Secure Connected Places Playbook
Cyber security resources for local authorities

Department for
Science, Innovation,
& Technology

Procurement & supply chain management

Advisory

The Secure Connected Places Playbook is designed to meet the general cyber security needs of local authorities across the UK's four nations when integrating smart cities technologies. Whilst this guidance is appropriate to all local authorities there may be separate nation specific guidance and processes that should be considered.

Similarly, the resources within the playbook generally assume the local authority has control over technology policies and their implementation. Additional consideration may be required where this is not the case such as the interactions between combined and unitary authorities where one must collaborate and co-ordinate with other parties.

Executive summary

What is this resource?

This resource provides local authorities with guidance on how to incorporate cyber security considerations into supply chain management lifecycle of their connected places, with a particular focus on the procurement stage.

How should I use it?

This resource should be used in conjunction with, and does not replace or supersede, local and national procurement policy and legislation. It is also not intended to be a step-by-step guide. Instead, local authorities should use the guidance to augment the specific stage of the supply chain management lifecycle that they are in. The guidance has a focus on procurement and provides a series of example security questions which can be asked of suppliers, these questions should be adapted to the specific procurement and local context.

Who does this resource apply to?

The guidance set out here is particularly relevant to those who design and manage connected places projects, such as project managers, and those in procurement and supply chain management roles.

What will I get out of using this resource?

All local authorities rely on their supply chains to provide hardware, software and other services for their connected places projects. While this has many benefits, it also introduces potential cyber security risks.

Weaknesses in the supply chain can be targeted by criminals intending to harm and exploit the end user/organisation.

Depending on the exact commercial model used, some cyber risk can be transferred to a supplier. However, it is ultimately still the local authority, its residents and businesses that will suffer from any cyber security incident.

Using this resource will help you understand the specific considerations that connected places supply chains need, with a particular focus on the procurement of secure connected places technologies.

Case study: Dorset Council

Dorset Council

Dorset Council has well-functioning, mature procurement processes and supply chain management. However, there is limited availability across their specialist technical resource. The council identified a need to upskill non-procurement colleagues and raise the profile of security considerations when procuring connected places systems.

Using this procurement and supply chain management resource, Dorset Council plans to implement a minimum-security requirement across all new connected places technology procurements, taking the suggested security questions as a baseline and adjusting for their local context and risk appetite.

See Appendix for more on this case study and how this resource draws on the content of the NCSC's Connected Places Cyber Security Principles.

Case study: City of Bradford Metropolitan District Council

When Bradford Council started its connected places journey, they found little guidance beyond the NCSC Connected Places Cyber Security Principles. Instead, they undertook security risk assessments based on good practice around hardware, applications and systems. Bradford Council have since enhanced their connectivity through their own network. The Council used the STRIDE-based threat analysis and Procurement and Supply Chain resource to address security issues before technology deployment and agree on the security boundaries with their suppliers. More recently, Bradford Council have applied this guidance to their real life projects by strengthening their questionnaire. When they were procuring IoT cameras with Artificial Intelligence (AI) built in to help reduce fly tipping in their rural areas, they implemented a checklist to make sure they covered the various elements of procurement before agreeing the contract with suppliers.

Contents

The supply chain management lifecycle

Supply chain management lifecycle

This resource provides guidance and support across the whole supply chain management lifecycle, from early industry engagement where expectations are set, through to end-of-life where projects close down and hardware and data must be appropriately handled.

Weaknesses in any of these areas can compromise the whole lifecycle and increase the cyber security risk in your local authority.

Engagement

Early engagement with the supply market allows the authority to understand the available solutions and prepare the market with the authority's expectations.

Requirements

Developing strong requirements, particularly on cyber security, will help ensure that you procure the right solution but also reduces incorrect interpretation by suppliers.

Procurement

Asking the right questions in procurement stages, and evaluating responses appropriately, helps to ensure that authorities procure the right solution.

Management

Cyber security must be fully considered when designing and building solutions. Continuous improvement through contract management is critical to good cyber security.

End-of-life

Being clear on what will happen to solutions once they reach their end-of-life will ensure that hardware, software, and data is securely managed and disposed of.

What is supply chain security management in connected places projects, and why is it important?

With many local authorities relying on their supply chain across the whole connected places project lifecycle, it's important that cyber security is considered a priority in supply chain management.

Good supply chain cyber security management will help ensure that suppliers (and sub-contractors) align with the cyber security goals of your local authority. It reduces the risk of incidents throughout the supply chain and the impacts on the local authority, its residents and businesses.

Supply chain security management is all about working in partnership with suppliers and getting them thinking about security from the outset of a connected places project, even before a contract begins.

It can be easy for authorities to take the view that they 'hand off' cyber risk to suppliers, but this is not the case. The risk always lies with the authority no matter what their suppliers say or do.

Good supply chain security is critical to secure connected places projects. Attackers are increasingly and purposefully targeting supply chains to disrupt end organisations such as local authorities. A cyber weakness in your supply chain is no different to one in your organisation in the eyes of an attacker.

