they judge it appropriate to do so. Information on the CSPST tool, and how to use it in Scottish public procurement processes, is available here.

Scottish Government procurement processes have been strengthened in line with these Key Points.

3. Overall this guidance note advocates a **proportionate approach** to cyber security. It is intended to enable public organisations to manage cyber risks while mitigating any possible unintended impacts, particularly on SME suppliers, for example by making procurements uncompetitive due to disproportionate barriers to entry for firms.

APPLICABILITY AND TIMELINES

"SUPPLIER CYBER SECURITY" – IN WHICH SITUATIONS DOES THIS GUIDANCE NOTE APPLY?

4. This guidance note uses the terminology "supplier cyber security" throughout, as it is primarily intended to be relevant to situations in which public sector organisations are relying on suppliers – whether they be public (e.g. "shared service"), private or third sector organisations – to deliver goods or services under commercial contractual arrangements (i.e. as part of a supply chain).

5. The broad approach set out in this guidance note may also be appropriate in circumstances where public sector organisations rely on other organisations to deliver services under non-commercial arrangements (e.g. services provided by third sector organisations under grant funding or partnership arrangements).

6. Central guidance on grant funding and proportionate cyber security requirements will be developed on the basis of this guidance note in due course, to ensure clarity around issues of proportionality.

7. In general, public sector organisations are encouraged to consider all relevant circumstances where a cyber risk to their own security may be present as a result of interactions with other organisations, and consider applying the approach set out in this guidance accordingly.

APPLICABILITY – NEW AND EXISTING CONTRACTS - TIMELINES

8. Scottish public sector organisations are encouraged to begin applying this guidance note to all new contracts and other relevant arrangements with suppliers as soon as they are able to update their processes accordingly, and in any case during **Financial Year 2019-20**.

9. Scottish public sector organisations are also encouraged to give consideration to applying 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, on the basis of relevant financial, legal and risk management advice). Public sector organisations are encouraged to make judgements around the prioritisation of such work on the basis of **risk** and **criticality of services**, adopting an appropriately selective and/or phased approach to implementation. It is for individual public sector organisations to make an assessment of the appropriate scope and timeframe for such review processes, based on their own specific circumstances and assessment of risk.

   An example approach of prioritisation of contract review, developed by a UK public sector organisation, is included at **Annex B** for illustrative purposes.

   Where public sector organisations are subject to the **Security of Network and Information Systems (NIS) Directive** (in Scotland, this currently includes those in the health and water sectors), it is expected that Competent Authorities may wish to work with those bodies to arrive at a view on which existing arrangements should be prioritised to bring them into line with this guidance note and NIS requirements.

KEY POINT 1 – ADOPTION OF NCSC SUPPLY CHAIN PRINCIPLES

10. Scottish public sector organisations are encouraged to have regard to the NCSC's 12 Principles of Supply Chain Security[3] and consider carefully how best to incorporate the principles into their procurement processes and policies in a proportionate and effective way. 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 on its website**.

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

Heading	NCSC Principle	Practical considerations for Scottish public sector organisations
Understand the risks	**1:** Understand what needs to be protected and why	▪ This principle may be understood by Scottish public sector organisations both in the context of (i) their overall **cyber risk governance** arrangements and (ii) **specific contractual arrangements**: (i) The Public Sector Action Plan asked that all organisations have in place **minimum cyber risk governance arrangements** by end June 2018. These should already be helping public sector organisations to **identify key assets/services** that must be protected from cyber threats that may be introduced through supply chains. This understanding should mature over time. In implementing this principle, public sector organisations may wish to give thought to how the supply chain cyber risk to these assets should be reflected in **corporate risk registers**. (ii) This principle can also be understood in the context of **risk assessment of specific contractual or other service-provision arrangements with suppliers** – i.e. understanding what needs to be protected in specific circumstances and why.

[3] Note: These principles are directly referenced under NIS Guidance, thus ensuring consistency for Operators of Essential Services in the Scottish public sector (health and water), who may be expected under NIS to have regard to them.

