Secure Connected Places Playbook
Cyber security resources for local authorities

Department for
Science, Innovation,
& Technology

Governance in a box

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 advises local authorities on the processes and considerations needed to set up good cyber security governance across all connected places projects, to enable the flow of cyber security information to those who need to make informed decisions.

How should I use it?

The guidance in this resource can be used to set-up new processes for connected places' cyber security governance, or to review your existing processes to ensure they are fit for purpose. The information provided throughout this resource provides recommendations and examples, however, it should be tailored to your local context.

Who does this resource apply to?

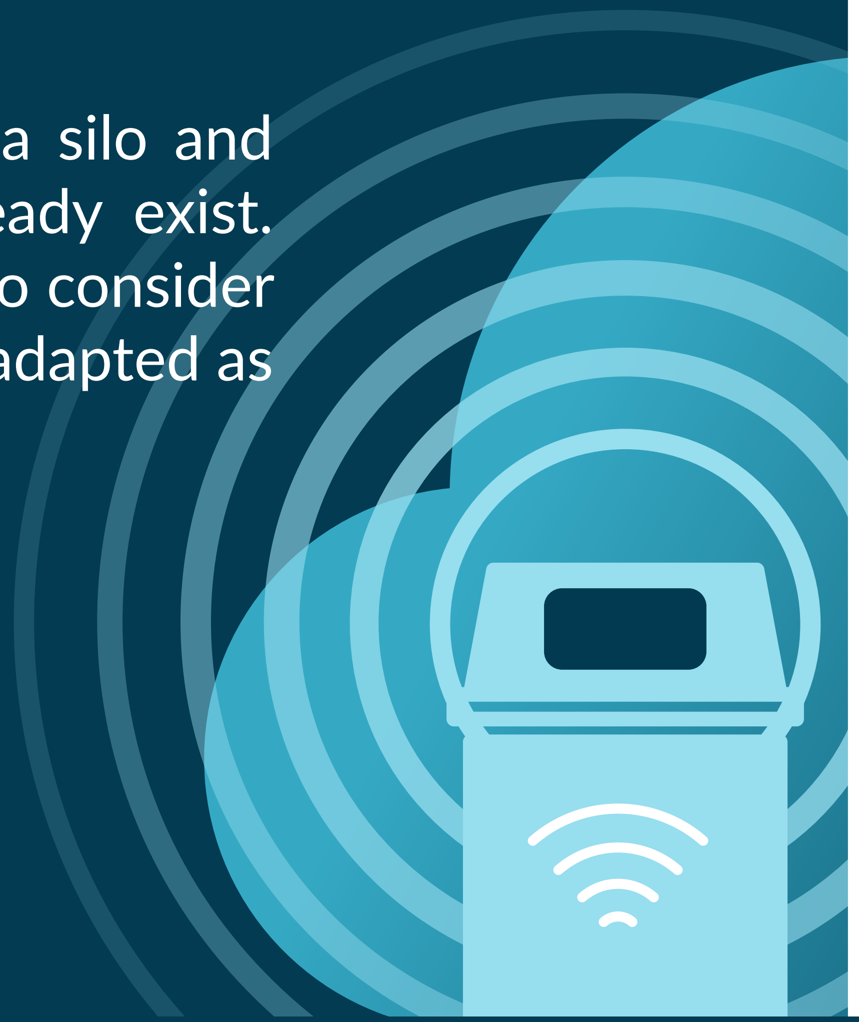
The contents of this resource apply to a broad range of stakeholders within your local authority, but much of the content is aimed towards those in programme and project management roles, plus those who have responsibility for technology and digital portfolios.

What will I get out of using this resource?

Setting up the necessary processes for effective cyber security management can be complex in the context of connected places, where there are many stakeholders in the local authority.

Without adequate process management, it can be difficult to have visibility of all connected places projects in a local authority, leading to wasted and repeated effort across projects and ineffective management of cyber risks.

Connected places cyber security should not sit in a silo and should not duplicate efforts where structures already exist. Rather than creating new processes, it is important to consider existing governance structures to see if they can be adapted as per the guidance in this resource.



Case study: Merthyr Tydfil County Borough Council

MERTHYR TYDFIL
County Borough Council
Cyngor Bwrdeistref Sirol
MERTHYR TUDFUL

Merthyr Tydfil County Borough Council's connected places projects were lacking involvement with Corporate Risk Management, meaning not all connected places projects were captured and monitored. They are now using the Connected Places Security Steering Group (CPSSG) Terms of Reference attached to this governance resource to involve their Governance Group in connected places projects and ensure that their staff know how to appropriately manage connected places risks.

Case study: Perth & Kinross Council

PERTH & KINROSS COUNCIL

Perth & Kinross Council have an established digital board chaired by the council's chief digital officer. After working with this resource, they are now taking the issue of connected places cyber security strategically through the Digital Board and at the operational level in terms of the implementation of Internet of Things (IoT) projects.

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

Contents

Introduction to connected places cyber security governance

Why do we need governance?

Every local authority has to make decisions and manage risk. In this context, this relates to the cyber security risks associated with connected places projects. Managing these risks is always a trade-off in how much time and money is spent in reducing the risk to an acceptable level.

To successfully manage risk, we must make informed decisions.

Having appropriate governance structures, processes and culture in place is the best way to share information with those who are empowered to make these risk management decisions. This requires coordination and integration of connected places projects.

What is connected places cyber governance?

It is how the organisation controls, directs and coordinates its approach to cyber security in connected places projects.

It should integrate and align with the organisation's wider cyber security and risk governance approach.

It sets out the organisation's approach to cyber security decision-making for connected places projects.

It should clearly articulate the organisation's risk appetite with regard to connected places, as well as what cyber security risk decisions staff at all levels within a connected places project can take.

There is no single correct answer to governance

There is **no single correct answer** to connected places cyber security governance. The approach that is taken will depend on a number of factors and should be tailored to your local context.

- Size and complexity of the organisation
- People and budget available
- Exact project(s) and their cyber security risk
- Legal and regulatory considerations
- Existing processes and structures within the organisation

Projects with small budgets may have low financial risk but could still have significant cyber risk.