This guidance is focussed on the management of cyber security in procurement and the supply chain, but the importance of accompanying personnel and physical security measures, and therefore a holistic security approach, should not be forgotten. Further information is available on the NPSA website.

Engagement

Engagement

You may wish to engage the potential supplier market before procuring a solution for your connected places project. This will depend on the size and complexity of your procurement, how well-defined your requirements are and your local procurement policy and processes.

Engagement

Early engagement with the supply market allows the authority to understand the available solutions and prepare the market with the authority's expectations.

Requirements

Developing strong requirements, particularly on cyber security, will help ensure that you procure the right solution but also reduces incorrect interpretation by suppliers.

Procurement

Asking the right questions in procurement stages, and evaluating responses appropriately, helps to ensure that authorities procure the right solution.

Management

Cyber security must be fully considered when designing and building solutions. Continuous improvement through contract management is critical to good cyber security.

End-of-life

Being clear on what will happen to solutions once they reach their end-of-life will ensure that hardware, software, and data is securely managed and disposed of.

Early supplier engagement

Engaging with the potential supplier market early in the process gives two main benefits:

1. It allows you, the authority, to **understand the state of the market and what is currently achievable.** This means you can develop requirements that are realistic and deliverable by the market but also push the boundaries.

2. It provides an opportunity for you to **communicate your expectations of connected places cyber security to the market**. This gives suppliers time to consider what developments they need to make to their solutions to meet your expectations.

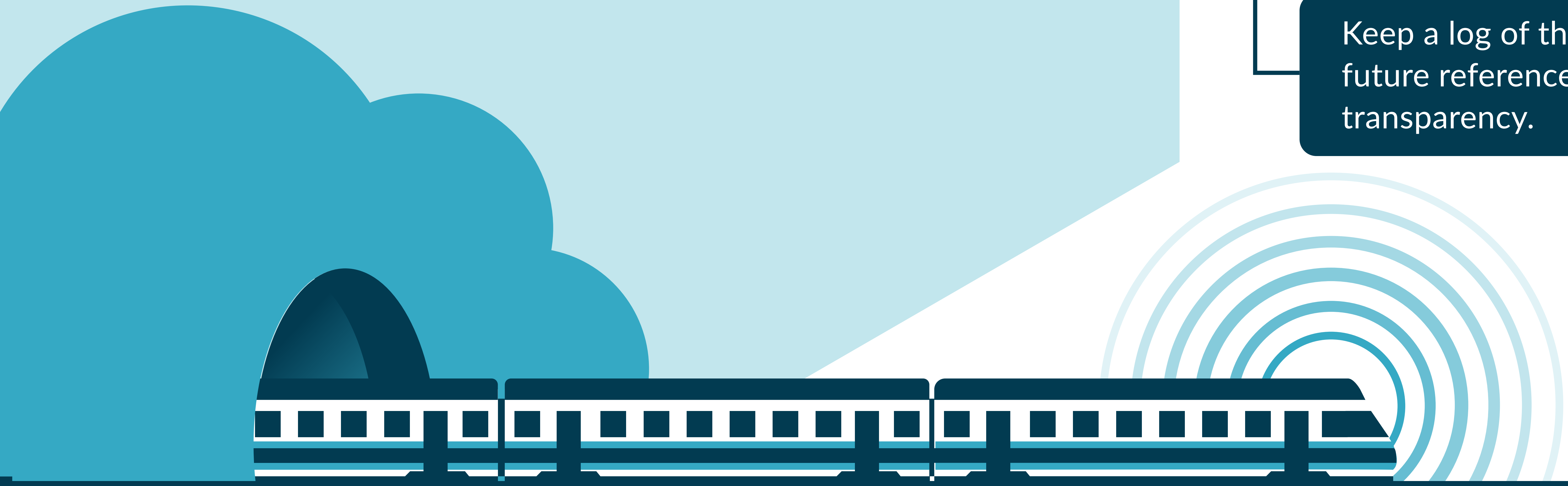
Industry engagement must be a formal part of the procurement process whereby the market is notified of any events and all are given the opportunity to attend, ask questions and receive responses.

There are additional ways to gather information such as **desk-based research, market intelligence reports and attending industry conferences/exhibitions.**

Keep a log of these for future reference and transparency.

It's important that care is taken **not to create unfair competition** by giving away information not available to others, or by making requirements specific to a single company or solution.

In conducting this type of research you should always be aware that the information from the supplier is likely to be marketing/sales material and so should be taken in context and viewed holistically with multiple sources.



Requirements

Requirements

After engaging the potential supplier market you must define your requirements that will be put to potential suppliers through the subsequent procurement phase(s).

Engagement

Early engagement with the supply market allows the authority to understand the available solutions and prepare the market with the authority's expectations.

Requirements

Developing strong requirements, particularly on cyber security, will help ensure that you procure the right solution but also reduces incorrect interpretation by suppliers.

Procurement

Asking the right questions in procurement stages, and evaluating responses appropriately, helps to ensure that authorities procure the right solution.