		Adoption of **information/cyber assurance processes** can therefore help support application of this principle. The **decision-making support tool** (CSPST) can support consistent implementation of information/cyber assurance processes. Information on what CSPST is and how to use it can be found here.
	2: Know who your suppliers are and build understanding of what their security looks like	▪ The first part of this principle represents broader good practice in the context of supplier arrangements. It is good practice for Scottish public sector organisations to build, over time, clear central records that help them understand who is supplying what goods or services to their organisations. They may wish to view this as a process of continuous improvement, and approach it in a proportionate way. They may, for example, wish to focus on areas of high risk identified as a result of governance processes (e.g. prioritising an understanding of which suppliers have access to **personal data** or **sensitive information** for which the organisation is responsible). ▪ The requirement to **understand suppliers' security arrangements** in the context of specific contracts can be supported by the development of appropriate **information/cyber assurance processes** as outlined later in this guidance. ▪ Scottish public sector organisations are encouraged to make proportionate judgements, on the basis of **risk,** as to "how far down" the supply chain they should go (1st tier, 2nd tier, etc.) to build a picture of their supply chain and their security arrangements. For example, where supplier arrangements involve access to **personal data** or **sensitive information** for which the organisation is responsible, they may wish to require "Tier 1" suppliers **as part of contractual arrangements** to provide information on relevant sub-contracting

		and to apply consistent minimum security requirements. The **decision-making support tool** (CSPST) can support implementation of this principle, by helping public bodies to seek proportionate information from suppliers about their security arrangements in the context of specific contracts, and to build up an overarching picture of supplier cyber security over time. Consideration is also being given to extending CSPST in due course, to allow contracting authorities to manage risk further down the supply chain (the first iteration of the tool only supports consideration at the Tier 1 level). Information on what CSPST is and how to use it can be found here
	3: Understand the security risk posed by your supply chain	▪ The **NCSC guidance** provides helpful links to relevant resources aimed at supporting consideration of risk, which may help to strengthen public sector organisations' overall governance arrangements. ▪ The **decision-making support tool** (CSPST) can also support effective application of this principle, by helping to build an overview of all contracts an organisation has where a cyber risk is present. Information on what CSPST is and how to use it can be found here
Establish Control	**4:** Communicate your view of security needs to your suppliers	▪ The Scottish Government is working with the **Supplier Development Programme** to raise awareness of this guidance note amongst suppliers to the public sector, and to help promote a general understanding of how they can comply with minimum cyber security requirements. ▪ The Scottish Government has also produced a **supplier communications toolkit and associated materials** – available here – that can be used to support **awareness raising** about this policy and cyber resilience generally amongst suppliers. Organisations are free to make use of this toolkit and associated materials to support general communication with their suppliers if they wish to do so.

		▪ The **decision-making support tool** (CSPST) can also support effective application of this principle in the context of specific contractual arrangements. Information on what CSPST is and how to use it can be found here
	5: Set and communicate minimum security requirement for your providers	▪ This principle is key to the effective application of the guidance note. It is explicitly linked to the NCSC use cases, which provide examples of the sorts 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. ▪ Responsibility for ensuring appropriate minimum security requirements are in place rests with individual public sector organisations. ▪ The **decision-making support tool** (CSPST) has been produced to help support effective, consistent application of this principle. It is intended to align with the broad approach set out in the NCSC Use Cases. Information on what CSPST is and how to use it can be found here
	6: Build security consideration into your contracting processes and require that your suppliers do the same.	▪ This guidance note encourages Scottish public sector organisations to build consideration of cyber risk and minimum cyber security requirements into their procurement processes at appropriate stages, via the proportionate incorporation of information/cyber assurance processes. ▪ **Scottish Government procurement processes** have been updated where relevant, so that they promote the appropriate, proportionate use of information/cyber assurance assessments. The model contractual terms and conditions made available by the Scottish Government to the wider public sector have been updated to reflect the Guidance Note and (where appropriate) to support use of CSPST.

		■ The **Procurement Journey** and **Supplier Journey** have also been updated to reflect the contents of this guidance note, and to promote use of CSPST. ■ The Scottish Government has produced some **example wording** that public sector organisations can incorporate into Invitations to Tender, reflecting the contents of this guidance note and use of CSPST. Information on what CSPST is and how to use it can be found here ■ Scottish public sector organisation should consider including contractual requirements for Tier 1 suppliers to provide information on **relevant sub-contracting**, and to apply consistent minimum security requirements that the public sector organisation requires. ■ Scottish public sector organisations should consider requiring contracts to be renewed at appropriate intervals, with reassessment of associated risks at the same time.
	7: Meet your own security responsibilities as a supplier and consumer	■ Scottish public sector organisations may in particular wish to view this principle in the context of: ■ their achievement of Cyber Essentials or Cyber Essentials Plus under the PSAP – demonstrating to stakeholders the importance they place on having basic technical controls in place across the public sector, and ensuring the ability to say to suppliers in appropriate circumstances: "We do this, so we expect you to do it too"; 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	■ The information/cyber assurance assessment process and the decision-making support tool (CSPST) will