What does good governance look like?

For further support on how you can ensure security is considered holistically within the context of connected places, please refer to BSI specification PAS 185. PAS 185 was commissioned by the Centre for the Protection of National Infrastructure (CPNI) and covers the specification for establishing and implementing a security-minded approach for smart cities (aka connected places).

While the exact implementation will differ, there are key aspects of good connected places cyber security governance.

Good governance should:

- ✓ **Identify the roles (and the individual(s)) at all levels in the organisation,** who are responsible for making security decisions related to connected places. Some of these roles may be outside of the connected places team remit.
- ✓ Ensure there is **accountability for these roles to make effective decisions** in a timely manner.
- ✓ Ensure **decision makers are empowered** in their role.
- ✓ Ensure **security decisions link to the connected places objectives** and the wider organisational objectives.
- ✓ **Integrate fully with existing governance approaches** across the organisation, including non-security governance such as finance. **Connected places cyber security governance must not sit in a silo.**
- ✓ Provide a holistic view of risk across all projects to the programme/portfolio level.

Creating a cyber security aware culture is the best way to build sustainable governance.

Creating a good cyber security culture

A cyber security aware culture is essential in significantly reducing the risk of cyber incidents and data breaches by ensuring that all staff are knowledgeable, vigilant, and proactive.

Key strategies to build this culture include:

Leadership Engagement:

Secure strong commitment from senior leadership to drive a security-first culture.

Continuous Learning:

Implement regular, engaging cyber security training for all employees, covering essential practices and threat awareness.

Clear Policies and Tools:

Develop accessible cyber security policies and procedures and provide necessary tools and training for their effective use.

Open Reporting Culture:

Establish easy-to-use mechanisms for reporting security incidents, promoting a responsible and proactive approach among staff.

Regular Assessments and Recognition:

Conduct frequent security assessments and reward compliance and proactive security behaviours to reinforce the culture.

Cultural change management

Implementing large scale cultural change is complex and can be challenging. Local authorities may wish to make use of one of several commonly used culture and business change methodologies available, each of which will have pros and cons and will be applicable in different contexts.

Local authorities should consult any existing business change teams within their organisation before doing this for connected places cyber security to avoid conflicting approaches and duplicated effort. Some methodologies may also require official licensing and training to use formally.

Some commonly used methodologies include, but are not limited to:

1. Lewin 3 Step Change Model
2. ADKAR
3. McKinsey 7-S Model
4. Kotter's Change Management Theory

It is recommended that local authorities wishing to implement culture and business change should research the methodology most appropriate to their needs. They may wish to also seek specialist advice.

Architectural options

Architecturally, Connected Places, can grow organically, piece by piece with little or no design specified by the authority. Alternatively, they can grow in a more co-ordinated fashion, where interfaces between suppliers and authority are well designed and documented, with design authority retained by the local authority or a systems integrator.

Whilst the organic approach may allow one to get started quickly and seemingly for a low budget, each of these deployments becomes its own island of data and security approaches. These approaches are typically specified by the supplier. Whilst this may support less mature operations it leads to highly siloed ways of working.

The co-ordinated approach has a higher upfront design cost and typically each deployment will carry higher integration costs with more discussion required during procurement, however it enables authority-wide data and security standards for integration and reuse across lines of business.

Architectural options

Type	Upfront cost	Ongoing cost	Cost to reuse	Alignment to corporate standards	Interface Owner	Typical interfaces
Organic	▼	▼	▲	▼	Supplier	Regular reports, Supplier defined APIs
Co-ordinated	▲	▲	▼	▲	Authority	Authority APIs to which suppliers integrate

API – Application Programming Interface

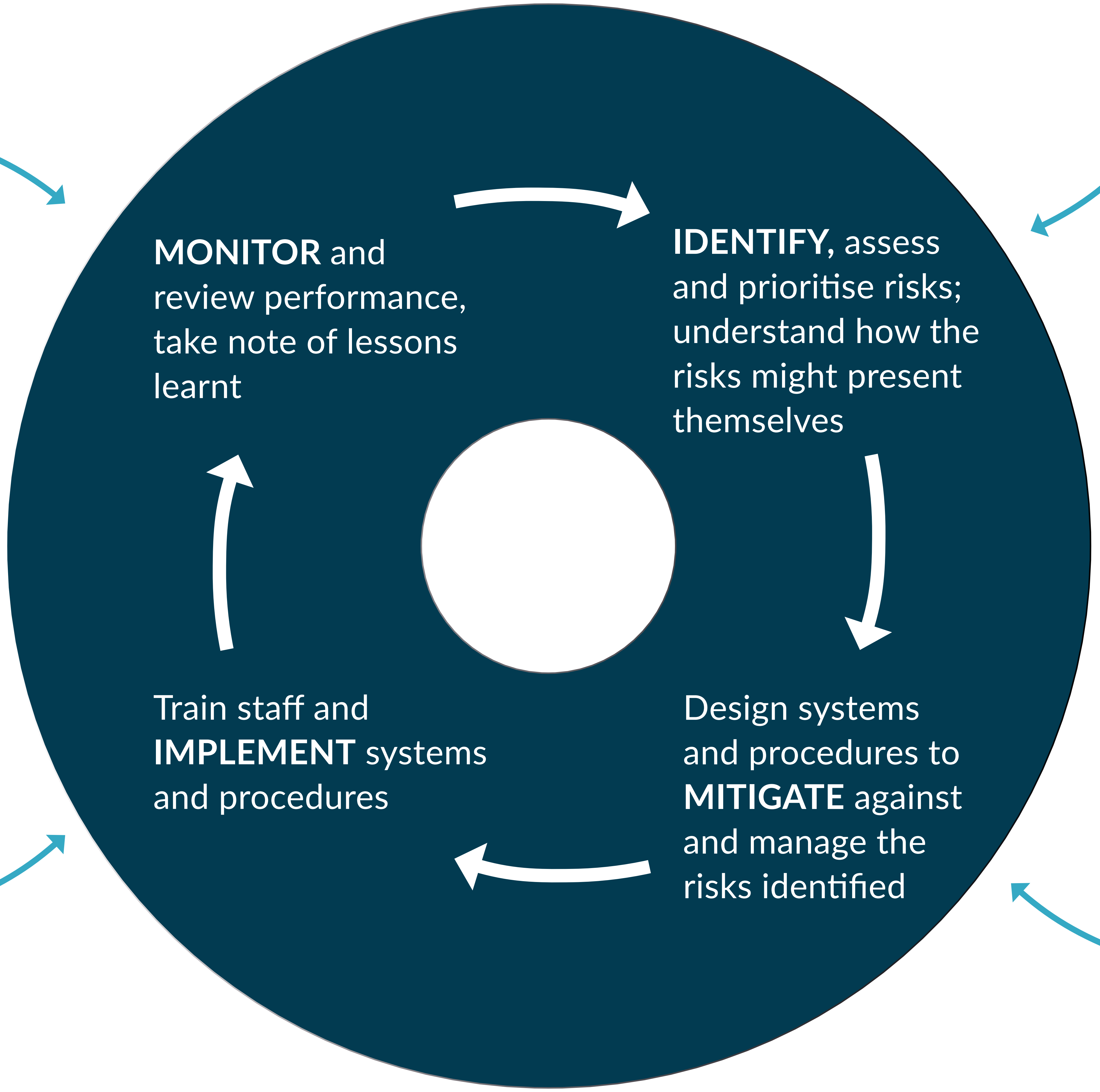
Appropriate risk management and treatment is a key first step in cyber security governance.