Management

Cyber security must be fully considered when designing and building solutions. Continuous improvement through contract management is critical to good cyber security.

End-of-life

Being clear on what will happen to solutions once they reach their end-of-life will ensure that hardware, software, and data is securely managed and disposed of.

How to define security requirements for procurement?

Defining requirements is potentially one of the most critical aspects of secure supply chain management.

Security requirements for connected places projects should:

- ✓ Tell suppliers exactly what you're trying to buy and how it will be managed throughout its lifecycle.
- ✓ Be consistent with the NCSC Connected Places Cyber Security Principles.
- ✓ Cover the whole project lifecycle, from design through to end-of-life.
- ✓ Be realistic, attainable and measurable. Think about how you would check that a requirement has been met by a supplier.

Types of requirements

It can be useful to think of requirements in a series of groupings or types. This can help you to ensure that you cover all bases.

<table>
<tr><th colspan="2">Solution Requirements</th><th>Business Requirements</th></tr>
<tr><td colspan="2">Solution requirements describe the specific security characteristics that a connected places solution must have to meet the needs of the local authority.
These can be further broken down into two categories:</td><td rowspan="3">These include high-level statements of goals, objectives and needs. Business requirements do not include any details or specific features, they state the problem and the business objective to be achieved.
Security requirements should be present here and align with the local authority’s wider security aims and posture.
E.g. one requirement may be to “Keep all personally identifiable data safe and secure in transit and at rest”.
While this may seem obvious, writing it down as a formal requirement makes all involved think of security from the start.</td></tr>
<tr><th>Functional</th><th>Non-Functional</th></tr>
<tr><td>Functional requirements describe the features that a solution must have.
Example: The sensor management system must implement a password for each user account</td><td>Non-functional requirements define how the solution must perform.
Example: User passwords for the sensor management system must have a minimum of 8 characters, including 1 number and 1 special character.
Example: User passwords must be stored using the PBKDF2 standard</td></tr>
</table>

Prioritising requirements

Security requirements should be prioritised to ensure that those which are absolutely essential are met by all suppliers. It is natural for a wide range of requirements to be developed but not all will be essential.

As outlined earlier in this resource in the example questions, buyers may wish to set a minimum standard that all suppliers must meet. This can be done by having a set of requirements as MUST.

The most common method for prioritising security requirements is **MoSCoW**.

This stands for:

Must

Must have this requirement to meet the authorities connected place security need.

Should

Should have this requirement if possible but the connected places project does not rely on it.

Could

Could have this requirement if it does not come at the detriment of other requirements.

Would

Would like to have this requirement but it will not be delivered at this time.

Communicating and documenting requirements

It is no use having a lot of well developed requirements if you are not able to communicate and manage them appropriately, particularly with suppliers during early engagement activities and the ITT.

A common method of documenting and communicating requirements is through user stories. These take the form of:

> “As a [user], I want [requirement], so that I can [reason]”.

This provides traceability of the requirement, we know who has come up with it (the specific user), it details the actual requirement and it provides some context and reasoning for that requirement existing.

It is useful to store requirements in a database or spreadsheet that provides easy filtering and management. All requirements should have unique reference numbers for simplicity, should have a source and have an owner (someone who can be contacted to find out more about that requirement if needed and can ‘sign off’ that it has been met).

Some requirements may also be better communicated in diagram form. For example, system architecture diagrams, data flow diagrams etc.

Procurement

Procurement

This resource starts with procurement as it is a particularly challenging area of cyber security and one of the more critical elements of the lifecycle. In this section, guidance is provided on asking the right questions of suppliers at the procurement stage.

Engagement

Early engagement with the supply market allows the authority to understand the available solutions and prepare the market with the authority's expectations.

Requirements

Developing strong requirements, particularly on cyber security, will help ensure that you procure the right solution but also reduces incorrect interpretation by suppliers.

Procurement

Asking the right questions in procurement stages, and evaluating responses appropriately, helps to ensure that authorities procure the right solution.

Management

Cyber security must be fully considered when designing and building solutions. Continuous improvement through contract management is critical to good cyber security.

End-of-life

Being clear on what will happen to solutions once they reach their end-of-life will ensure that hardware, software, and data is securely managed and disposed of.

Questions to ask, and how to score them

Assessing the security of solutions should be done at all points in the procurement phase. For example, if running an early-stage supplier engagement, it can be useful to include security questions to exclude solutions early that are not going to meet your cyber security requirements and also to give suppliers a view on what to expect on cyber security at the Invitation to Tender (ITT) stage.

The proportion of evaluation scores and weighting allocated for cyber security will vary depending on the exact procurement and the cyber security posture of your authority. For example, if you are procuring a solution which uses lots of Personally Identifiable Information (PII) and there is increased cyber risk then appropriate cyber security questions may make up a greater proportion of available scores.

Questions which suppliers must meet should be scored pass/fail while others can be scored on a scale in the same way as other technical questions. It is important to engage a broad range of other stakeholders within the local authority to decide which cyber security questions to ask.