	your own supply chain.	help support communication of minimum security requirements in the context of specific contracts. ■ The Scottish Government is working with the Supplier Development Programme to help raise awareness of this guidance note amongst suppliers to the public sector, and to help promote a general understanding of how they can comply with minimum cyber security requirements. ■ The Scottish Government has also produced a communications toolkit and associated materials – here – that can be used to support **awareness raising** about this policy and cyber resilience generally amongst suppliers. Organisations are free to make use of this toolkit and associated materials to support general communication with their suppliers if they wish to do so. ■ Scottish public sector organisations should encourage suppliers that manage their own networks to join the Cybersecurity Information Sharing Partnership (CiSP) to help raise awareness of cyber threats.
	9: Provide support for security incidents.	■ Suppliers should have clear contractual obligations placed upon them in appropriate circumstances 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. ■ Scottish public sector organisations should also think carefully about what support they may reasonably need to provide to deal with security incidents, particularly those involving networks or systems that, if affected, could have a significant impact on their operations. ■ All Scottish public sector organisations should have developed **Cyber incident response plans** under the PSAP, which should detail procedures when cyber incidents occur as a result of supplier arrangements.

		▪ Scottish public sector organisations are encouraged to **share any key lessons learned** from incidents with the SG Cyber Resilience Unit (CRU). CRU will facilitate **sharing of these with the wider public sector** as appropriate.
Check your arrangements	**10:** Build assurance activities into your supply chain management.	▪ Model terms and conditions (available here) and example wording (available here) for inclusion in ITTs 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).
Continuous improvement	**11:** Encourage the continuous improvement of security within your supply chain.	▪ Scottish public sector organisations are encouraged to note the pragmatic, proportionate approach that is set out later in this guidance note with respect to minimum security requirements, and encapsulated in the decision-making support tool (CSPST). ▪ The Scottish Government has also produced a communications toolkit and associated materials – here – that can be used to support **awareness raising** about this policy and cyber resilience generally amongst suppliers. Organisations are free to make use of this toolkit and associated materials to support general communication with their suppliers if they wish to do so.
	12: Build trust with suppliers.	▪ Scottish public sector organisations are encouraged generally to build good relationships with suppliers, and to view cyber security as a shared concern.

KEY POINT 2 – ALIGNMENT OF MINIMUM SECURITY REQUIREMENTS (PRINCIPLE 5) WITH NCSC USE CASES

1. As noted above, **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 offers examples of appropriate minimum security requirements for different circumstances.

2. Scottish public sector organisations are encouraged to consider these "use cases" as their starting point for consideration of 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)

3. One way for public bodies to implement this principle effectively and align with the NCSC Use Cases is to build appropriate requirements into organisational information/cyber assurance assessment processes.

   A **decision-making support tool** (the Cyber Security Procurement Support Tool – CSPST) has been made available to the Scottish public sector to help support this, and to ensure consistent application by public sector organisations in Scotland. Further information on the CSPST tool, and how its use can help support the effective implementation of NCSC Principle 5, can be found here.

KEY POINT 3 – IMPLEMENTING THE PRINCIPLES: INFORMATION/CYBER ASSURANCE PROCESSES

4. One effective way of implementing many of the NCSC principles, and Principle 5 in particular, is to ensure that an **information/cyber assurance assessment** is undertaken. The purpose of this is to help public bodies to understand the levels of cyber risk present in specific contractual or other arrangements with suppliers, and identify the appropriate minimum cyber security requirements to address that risk.

5. Information/cyber assurance processes will generally involve a **questionnaire** to help 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 then generally inform the cyber security requirements that are placed on suppliers, and the questions asked of them to demonstrate they can appropriately mitigate risk.

6. 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.