Without properly identifying and escalating risks in connected places projects there is no way for people to make the necessary decisions to reduce the risk exposure of the local authority.

While many risks are identified at a project level, they may be escalated and managed at a programme, portfolio or even corporate level where they may need to be included on the corporate risk register.

Having a view of risk across a connected places portfolio is important given the interconnected nature of these projects.

A continuous approach to risk management



Review and consider feedback from all stakeholders

MONITOR and review performance, take note of lessons learnt

IDENTIFY, assess and prioritise risks; understand how the risks might present themselves

Risk assess any new areas of work or projects as they come

Design systems and procedures to **MITIGATE** against and manage the risks identified

Consider input from ‘critical friends’ or other similar organisations’ risk assessments

Train staff and **IMPLEMENT** systems and procedures

Involving staff in the process makes the risk assessment more likely to succeed

Diagram informed by The Charity Commission’s risk assessment cycle – see here.

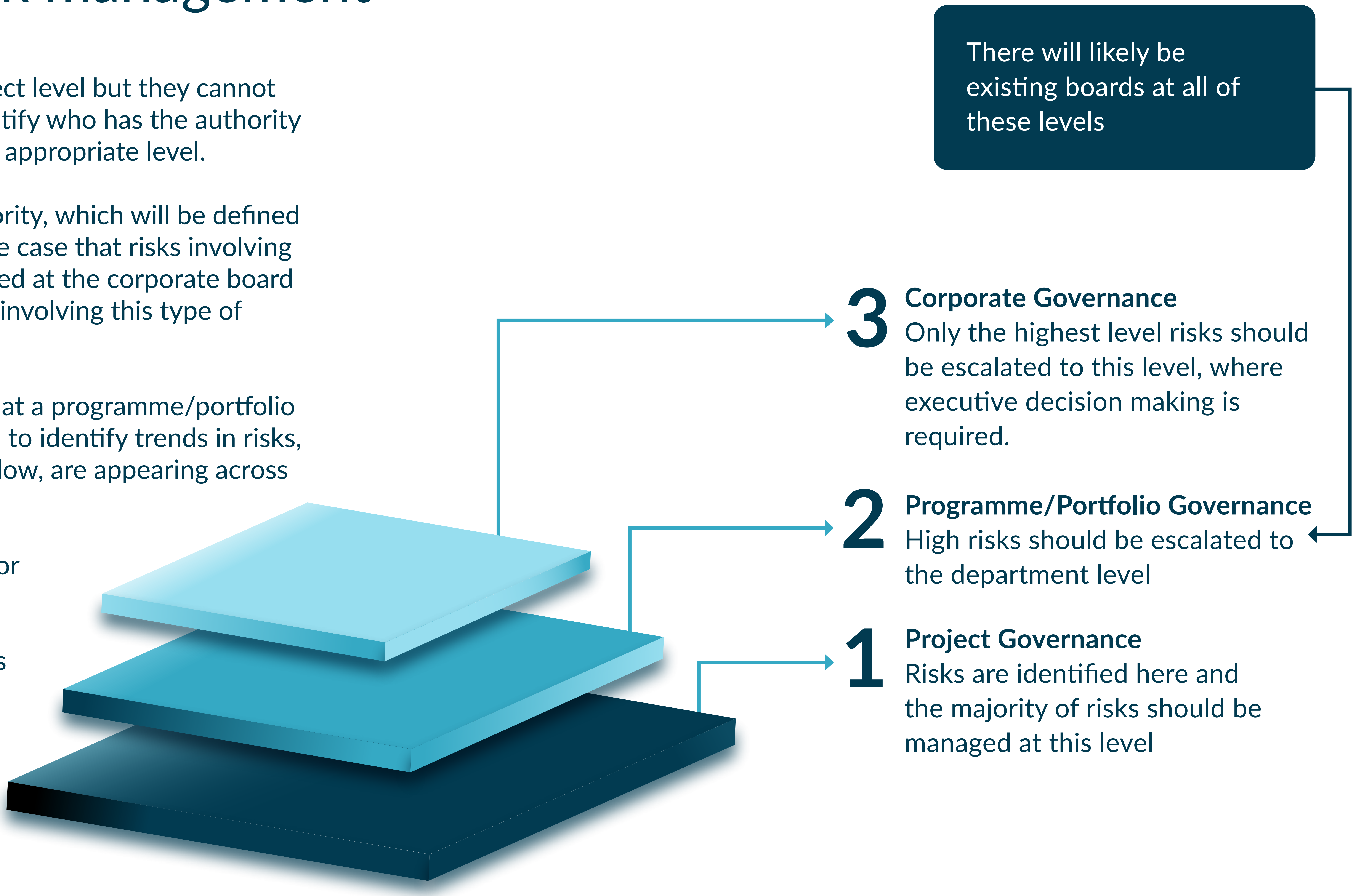
A layered approach to risk management

Risks from connected places are identified at the project level but they cannot always be managed at this level. It is important to identify who has the authority to appropriately manage the risk and escalate it to the appropriate level.