Evaluating responses appropriately will ensure fairness for bidders and that the local authority has the best solution for their needs. It is therefore essential to have the right expertise from across the local authority to evaluate responses.

Example questions

The following are example questions which can be used as a starting point and tailored appropriately depending on the exact procurement taking place. The questions chosen will depend on any local authority context and policy. A range of internal stakeholders should be consulted to ensure that the most appropriate questions are included, and that there is sufficient expertise to evaluate responses.

Security Governance

	Question	**Response guidance**
1	Provide evidence of relevant security certifications for your organisation and solution (e.g. ISO27001, Cyber Essentials or Cyber Essentials Plusn	A minimum certification that suppliers must comply with is Cyber Essentials or Cyber Essentials Plus. Does the scope of the certifications cover the parts of the service(s) the supplier will be providing and how TVCA will be using them?
2	Does the supplier have people and processes in place that are responsible for cyber security?	Produce evidence e.g. process maps, team structure etc. Are policies in place which are accessible to everyone affected. What feedback mechanisms are in place to identify whether policies are followed in practice.
3	Are the people occupying security roles suitably skilled and experienced?	Provide evidence of skills and experience e.g. relevant certifications

Example questions

	Question	Response guidance
4	Provide details of any penetration (pen) testing conducted by your organisation or a third party on your solution. Was this carried out by a CHECK or CREST registered organisation?	Suppliers should be able to provide evidence of pen testing.
5	Detail how data will be encrypted in transit, including details of the encryption standard(s) to be applied. A diagram can be used as a response	Data should be encrypted while in transit. The specific encryption standard(s) used (e.g.TLS1.3, HTTPS, AES-256, SHA384) and where they are applied will likely vary by supplier but they should aim to be using the latest standard, or have a roadmap to adopting the latest standard(s). The supplier should provide evidence showing what encryption is applied and where in the system data is encrypted and decrypted. This may not be applicable depending on procured solution.
6	Where appropriate, detail how data will be encrypted at rest, including details of the encryption standard(s) to be applied. A diagram can be used as a response	Data with protection requirements should be encrypted while at rest. The specific encryption standard(s) used (e.g. AES-256, SHA384) and where they are applied may vary by suppliers. Suppliers should provide evidence showing what encryption is applied and where in the system data is encrypted and decrypted.
7	Describe how and where data is stored for your solution (e.g. cloud, on-prem, public, private), including geography (e.g. within the UK, transferred overseas)	Suppliers should provide details on where data centres are located and what type of infrastructure it is.
8	Describe your understanding of the NCSC Connected Places Cyber Security Principles and how your solution is consistent with the Principles?	Describe your understanding.

Example questions

Managing & Recovering from Incidents

	Question	Response guidance
1	Detail the business continuity and recovery processes and policies applied to your solution, including detail on any data back-ups.	Suppliers should provide details of a robust plan for what happens to their solution in case of disruption, this may include backup infrastructure such as networks and data processing/compute. Suppliers should provide detail on their data back-up systems including the frequency of these and what is included in each back-up.
2	Has the supplier suffered any material security breaches or compromises which they need to declare?	Provide evidence.
3	What business continuity / disaster recovery plan does the supplier have for maintaining minimum service levels to you, should they suffer an incident.	Provide evidence.

Network Protection

	Question	Response guidance
1	Describe the process for continuous improvement of your solution, including any routine schedule patching/maintenance and emergency patching timescales.	Suppliers should provide detail of any upcoming planned maintenance and patching of their solution, for example, updating to latest software/coding versions. You should also provide timescales for patching of newly identified bugs/vulnerabilities.

Example questions

Cloud Services Only

	Question	Response guidance
1	How does your solution collect, store and analyse event logs for security purposes?	Supplier solutions should include logging functionality which records security logs such as logins, data transfers etc. If appropriate, local authorities should be integrated these logs into the suppliers existing Security Operations Centre (SOC).
2	Describe the account access policies applied to your solution (e.g. minimum password requirements, multifactor authentication, password expiration, inactivity expiration, IP Address whitelisting etc). Where the authority has policy on this it should be included with the question e.g. the local authorities minimum password policy.	Suppliers should provide detail on their account access policies and where there is alignment to any provided local authority policies.
3	Describe the process for account creation and deletion for your solution (e.g. when a member joins or leaves the authority or supplier teams)	Suppliers should provide details on a robust process for creating and deleting accounts for their solution. Authorities may wish to make this a pass/fail requirement in alignment with their own local policy.

Example questions

Protecting Data

	Question	Response guidance
1	Do they encrypt data on portable devices such as laptops, mobile phones, tablets and removable media, in case of loss or theft?	Provide evidence.
2	Does the supplier securely wipe or destroy all storage media prior to disposal or re-use?	Provide evidence.
3	If they allow BYOD, how do they protect data on BYOD devices?	Provide evidence.
4	Does the supplier have processes in place to detect and prevent unauthorised or unusual (e.g. very large) data transfers from their network?	Provide evidence.
5	Do they use secure email and secure data connections to their network, to protect data in transit?	Provide evidence.
6	How do they constrain access to sensitive data?	Provide evidence.