7. **Scottish Government procurement processes** have been updated so that they:

   i. promote the use of information/cyber assurance assessments at the **strategy development stage** for individual procurements, to help understand what cyber risks may be present;

   ii. encourage **consultation with expert cyber colleagues** where available and appropriate. Internal cyber resilience and/or data protection colleagues within organisations are often well-placed to help "sense-check" an initial risk assessment outcome, and help provide guidance as to what cyber security requirements should be placed on suppliers based on the outcome of the information/cyber assurance assessment. Where such expertise is available, this can greatly assist with ensuring appropriate application of cyber security standards based on the specific circumstances of the case. Where such 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 3 of the Dynamic Purchasing System);

   iii. encourage (where appropriate) the **identification and communication of clear, proportionate minimum cyber security requirements when procuring**. Bidders will then be required, where appropriate, to demonstrate how they meet these requirements when responding to tendering opportunities; and

iv. in order to ensure proportionality, allow for buyers to opt to **manage cyber risks in a proportionate way**. This may include requiring suppliers to achieve compliance with minimum security requirements over a certain timeframe on condition of contract award (thus preventing automatic exclusion of suppliers that do not initially have appropriate protections in place, but who are willing to work towards achieving these).

Where appropriate, these processes make use of the **decision-making support tool** (the **Cyber Security Procurement Support Tool)**, in order to ensure greater consistency of application, and to minimise the additional necessary burdens placed on buyers and suppliers. Further information on CSPST, and how to use it in procurement processes, can be found here.

8. Where public sector organisations are using their own procurement or other processes to secure goods or services from suppliers, they are **encouraged to consider incorporating their own information/cyber assurance processes as appropriate**. They may also make use of the decision-making support tool described below to facilitate this.

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. Some Scottish public sector organisations already ask suppliers to demonstrate that they hold cyber security certifications in certain circumstances.

10. Certification should be seen as one way of gaining greater assurance around a supplier's cyber security, beyond assertions made by the supplier. Others include the incorporation of cyber security requirements into contractual terms and conditions, and audit.

    While the CSPST tool provides a way for suppliers to self-assess against a contract's cyber security requirements, and answers can be incorporated into terms and conditions and audited where appropriate, certification can provide another type of independent confirmation that a supplier's answers are accurate.

11. Scottish public sector organisations are encouraged to adopt the following broad approach to cyber security accreditation and certification when procuring goods and services:

    - They should judge the need for accreditation or certification on the basis of an appropriate **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.

    - Questions around the **scope of certification**, any **expiry date**, and ensuring **ongoing good practice** are vitally important.

    - Certification/accreditation should be viewed as **one way of achieving independent assurance that cyber security requirements are in place**. It should not be viewed as a "silver bullet" – good cyber security is fundamentally a cultural issue. Wider measures such as adherence to the 12 NCSC supply chain principles, use of contract requirements and use of audit are equally important.

    - The use of certification/accreditation can impose costs on both suppliers and purchasers and this means that **cost effectiveness and proportionality** must always be taken into account. 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.

- Public sector bodies should also consider accepting assurances from a supplier that they will **work towards achieving any certification/accreditation by an agreed date**.

- Public sector bodies should be willing to accept **equivalent evidence** that demonstrates a level of cyber security that equates to or exceeds the requirements of certification/accreditation. They may wish to ask suppliers to provide concise, accessible evidence that this is the case (e.g. clear "mapping" of the controls under the actual certification produced by the supplier against the controls under the certification requested by the public sector organisation). The decision-making support tool has been designed to help "translate" the requirements of 3 key standards widely used in public and private sector procurement: Cyber Essentials, IASME Gold and ISO27001.

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

OTHER IMPORTANT ISSUES

REQUIREMENT TO ENSURE PROPORTIONALITY

13. 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 decision-making support tool, CSPST, is intended to help inform these judgements, and ensure that appropriate, but not overly prescriptive or expensive security controls, are considered. In particular, it supports and encourages the use of **Cyber Improvement Plans** for suppliers who do not, at the time of bidding, meet minimum cyber security requirements. More information on these issues can be found in "Using CSPST in Procurement", which is available here.

RESPONSIBILITY FOR CYBER RISK MANAGEMENT

14. 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.

15. This guidance note and the decision-making support tool (CSPST) 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.

16. 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.

ANNEX A – CERTIFICATION AND ACCREDITATION – COSTS

1. Key Point 4 of this guidance note encourages the appropriate, proportionate use of certification and accreditation in order 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 – COSTS

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. The table below provides some information on the broad costs associated with achieving certification under those schemes. It should be noted that, where a supplier does not currently meet the requirements for certification/accreditation, additional costs may need to be incurred in order to improve their cyber security arrangements to the point where certification/accreditation can be achieved.

Certification/accreditation scheme	Costs	Further information
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.	The costs of Cyber Essentials self-assessment are around **£300**, although some accreditation bodies (notably CREST) require more rigorous tests as part of entry level certification, which increase costs to around **£1,000**. If an organisation is not meeting the basic requirements of Cyber Essentials, they may need to spend additional money to improve their cyber security. However, an organisation that does not meet the basic requirements of the scheme may be at increased risk of cyber attack.	Further information can be found at the Cyber Essentials website, here.