This will depend on the risk appetite of the local authority, which will be defined at the whole authority level. For example, it may be the case that risks involving personally identifiable information needs to be managed at the corporate board level, given the potentially high costs of a data breach involving this type of information.

Local authorities may wish to have visibility of all risks at a programme/portfolio level to give a holistic view of risks across projects and to identify trends in risks, for instance if certain risks, although potentially rated low, are appearing across multiple projects.

As part of creating a cyber security aware culture senior leaders should ensure that projects consider cyber security risks. They may be able to do this through, for example, requesting to see cyber security specific risks at project reviews, gates and other sign-offs.



There will likely be existing boards at all of these levels

3 **Corporate Governance**
Only the highest level risks should be escalated to this level, where executive decision making is required.

2 **Programme/Portfolio Governance**
High risks should be escalated to the department level

1 **Project Governance**
Risks are identified here and the majority of risks should be managed at this level

Risk treatment

Once risks have been identified with a designated owner and escalated to the appropriate level, they can be treated effectively. Risks would typically be treated at a project level but the programme/portfolio level should be aware of risk treatments to have a holistic view across all connected places projects.

There are four ways of treating risk

Accept

Accept the risk and the consequences of it being actualised.

Risks may only be reduced and not brought to zero, therefore it is important to understand the residual risk and whether a combined treatment plan may be required.

Avoid

Avoid the activity that leads to the risk.

If the activity is deemed too risky, and there are no other mitigations that suitably reduce the risk, a decision may be made to avoid that activity.
If this is the case, you should consider the other non-cyber security risks of avoiding that activity.

Mitigate

Implement a change to the system (be that people, process or technology) that reduces the likelihood and impact of the risk.

It is important to consider your resilience needs should a risk materialise even after treatment.

Transfer

Accept accountability for the risk but shift the financial consequences to a third party through an insurance policy or outsourcing the process.

This transfers the financial impact of the risk, not the accountability or the likelihood of it happening.

Risk treatment plans

Before deciding on a particular treatment plan for risk, it is important to **weigh up the trade-offs** of doing so.

Whilst mitigating particular threats may improve the cyber security of connected places, the costs of doing so may include:

- **Financial outlay**
- **Reduction in system usability and user experience**
- **Encouragement of workarounds**

Additionally, transferring the risk does not absolve the organisation of accountability – were the risk to be realised, it may still have a reputational cost and consequential losses.

Connected places are systems problems and require a whole system approach to secure, which means all parts must be considered together and not in silos. For example, securing a sensor without securing the network it connects to will not reduce the overall cyber security risk of that connected place.

Risk treatment should **not be a static decision** made at a single point in time. Risk registers are living documents; threats and adversarial capability change constantly and therefore probabilities, impacts and residual risks also change. Treatment plans and their impact on the **risk register should also be reassessed regularly**, the frequency of which will depend on the project itself, but typically a quarterly review is appropriate.

It might be that to get a project started the organisation accepts the risk of doing so and sanctions an exception from standard policy and processes to accommodate. However, it is important that in such cases the ongoing project changes are understood and that there is a process/roadmap to realign the project with “business as usual” policies and processes.

One of the common areas of cyber security risk in connected places is **data protection and privacy**.

In connected places projects there may be unique risks that do not typically appear in other local authority projects and require specialist treatment.

Privacy for connected places

Whilst many data protection requirements for connected places are similar to those in other areas for local authorities, certain nuances should be appreciated when designing connected places. This is especially true when performing their Data Protection Impact Assessments (DPIAs) for connected places and considering how these risks are managed.

Due to the nature of **data being aggregated** across connected places (even when data may initially seem anonymous and benign) when it is correlated and enriched with other datasets, it may become personally identifiable and worthy of increased scrutiny.

Connected places projects tend to evolve over time and therefore the collection, processing, storage and sharing of data are also likely to change. **DPIAs should be regularly revisited** to ensure data protection treatments effectively manage the risk.

Detailed guidance on DPIAs can be found from the ICO

The effective identification and management of cyber security risks in connected places projects requires specific skillsets and roles in the local authority.

Without defined roles, the job of identifying and managing cyber risks becomes nobody's job and may not be done at all.

Role definitions

Many of the roles required to implement good cyber security governance in connected places will likely already be in place within your local authority, and may already be familiar to project teams, for example: project managers, IT managers, data protection officers, risk managers, procurement managers and chief information security officers etc.

However, there are some roles (particularly those involved in designing and developing connected places projects) without which it is difficult for these managers to be informed on the true extent of cyber security risks and the details of potential mitigations.

Some of these roles are defined on the following pages. **Local authorities should focus on the responsibilities of each role. Every local authority is unique, so these responsibilities may be performed by individuals with varying job titles, who may also have additional responsibilities, or be spread across multiple individuals.**

Please review the procurement and supply chain management resource for further support.

It is possible that the responsibilities described could be performed by suppliers for your connected places projects. In this case, the responsibilities should be clearly set out and expectations understood by all. Though it should be noted that accountability for the cyber security of your connected place cannot be outsourced to suppliers.

Typically, a connected places project manager might need to identify who in the organisation has the responsibilities described in the role descriptions that follow.

Role definitions **Technical/Data Architect**

Purpose:

Technical/data architects provide technical leadership and architectural design – taking business problems and translating them into technical designs, architectures and models – working collaboratively with other architects such as security and enterprise architects.