Example questions

Offshoring & Personal Data

	Question	Response guidance
1	Does the supplier offshore any components of their service to you, such as data storage, data processing, support, development or maintenance of services?	If the answer is YES: - In which locations and what security controls are in place around those offshore components? - Will they notify you if any of the locations change, or if they change any of their offshore subcontractors? - Will any of your personal data be subject to offshore storage or processing?
2	Does the supplier handle or process any personal data as part of their service to you, and if so, does it meet the GDPR security principles?	If the answer is YES: - Is their use of personal data lawful, fair and transparent? - Is it only used for the purposes it was collected for and nothing else? - Do they only collect the minimal amount of personal data required? - Is the personal data accurate, up to date, protected and deleted when no longer required?

Data Retention

	Question	Response guidance
1	Describe the data retention and deletion policy that will be applied to your solution, including at end-of-life, including any data stored on hardware (e.g. on sensors)	Suppliers MUST provide detail on how data is treated at the end of contract/product/service life. This should include what data is retained, where it is retained, who owns that data, and for how long, including what data is destroyed and how this takes place. If hardware is included the supplier should detail how this hardware is destroyed.

Example questions

Personnel Security

	Question	Response guidance
1	Does the supplier carry out suitable background checks on employees and have processes in place for in-house personnel security controls?	Provide evidence.
2	Does the supplier have security awareness training, covering common attacks on users, such as phishing and other means of enticing users to disclose sensitive information, or download unauthorised code?	Provide evidence.
3	Does the supplier encourage a positive security culture? For example, do they encourage users to report suspected or actual incidents promptly in a no-blame environment?	Provide evidence.
4	Has the supplier performed a risk assessment to understand their insider threat?	Provide evidence.

Example questions

Physical Security

	Question	Response guidance
1	Does the supplier have suitable physical controls in place to protect data, networks and premises?	Provide evidence.
2	Do they securely dispose of sensitive printed information?	Provide evidence.

Independent Testing & Assurance

	Question	Response guidance
1	How does the supplier monitor, identify, assess and mitigate new cyber security risks to your solution?	Suppliers should detail their threat management process, which should include the four elements mentioned in the question. This should include monitoring your own supply chains.
2	Does the supplier conduct any independent security tests, such as penetration tests of their internal and external IT infrastructure and remediate any findings?	Provide evidence.

Example questions

Other Considerations

	Question	Response guidance
1	Detail any Application Programming Interfaces (APIs) used in your solution, including the technology used and where in the architecture they are used.	Suppliers should detail any APIs used and the security controls around these.
2	Describe the governance and risk management process for your solution, throughout the lifecycle from design/build to run/maintain and end-of-life.	Suppliers should detail their organisational structure which should include how risks are escalated, how they are identified and assessed, and which risks get escalated where. They should include how risks are treated.
3	Will the supplier (or any subcontractors employed by the supplier) connect, or have access to, your data, IT network or premises?	If so, How will this be limited, controlled, and monitored? - For any remote access to Your data or IT network, (for example in cases of outsourced IT support), do you have a remote access support agreement in place? - Do you log their remote access sessions on Your systems, with logs captured to reflect the work done?

Crown commercial frameworks

Crown Commercial Services (CCS) helps the public sector buy what it needs, when it needs, saving them time and money.

CCS have a wide range of commercial agreements which use competition among suppliers to deliver high-quality services, good outcomes and value for money. These agreements, known as frameworks, provide an easy and compliant route to market for buying organisations. A number of these frameworks include cyber security as a standard, either covering an entire organisation or to support the delivery of specific local government services.

Suppliers on these frameworks are evaluated for cyber security capability by CCS using the Cyber Essentials Plus accreditation. CCS does not evaluate every individual product that may be offered by a supplier. For example, if the framework is for the provision of CCTV equipment, then the buying organisation may wish to check the cyber security standards which apply to individual pieces of hardware before committing to a purchase.

CCS can provide more bespoke support and advice in selecting the best route to procure your secure connected places products and services. Their sector managers have detailed knowledge of which framework(s) and solutions best match your needs.

There are many CCS frameworks which may be suitable for procuring connected places products and services, more detail can be found on the CCS website, along with specific guidance found here.

Network Services 3 Framework

With CCS being the biggest public procurement organisation in the UK, they have a tailored free to use framework called Network Services 3.

- ✓ This framework and specifically lot 3a has been crafted to enable the procurement of complete IOT and connected spaces solutions.
- ✓ The Framework complies with public procurement regulations and gives you access to 26 vetted suppliers who are leaders in their respective capabilities.
- ✓ Suppliers are required to comply with key security principles when providing a solution and meet the NCSC standards pertaining to security standards and practices.
- ✓ As a Buyer you would have access to competitive large scale enterprise pricing.

Details of this framework can be found at https://www.crowncommercial.gov.uk/agreements/RM6116 Alternatively you can contact the team directly at info@crowncommercial.gov.uk who will be happy to discuss your requirements further with you.