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.		
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.	The costs of Cyber Essentials Plus certification will depend on the size and complexity of the organisation's network. For SMEs, some certifying bodies quote between **£1,000 to £3,000.** Again, if an organisation is not meeting the basic requirements of Cyber Essentials, they may need to spend additional money to improve their cyber security.	Further information can be found at the Cyber Essentials website, here.
IASME (Information Assurance for SMEs) Governance Standard (Audited): Audited IASME Governance (sometimes known as IASME Gold) is an independent on-site audit of the level of information security provided by an organisation. IASME state that it offers a similar level of assurance to the ISO 27001 standard but is designed to be simpler and often cheaper for small and medium-sized	The costs of Audited IASME Governance certification will depend on the size and complexity of the organisation. For SMEs, some certifying bodies quote between **£1,500 to £4,000.** This is in addition to **£400** to gain the initial IASME Governance verified self assessed certification. (All prices exclude VAT).	Further information can be found at the IASME website, here.

organisations to implement. The standard includes all of the five Cyber Essentials technical topics and adds additional topics that mostly relate to people and processes, for example: - Risk assessment and management - Training and managing people - Change management - Monitoring - Backup - Incident response and business continuity The Audited IASME Governance certificate builds on a self-assessment similar to the basic Cyber Essentials one.	If an organisation is not meeting the basic requirements of the IASME Governance standard, they may need to spend additional money to improve their cyber security and governance.	
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	The cost of an ISO 27001 accreditation is considerably more than for Cyber Essentials and Cyber Essentials Plus. The price will vary based on complexity and size of organisation. Whereas Cyber Essentials and Cyber Essentials Plus can be implemented in a relatively short time frame it is likely that an ISO 27001 accreditation will take considerably longer. This is again dependent on an organisation's complexity and size. Factors such as the cost of training and literature for staff, the cost for external remedial assistance and	Further information can be found at the BSI website, here.

independently audited and accredited.	technology to achieve the specification and the cost of the actual certification itself are all factors. Estimated costs for the certification process alone without remedial work for an organisation of around 150 employees can be in the region of **£10,000 plus.**	

ANNEX B – REVIEW OF EXISTING CONTRACTS – PRIORITISATION – ILLUSTRATIVE EXAMPLE

1. An example approach of how to conduct a review of cyber risks in **existing contracts** is set out below. This approach was adopted by a public sector organisation, and has been shared for illustrative purposes only.

Overarching approach

- All relevant areas should conduct a Risk Assessment on any contract which is currently live but has not had a Risk Assessment completed. The Risk Assessment is conducted using *[the online decision-making support tool]*, and should take no more than *[1 – 2 hours]* to complete.

- Suppliers should then be requested to complete a Supplier Assurance Questionnaire in line with the prioritisation approach set out below (which proposes a series of Tranches and Steps). This will identify compliance, the need for risk acceptance, or the requirement to discuss the implementation of a Cyber Improvement Plan to address non-compliance where the risk is deemed not acceptable.

- The review process is complete once all Risk Assessments and SAQs are complete for each contract.

Prioritisation

- A logical and risk-based approach will be adopted. It will use Tranches and Steps to prioritise work to address the contracts with the greatest risk first.

- Contracts with fewer than 2 years left to run are out-of-scope (unless a 'wild card' – see below).

- Older contracts which still have more than 2 years left to run are assessed as being at greater risk and are prioritised for risk assessment and remediation/acceptance of risk.