Responsibilities:

- Be responsible for leading the technical design of systems and services, justifying and communicating design decisions.
- Assure other services and system quality, ensuring the technical work fits into the broader strategy for the authority.
- Provide leadership to and collaborate with other architects.
- Communicate with senior stakeholders across organisations.
- Support multiple teams, finding and using best practices and emerging technologies.
- Solving complex and high-risk issues or delivering architecture design.

Role in cyber governance:

The technical/data architects should identify cyber security risks in the solutions that they design, working closely with others to reduce risk and implement cyber security best practice in their solutions. They should advise the risk owners on risk impact and appropriate mitigation options.

Role definitions
Enterprise Architect

Purpose:

Enterprise architects are leaders working across different levels within an organisation to translate the business strategy into business change and technical delivery.

Responsibilities:

- Identify priorities for change to enable delivery at pace.
- Own the enterprise architecture vision, strategy and roadmaps from a business, technology and data perspective, including ‘as is’, ‘to be’ and transitional states.
- Understand the organisation’s ecosystem and its interdependencies, including reference architectures.
- Take a strategic view across all architectural domains, portfolios and programmes.
- Guide the organisation to make appropriate business, technology and data decisions by recommending reuse, sustainability and scalability to achieve value for money and reduce risk.
- Establish architectural principles, policies and standards.
- Carry out horizon scanning across the industry, identifying emerging trends and their potential impact and opportunity for the organisation.

Role in cyber governance:

The enterprise architect should identify cyber security risks at an architectural level, across business, technology and data perspectives, and advise the risk owner(s) on risk impact and appropriate mitigation options.

Role definitions
Security Architect

Purpose:

A security architect creates and designs security for a system or service, maintains security documentation and develops architecture patterns and security approaches to new technologies.

Responsibilities:

- Recommend security controls and identify solutions that support a business objective.
- Provide specialist advice and recommend approaches across teams and various stakeholders.
- Communicate widely with other stakeholders.
- Advise on important security related technologies and assess the risk associated with proposed changes.
- Inspire and influence others to execute security principles.
- Help review other people's work.

Role in cyber governance:

The security architect should identify cyber security risks at a system level and advise the risk owner(s) on risk impact and appropriate mitigation options. A security architect would not typically own cyber risks but should enable informed risk based decisions.

Role definitions
Procurement Officer

Purpose:

A procurement officer is responsible for supporting and enabling teams to procure the best solution cost-effectively, ensuring that this is done legally and ethically following all relevant policies and procedures.

Responsibilities:

- Recommend appropriate options for procurement routes, such as central frameworks.
- Provide specialist advice on procurement policies and procedures.
- Support teams with supplier engagement, being the commercial/procurement point of contact.
- Provide advice and guidance on the non-technical aspects of technology procurements.
- Support with assessing received proposals.

Role in cyber governance:

The procurement officer should ensure that connected places projects follow appropriate internal and external policies and procedures. This should include notifying the appropriate team(s) within the authority e.g. the IT Security team, and ensuring that appropriate cyber security aspects are included throughout the procurement.

Please review the procurement and supply chain management resource for further support.

Role definitions **Data Protection Officer**

Purpose:

A Data Protection Officer (DPO) is responsible for ensuring that data in the authority is protected and that work conducted by the authority complies with legislation, such as UK GDPR. They are the main point of contact in the authority for issues related to data protection within connected places projects.

Responsibilities:

- Draft new, and amend existing, internal data protection policies, guidelines, and procedures, in consultation with key stakeholders.
- Deliver training across all business units to staff members who are involved in data handling or processing.
- Conduct audits to ensure compliance and address potential issues.
- Maintain records of all data processing activities of the company.
- Serve as point of contact for data protection.

Role in cyber governance:

The DPO should advise those involved in designing and managing connected places projects on the risks associated with the processing of data, and ensure that projects comply with local data protection policies and processes.

It is recognised that local authorities must, by UK GDPR law, already have a DPO in place, and so this description refers to suggested responsibilities for connected places.

Role definitions
Security Operations Manager

Purpose:

A security operations manager is responsible for the day-to-day management of the cyber security of connected places projects, including identifying new threats and assisting in implementing mitigations for these. Some local authorities may have an existing Security Operations Centre (SOC) where this role may already exist.

Responsibilities:

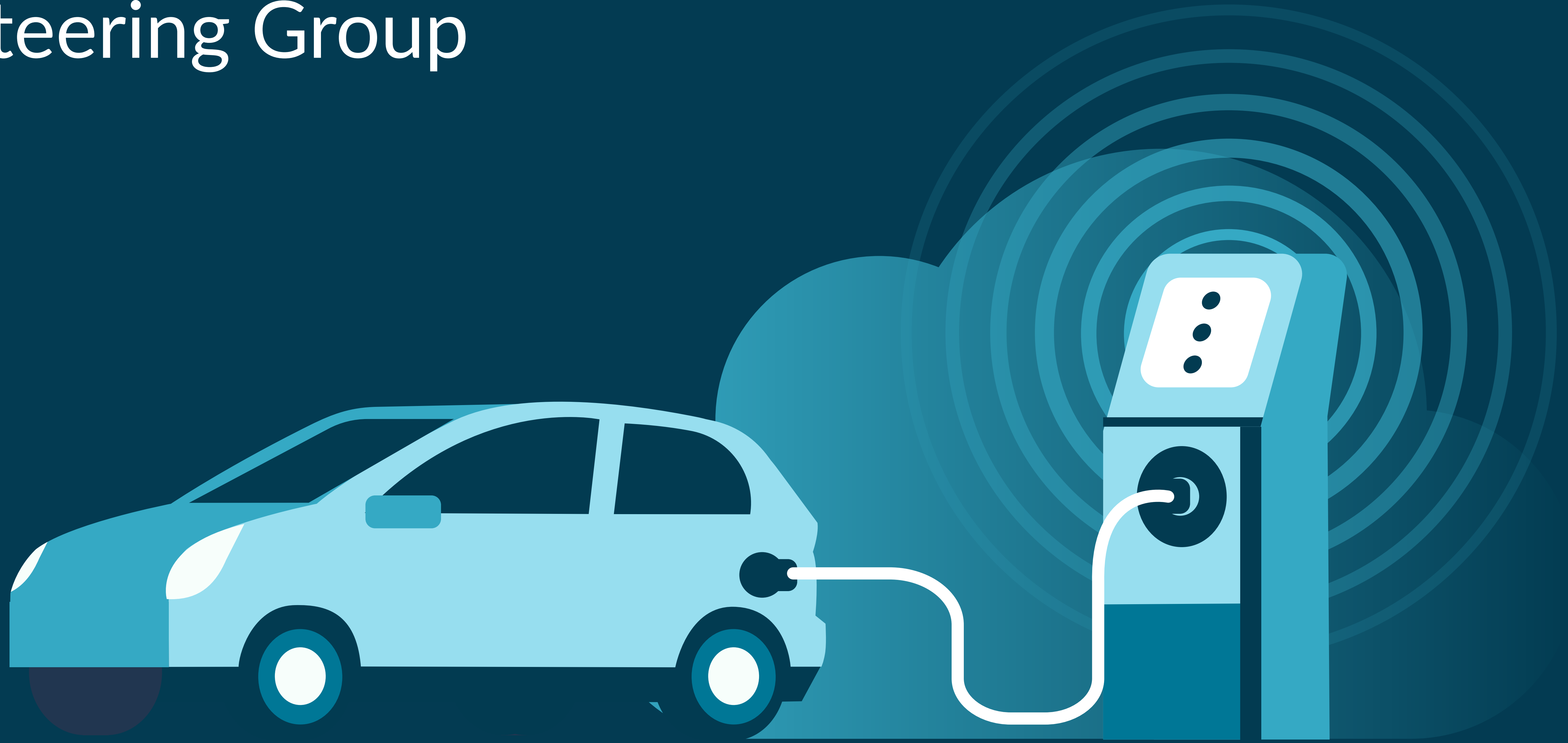
- Monitoring and analysis of incidents to protect people, technology and process addressing all security incidents and ensuring timely escalation.
- Identify and assess potential threats delivering strategies to minimise the impact of the threat.
- Directing security event monitoring, management and response and cyber intelligence.
- Ensuring incident identification, assessment, quantification, reporting, communication, mitigation and monitoring.
- Ensuring compliance with policy, process, and procedure.
- Revising and developing processes to strengthen the current security operations.
- Co-ordination with stakeholders.

Role in cyber governance:

The security operations manager should identify new risks to in-flight connected places projects, inform risk owners of these, and work with others – such as architects and developers – to identify and implement mitigations.

A good way of identifying risks, sharing knowledge, providing consistent advice to risk owners and managing risk at a programme level is through a group or board.

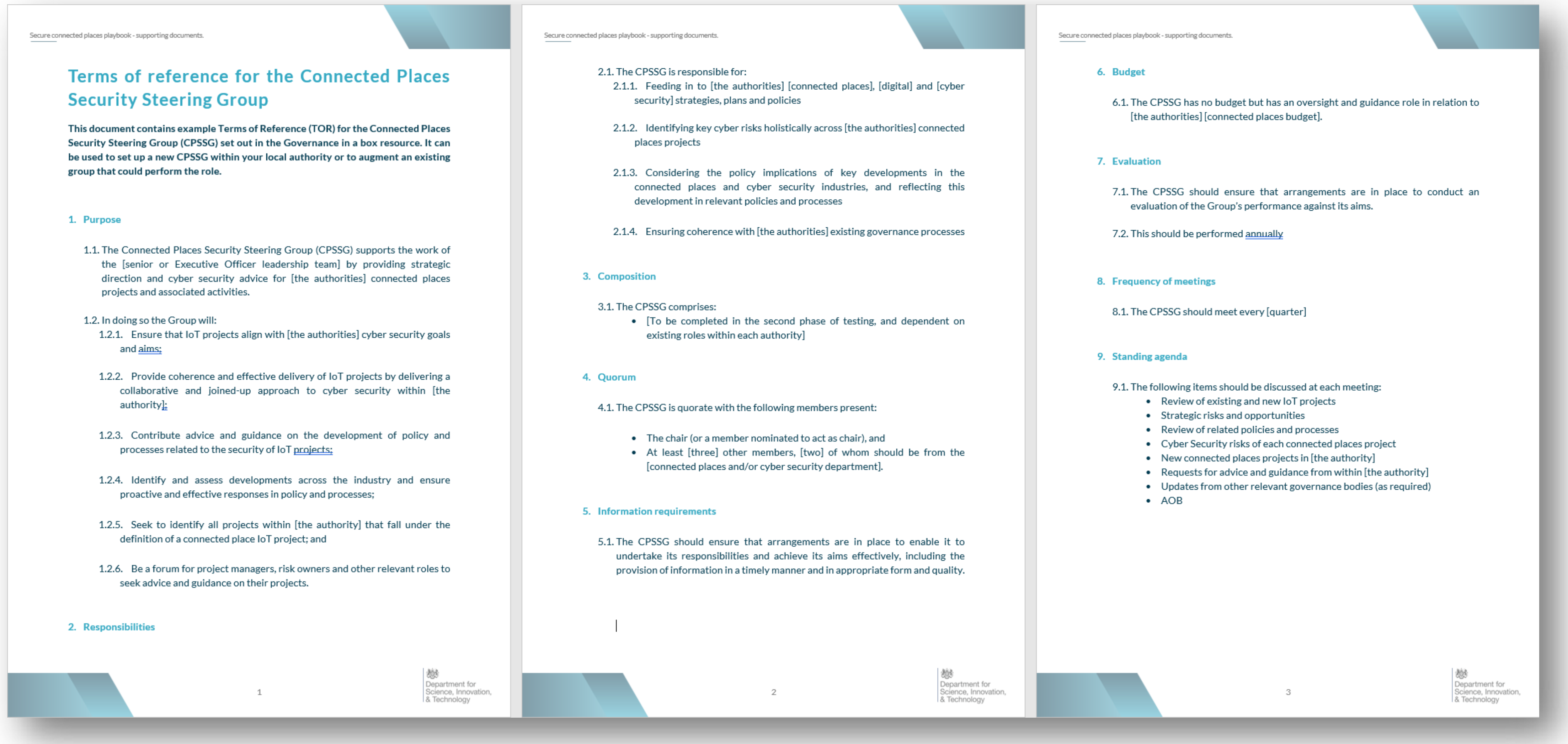
A Connected Places Security Steering Group (CPSSG) is one option for this.