Cyber security certifications

There are common cyber security standards and certifications that suppliers may align to. It is important to understand what these mean in reality as they are often misunderstood by buyers.

<table>
<tr><th colspan="2">Cyber Essentials</th><th>ISO 27001</th></tr>
<tr><td colspan="2">A government-backed certification scheme which helps organisations of all sizes to protect themselves from the most common cyber attacks.
It does not certify that any product or service provided by the company is safe and secure, only that the company has basic cyber hygiene.
There are two levels of certifications:</td><td rowspan="3">ISO 27001 is the international standard for information security. It sets out the specification for an information security management system (ISMS).
The best-practice approach helps organisations manage their information security by addressing people, processes, and technology.
It does not certify that any product or service provided by the company is safe and secure, only that the company's information management aligns with some provisions of the standard. It is worth local authorities asking for which specific provisions the certificate is for and setting exact provision compliance requirements rather than broad certification.</td></tr>
<tr><th>Cyber Essentials</th><th>Cyber Essentials Plus</th></tr>
<tr><td>A verified self-assessment option which gives protection against the most common cyber attacks. It shows organisations how to implement the basics and prevent common attacks.</td><td>A hands-on technical audit takes place by a third-party assessor, ensuring that all Cyber Essentials controls have been implemented correctly and are operating effectively.</td></tr>
</table>

Management

Management

You’ve successfully procured a secure solution for your connected places project and must now manage the supplier(s) throughout the project lifecycle.

Engagement

Early engagement with the supply market allows the authority to understand the available solutions and prepare the market with the authority’s expectations.

Requirements

Developing strong requirements, particularly on cyber security, will help ensure that you procure the right solution but also reduces incorrect interpretation by suppliers.

Procurement

Asking the right questions in procurement stages, and evaluating responses appropriately, helps to ensure that authorities procure the right solution.

Management

Cyber security must be fully considered when designing and building solutions. Continuous improvement through contract management is critical to good cyber security.

End-of-life

Being clear on what will happen to solutions once they reach their end-of-life will ensure that hardware, software, and data is securely managed and disposed of.

Micro-Businesses and SMEs

Connected places technology and expertise is often procured from micro, small and medium-sized enterprises (SMEs). This has several benefits including agility, innovation and in supporting the local economy.

Working with these businesses may come with additional considerations for which it is important to have a plan in place for:

- They are more likely than large and established businesses to go out of business, and this can happen suddenly.
- They may be acquired by larger and established businesses either wholly or in parts.
- Key staff may leave which can have an outweighed impact on their ability to deliver.
- They may pivot their business to a new area and stop supporting the solution procured.

This does not mean you should not work with these businesses, they must be fairly included and considered in any procurement.

Network Services 3 Framework

With CCS being the biggest public procurement organisation in the UK, they have a tailored free to use framework called Network Services 3.

- ✓ This framework and specifically lot 3a has been crafted to enable the procurement of complete IOT and connected spaces solutions.
- ✓ The Framework complies with public procurement regulations and gives you access to 26 vetted suppliers who are leaders in their respective capabilities.
- ✓ Suppliers are required to comply with key security principles when providing a solution and meet the NCSC standards pertaining to security standards and practices.
- ✓ As a Buyer you would have access to competitive large scale enterprise pricing.

Details of this framework can be found at https://www.crowncommercial.gov.uk/agreements/RM6116 Alternatively you can contact the team directly at info@crowncommercial.gov.uk who will be happy to discuss your requirements further with you.

End-of-life

End-of-life

All projects come to an end, but it is often an area that is not carefully considered and well contracted for. It is important that everyone knows what will happen once a connected places project finishes.

Engagement

Early engagement with the supply market allows the authority to understand the available solutions and prepare the market with the authority's expectations.

Requirements

Developing strong requirements, particularly on cyber security, will help ensure that you procure the right solution but also reduces incorrect interpretation by suppliers.

Procurement

Asking the right questions in procurement stages, and evaluating responses appropriately, helps to ensure that authorities procure the right solution.

Management

Cyber security must be fully considered when designing and building solutions. Continuous improvement through contract management is critical to good cyber security.

End-of-life

Being clear on what will happen to solutions once they reach their end-of-life will ensure that hardware, software, and data is securely managed and disposed of.

End-of-life

Connected places projects tend to be long-term, potentially decades in length. This means that the end-of-life considerations are often not thought through in much detail, with the potential to leave gaps in the cyber security of the project.

There are several reasons why a project may reach end-of-life:

- The system or components reach their expected lifespan or become obsolete.
- The system or key components stop working and repair costs cannot be justified.
- It is no longer wanted or needed by the users.
- Components can no longer receive critical updates and patches.

Depending on the reason and other factors the authority could:

- Repair or upgrade the system or components of.
- Re-use or repurpose components.
- Return components to the manufacturer or service provider.
- Securely and environmentally dispose of components.

This should be incorporated into contractual terms appropriate for your specific project.