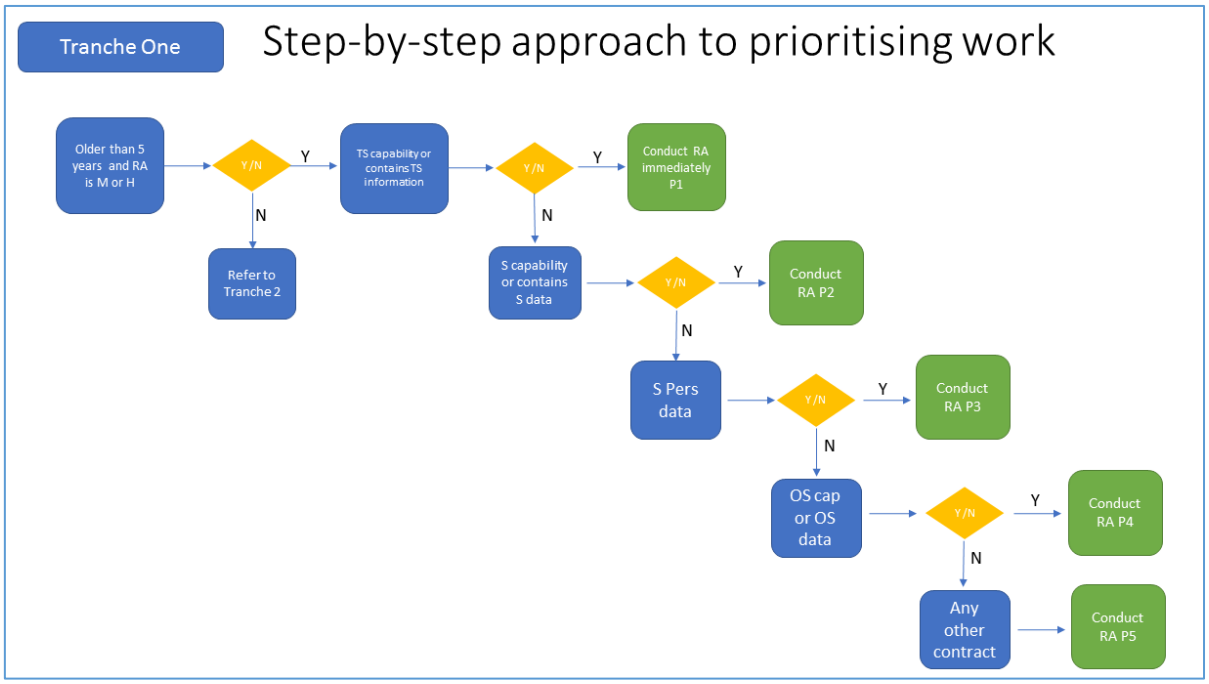
- Remediation will be effected via contract change. Cyber risk in existing contracts can be accepted via a defined process.

- Contracts may be identified as a 'Wild Card' and prioritised at discretion of the risk owner, despite not meeting the relevant criteria set out above.

Tranches and steps

- **Tranche 1** will begin on [X date] with a target completion date of [Y date]. It will focus on contracts that are **more than five years old but which still have more than 2 years left to run, and which are assessed by the decision-making support tool as being [moderate/high risk]**. Within this class of contracts:
    - The first step will be to address any contract which supports a TOP SECRET (or above) capability or contains TOP SECRET (or above) information.
    - The second step will be to address any contract which supports a SECRET capability or contains SECRET information.
    - The third step will be to address any contract which processes sensitive personal data as defined by the GDPR.
    - The fourth step will be to address any contract which supports an OFFICIAL SENSITIVE capability or contains OFFICIAL SENSITIVE (this includes any personal data) data.
    - The fifth step will be to address any other relevant contract.

    The diagram below presents a visual representation of this process.



- **Tranche 2** will begin on [X date] with a target completion date of [Y date]. It will focus on contracts that are **fewer than five years old but which still have more than 2 years left to run, and which are assessed by the decision-making support tool as being [moderate/high risk]**. Prioritisation of steps will be as for Tranche 1.

- **Tranche 3** will begin on [X date] with a target completion date of [Y date]. It will focus on contracts that are **more than five years old but which still have more than 2**

years left to run, and which are assessed by the decision-making support tool as being [low risk]. Prioritisation of steps will be as for Tranche 1.

- **Tranche 4** will begin on [X date] with a target completion date of [Y date]. It will focus on contracts that are **fewer than five years old but which still have more than 2 years left to run, and which are assessed by the decision-making support tool as being [low risk]**. Prioritisation of steps will be as for Tranche 1.

- **Tranche 5** will begin on [X date] with a target completion date of [Y date]. It will address any remaining contracts.

Process completion and outcomes

- The review process is complete once all risk assessments and SAQs are complete for each Tranche.

- A successful outcome will be to illuminate, understand and manage the cyber risk exposure across the department's supply chain; not to mitigate every single risk.

This guidance note has been produced by the Scottish Government Cyber Resilience Unit to support implementation of the Scottish Public Sector Cyber Resilience Framework.

Please send all comments, questions or additions to cyberresilience@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: 978-1-83960-139-2 (web only)

Published by The Scottish Government, August 2020

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS756626 (08/20)