Terms of reference

Example terms of reference are provided as a supporting document to the playbook.

The example provided in this supporting document is a template and can be merged into existing terms of reference for existing groups and boards that perform a similar function.



Terms of reference for the Connected Places Security Steering Group

This document contains example Terms of Reference (TOR) for the Connected Places Security Steering Group (CPSSG) set out in the Governance in a box resource. It can be used to set up a new CPSSG within your local authority or to augment an existing group that could perform the role.

1. Purpose

1.1. The Connected Places Security Steering Group (CPSSG) supports the work of the [senior or Executive Officer leadership team] by providing strategic direction and cyber security advice for [the authorities] connected places projects and associated activities.

1.2. In doing so the Group will:

1.2.1. Ensure that IoT projects align with [the authorities] cyber security goals and aims;

1.2.2. Provide coherence and effective delivery of IoT projects by delivering a collaborative and joined-up approach to cyber security within [the authority];

1.2.3. Contribute advice and guidance on the development of policy and processes related to the security of IoT projects;

1.2.4. Identify and assess developments across the industry and ensure proactive and effective responses in policy and processes;

1.2.5. Seek to identify all projects within [the authority] that fall under the definition of a connected place IoT project; and

1.2.6. Be a forum for project managers, risk owners and other relevant roles to seek advice and guidance on their projects.

2. Responsibilities

2.1. The CPSSG is responsible for:

2.1.1. Feeding in to [the authorities] [connected places], [digital] and [cyber security] strategies, plans and policies

2.1.2. Identifying key cyber risks holistically across [the authorities] connected places projects

2.1.3. Considering the policy implications of key developments in the connected places and cyber security industries, and reflecting this development in relevant policies and processes

2.1.4. Ensuring coherence with [the authorities] existing governance processes

3. Composition

3.1. The CPSSG comprises:

- [To be completed in the second phase of testing, and dependent on existing roles within each authority]

4. Quorum

4.1. The CPSSG is quorate with the following members present:

- The chair (or a member nominated to act as chair), and
- At least [three] other members, [two] of whom should be from the [connected places and/or cyber security department].

5. Information requirements

5.1. The CPSSG should ensure that arrangements are in place to enable it to undertake its responsibilities and achieve its aims effectively, including the provision of information in a timely manner and in appropriate form and quality.

6. Budget

6.1. The CPSSG has no budget but has an oversight and guidance role in relation to [the authorities] [connected places budget].

7. Evaluation

7.1. The CPSSG should ensure that arrangements are in place to conduct an evaluation of the Group's performance against its aims.

7.2. This should be performed annually

8. Frequency of meetings

8.1. The CPSSG should meet every [quarter]

9. Standing agenda

9.1. The following items should be discussed at each meeting:

- Review of existing and new IoT projects
- Strategic risks and opportunities
- Review of related policies and processes
- Cyber Security risks of each connected places project
- New connected places projects in [the authority]
- Requests for advice and guidance from within [the authority]
- Updates from other relevant governance bodies (as required)
- AOB

What is a CPSSG and why do we need one?

A Connected Places Security Steering Group (CPSSG) brings together specialist skills and expertise from within the organisation, and potentially externally, to steer connected places projects towards a clear cyber security goal and keep projects in scope and on-plan to deliver the outcomes the authority needs in a secure way.

The CPSSG should be:

1. A forum for decision making and acting across all connected places projects within the local authority.
2. Collaborative with representation from across the authority and relevant external players.
3. Have a diverse representation from across local authority departments, but only the minimum number of necessary people.
4. Held at regular intervals with a consistent agenda, aligned to the goals of the authority and pace of connected places projects. It is recommended that this should take place quarterly, but ultimately should align to the existing meeting cycle within a local authority (e.g. if all other boards meet monthly, then this should too).
5. Align with existing governance processes, including any existing boards within the local authority.

By bringing together expertise and lived experience, the CPSSG can ensure that connected places projects have the right support and momentum throughout their lifecycle and can meet the cyber security aims of the authority, while still delivering the value needed.

Where existing governance groups exist that provide a similar function to the described CPSSG, for example, a Digital Board, it may be more appropriate to integrate the two together into a single group rather than duplicate effort.

The example ToRs in this resource can be used to supplement any existing ToRs, ensuring that relevant connected places items are discussed.

Connected places project visibility

One of the CPSSG's aims should be to identify and monitor all the projects within the authority that come under the definition of connected places. There are several methods to do this:

Method	Description	Pros	Cons
Commission document	Issue a request across the organisation to declare any connected places projects that exist or are planned, and identify those that may not be immediately recognised as a connected places project.	• Spreads workload across the organisation • Simple and cost effective • Easy to replicate	• Relies on input and self-assessment from others • Not real-time, projects may be identified only after they have started • Needs to be conducted regularly
Cultural change management	If willing to invest upfront to develop a culture where motivations are aligned and the organisation's needs are widely understood, then organisations can rely on people to do the right thing from the start. A strong cyber security culture should view this as an enabler, not a blocker or forcing unnecessary processes. Commonly used frameworks to manage this process are provided on page 28.	• Once implemented well it can be transformational • Long term benefit	• Potentially requires significant upfront business and culture change project(s) • Typically requires specialist skills to implement • May not yield short term results • Should be conducted in parallel to other methods to deliver short term results
Forensic accounting	Review projects that spend within given thresholds with certain suppliers, to identify potential connected places procurements. Depending on the scale of the underreporting and whether individuals repeat this behaviour, this may need only be a one-off act, otherwise should be conducted annually at a minimum.	• Provides a comprehensive view of projects that have gone through a procurement	• Time-consuming • Connected places projects are only identified once they have started • Needs to be conducted regularly • Is passive and doesn't support the development of a strong cyber security culture
Network analysis	Monitor authority network traffic and detect connected places traffic and assets such as sensors.	• Once implemented can be a long-term and automated solution • Can potentially improve cyber security in other ways such as monitoring abnormal behaviour	• Requires specialist technical skills to implement • Only works if connected places are connected to the authority network

Example commission document

This is an example commission document that the relevant team e.g. IT or Connected Places team, can send out to relevant other teams within the local authority to understand the extent of current and planned projects. If you would like an editable version of this, please contact DSIT's Secure Connected Places team.