Keeping end-of-life components connected to networks poses a significant cyber security risk and they must be removed as a matter of urgency.

End of life policy

Local Authorities may also find it beneficial to develop an internal end-of-life policy which can provide consistency across connected places projects. This should include elements such as:

- ✓ Establishing clear and transparent end-of-life criteria and timelines for projects, systems, and components. These should be clearly communicated to stakeholders.
- ✓ Providing regular and timely updates and notifications to relevant stakeholders about the end-of-life status, the implications, and options for managing this.
- ✓ Offering incentives and options for stakeholders to upgrade or replace their end-of-life systems or components, with newer models that offer improved security, compatibility, functionality, sustainability. These could include discounts, trade-ins, buybacks, or subscription models.
- ✓ Implementing proper disposal methods that comply with regulations, policies and standards for cyber security and privacy, as well as environment disposal of e-waste.

Summary and next steps

Procurement & supply chain: summary and next steps

1

Key take aways

Cyber security must be considered at all stages in procurement and supply chain management.

Set expectations with suppliers as early as possible.

Crown Commercial frameworks can provide an efficient way to procure but be aware of what they do and don't do.

Ensure the end-of-life considerations are included from the start.

2

Questions to ask

Have the right people internally been consulted?

Are my requirements clear, realistic and prioritised?

Have I engaged the potential supplier market to understand the art of the possible, and to set expectations?

Am I clear on how the contract(s) will be managed and what happens at end-of-life?

3

Next steps

Review internal policies and processes, to identify gaps and align with relevant aspects of this resource.

Develop a list of internal specialists who can support connected places procurements.

Engage Crown Commercial Services and build a working relationship with relevant teams.

Appendix

Example implementation

Case study: Dorset Council

Dorset Council

Need:

Dorset Council has well-functioning and mature procurement and supply chain management. However, there is limited availability across their specialist technical resource. The council identified a need to upskill non-procurement colleagues and raise the profile of cyber security considerations when procuring connected places systems.

They also recognised that their current practices for connected places end-of-life planning were limited. For example: whether the hardware is retained versus removed and how this is done, or the retention period and destruction policy for legacy data that may persist on a system after technology products have been decommissioned.

Solution:

Using this resource, Dorset Council plans to implement a minimum-security requirement across all new connected places procurements, taking the suggested security questions as a baseline and adjusting for their local context and risk appetite.

They also plan to use this end-of-life guidance to tighten processes and policies to ensure that it is clear what should happen and who is responsible for end-of-life management.

Outcome:

Dorset Council has used the guidance in this resource to effectively review their existing procurement, supply chain and end-of-life management. Through this, they have gained a renewed appreciation for their internal expertise and processes and have identified ways to enhance them. One such method is forensic accounting to identify uncontrolled potentially insecure procurements.

In the future, as a result of learnings from their involvement in the Secure Connected Places Playbook, Dorset Council will be better placed to apply a well-informed, contemporary, effective and proportionate cyber security response to all connected places proof of concepts, pilots and projects.

Example implementation

Case study: City of Bradford Metropolitan District Council

City of
BRADFORD
METROPOLITAN DISTRICT COUNCIL

Use case(s):

Environmental management, community safety

Need:

When Bradford Council started its connected places journey, they found little guidance beyond the NCSC Connected Places Cyber Security Principles. Instead, they undertook security risk assessments based on good practice around hardware, applications and systems. Bradford Council have since enhanced their connectivity through their own network. However, there was a fly tipping problem in their rural areas. Nitrous Oxide was also being used increasingly in the area and it could be weeks before the Council knew what had happened in an area due to the lack of connectivity. Therefore, Bradford Council ran a project using the resources where they could enhance the deployment of their project to create real-time images and get the appropriate authorities to the scene in time to catch the offenders.

Solution:

Bradford Council initially used the STRIDE-based threat analysis resource to address security issues before technology deployment and agree on the security boundaries with their suppliers. More recently, Bradford Council have strengthened their questionnaire by adding more STRIDE questions to their Cloud Hosted and IoT Questionnaires. They used the Procurement and Supply Chain Management resource to enhance the deployment of their project. When they were procuring IoT cameras with Artificial Intelligence (AI) built in to help reduce fly tipping in their rural areas, they made sure they had clear roles and responsibilities from a procurement point of view and implemented a checklist to make sure they covered the various elements of procurement before agreeing the contract with suppliers.

Outcome:

Bradford Council have had no issues with the security of this project and have been able to significantly reduce their fly tipping and Nitrous Oxide in their rural areas. They are now looking to create a business case for funding to roll out their solution to the wider rural areas in line with their procurement requirements for suppliers.

Example implementation

Case study: Sheffield City Council

Use case(s):

Adult social care

Need:

Sheffield City Council are enhancing their Adult Social Care Technology Enabled Care Service to ensure it is human centric. They are looking to introduce new solutions with digital capabilities to enable the delivery of more proactive and preventative services. In line with this, the Council want to ensure these new solutions are consistently secure for citizens to use.

Solution:

By drawing upon the Supply Chain and Procurement resource, Sheffield Council have been able to discuss in more depth how they can enhance the security of smaller companies. These companies can sometimes offer more innovative services but may not always be aware of the expectations of councils in terms of the security certifications and accreditation required.

Outcome:

As a result, Sheffield City Council have now built in more governance processes and supply chain questions when reviewing suppliers to enhance their standard set of non-functional requirements. This has meant their approach to procuring new solutions is increasingly becoming more consistent. They will now also seek to include the other elements of the Playbook into future governance arrangements for new solutions to be deployed.

Example implementation

Case study: Tees Valley Combined Authority

TEES VALLEY COMBINED AUTHORITY

Use case(s):

Traffic Management

Need:

Tees Valley Combined Authority represent five local authorities and wanted to support them in securing and futureproofing their connected places projects. The Combined Authority rarely procures connected assets directly due to this structure, but wanted to understand if there could be any guidance that could enhance the already well-established procurement processes the local authorities had in place.

Solution:

The Combined Authority used the Cyber Security Principles 101 resource to deliver a cyber security awareness training session to their Group Procurement and Purchasing Manager which enabled them to review their current procurement processes. They also used the Procurement & Supply Chain Management resource to develop a questionnaire that took into consideration the risk appetite of the Combined Authority. The Combined Authority then engaged internally with its digital, transport, procurement and legal teams, then IT teams at its five local authorities to create supplier questionnaires that would increase cyber security confidence internally when procuring connected assets.

Outcome:

The supplier questionnaire has formed part of the wider procurement processes at Tees Valley Combined Authority and it was shared with the local authorities to assist them when procuring connected assets. They have also worked with their legal team to create a set of contract clauses including areas such as the data breaches, supplier subcontractor changes and disaster recovery and are looking to share this approach with their local authorities.

Glossary of terms

Term / acronym	Definition
Architecture	The designed structuring of something e.g. an agreed set of components for IT systems
Bug	An error, flaw or fault in the design, development or operation of a piece of software that causes it to produce incorrect or unexpected outputs
Connected places	Connected places are a community that integrates information and communication technologies and Internet of Things devices to collect and analyse data to deliver new services to the built environment, and enhance the quality of living for citizens. A connected place will use a system of sensors, networks, and applications to collect data to improve its operation, including its transportation, buildings, utilities, environment, infrastructure, and public services
Connected places security governance	Connected places security governance is the means by which an organisation can control and direct its approach to cyber security in connected places projects.
Connected technology	Products with technology built in that allow them to connect with their environment and other products, for instance, Internet of Things devices.
Cyber security	The practice of protecting computer systems from attack
DSIT	Department for Science, Innovation and Technology
Invitation to Tender (ITT)	A step in competitive tendering, in which suppliers and contractors are invited to provide offers for supply or service contracts
IoT	The Internet of Things describes physical objects with sensors, processing ability and software that connect and exchange data with other devices and systems over the Internet or other communications networks
NCSC	National Cyber Security Centre
Patching	A set of changes to a piece of software to update, fix, or improve functionality and security

Glossary of terms

Term / acronym	Definition
Personally Identifiable Information	Information that relates to an identified or identifiable person. This can be a name, phone number, IP address etc. If it is possible to identify an individual from the information then it may be personal information.
Requirement	A feature that is needed or wanted
Supply Chain	The system of people and things that are involved in getting a product from production to the buyer
System approach	A philosophy that considers a problem as the result of, or to be solved by, a system
The Principles	The NCSC's Connected Places Cyber Security Principles

NCSC Principles coverage

This key depicts where this resource draws content from the following principles of the NCSC's Connected Places Cyber Security Principles

Focus: The guidance provided in this resource will help you to understand your suppliers' role and manage your supply chain throughout your connected place's lifecycle.

Gaps: There are some gaps in the principles around understanding and designing the connected place, but there is broad coverage given the end-to-end lifecycle nature of this tool.

■ Fully aligns with the Principle

□ Does not align with the Principle

Understanding your connected place

#1 Understanding your connected place and the potential impacts	■
#2 Understanding the risks to your connected place	■
#3 Understanding cyber security governance and skills	■
#4 Understanding your suppliers' role within your connected place	■
#5 Understanding legal and regulatory requirements	■

Designing your connected place

#6 Designing your connected place architecture	■
#7 Designing your connected place to reduce exposure	■
#8 Designing your connected place to protect its data	■
#9 Designing your connected place to be resilient and scalable	■
#10 Designing your connected place monitoring	■

Managing your connected place

#11 Managing your connected place's privileges	■
#12 Managing your connected place's supply chain	■
#13 Managing your connected place throughout its life cycle	■
#14 Managing incidents and planning your response and recovery	■

Secure Connected Places Playbook
Cyber security resources for local authorities

Department for
Science, Innovation,
& Technology

Please contact secureconnectedplaces@dcms.gov.uk with any questions or feedback on these resources.

This Playbook was produced in collaboration with:

plexal DAINTTA Configured THINGS