This form is intended to gather information from across [authority name] in order to identify where there are existing or planned projects that make use of connected technologies (e.g. sensors, cameras, networks), so that we can appropriately identify, manage, and ultimately reduce cyber security risk across these projects.			
Project title:		**Project Manager:**	
		Start date:	
Description:		**End date:**	
		Budget:	
		Has the IT team been engaged? Please detail who	
What connected places technology does this project include? E.g. air quality sensors, footfall sensors, AI cameras		**What approvals process has the project been through?**	
Does the project include procurement activity? Please detail and name any suppliers involved		**Has a Data Protection Impact Assessment (DPIA) been completed?**	
		Next review date for DPIA:	

Summary and next steps

Governance in a box: summary and next steps

1

Key take aways

To successfully manage risk, we must make informed decisions, and good governance should provide the right information to the right people to enable their decision making.

There is no one size fits all solution, connected places governance should fit within the local context.

All risks should be identified, and logged with an owner at the right level of seniority.

A CPSSG is one method to provide consistent governance across all connected places projects.

2

Questions to ask

Are all the cyber risks in my connected places projects identified?

Do they have owners, and treatment plans?

Is there a board within my local authority that can own this?

How do I identify existing connected places projects?

Do we have the right roles within the authority?

3

Next steps

Gain visibility of all connected places projects in the authority.

- Identify cyber risks associated with these.
- Set-up processes to manage these risks.

Identify the individuals in the authority who perform the suggested roles.

Set up a CPSSG or integrate this into an existing governance board.

Engage IT teams on any existing or planned connected places projects.

Appendix

Example implementation

Case study: Perth & Kinross Council

Need:

Perth & Kinross Council has a growing interest in Internet of Things (IoT) deployments. They have been involved in many IoT projects, some supported by the EU ERDF Structural Funds (for instance smart waste, intelligent street lighting, CCTV enhancement and IoT in social housing) and by other sources (such as sensors placed in rural sites to detect vehicles and visitors, for example). The Council has an established cross Service Digital Board, chaired by the Council's Chief Digital Officer. This Board will oversee and assure delivery of the recently released Digital Strategy 2023-2027, Digital Perth and Kinross. The Digital Strategy includes an increased focus on connected places. As part of this work, the Council commissioned a consultant to advise on development of an IoT Roadmap. Consultants recommended the Council take a more active role in ensuring their IoT service providers were demonstrating cyber security compliance.

Solution:

Through participating in the Secure Connected Places research project and picking up on the recommendations of the IoT Roadmap report, the council is now using the Connected Places Security Steering Group (CPSSG) guidance to take the issue of connected places cyber security strategically through its appropriate governance channels. Doing so will ensure that appropriate scrutiny, assurance and approval is undertaken to oversee the implementation of the following security measures:

- How the network architecture has been securely designed, constructed, developed, and maintained.
- Means to protect data, software, devices, and equipment responsible for the operation of networks and services.
- Measures are taken to protect monitoring tools and to ensure they are not located in high-risk countries.
- Demonstrate they have undertaken a security review of their suppliers and third-party contractors and have contingency plans in place in the case of a security breach by a supplier.
- Discuss what actions have been taken to minimise the risk of unauthorised access to networks or services applying multi-factor authentication and password protection where appropriate.
- Plans to recover networks, services, and data in the event of a security compromise.

Outcome:

By implementing the CPSSG guidance set out in this governance resource, Perth & Kinross Council have been able to further mature their consideration of cyber security in their connected places projects. Their Digital Board will now be able to ensure that risks are being properly managed and projects properly governed, with consideration being given to the Principles. The council has learned a great deal from the Secure Connected Places research project, both in terms of the requirements for cyber security but also how it can work cooperatively across different services to ensure greater security. The council has plans for further IoT projects – as outlined in their IoT Roadmap – and will take both a strategic and operational approach to ensure that cyber security is addressed in all connected places projects.

Example implementation

Case study: Merthyr Tydfil County Borough Council

MERTHYR TYDFIL
County Borough Council
Cyngor Bwrdeistref Sirol
MERTHYR TUDFUL

Use case(s):

Public WiFi

Need:

Merthyr Tydfil County Borough Council found that 90% of their town centre businesses had access to the internet but the majority (66%) accessed this via their mobile internet and a sixth of these users wanted a public Wi-Fi offering in their town centre. The current set up was making their systems too slow, creating inefficiencies, and limiting the volume of card payments businesses could take. As part of the Council's Smart Town Strategy, they decided to implement a public WiFi offering but wanted to ensure it was secure and in line with the Council's processes.

Solution:

The Council built upon the governance structures they had set up from using the Governance in a Box resource and used the Cyber Security Principles 101 resource to present to the Corporate Management Team and Senior Leadership Teams to increase their awareness and understanding of connected places cyber security for current and future work. Merthyr Tydfil bolstered this by using the Procurement & Supply Chain Management resource to enhance their supplier questionnaire which would be used to procure connected places assets.

Outcome:

As a result of drawing upon the various resources within the Playbook, Merthyr Tydfil County Borough Council were able to engage 29 people across their Corporate Management Team and Senior Leadership Group on the cyber security of connected places assets. Going forwards this will provide better visibility for, and oversight of, their connected places projects to ensure that connected places projects are fully signed off and their public Wi-Fi project can be executed efficiently. Merthyr Tydfil County Borough Council are now looking to create an eLearning version of the Cyber Security Principles 101 resource to increase the reach and cyber security awareness of connected places projects throughout the Council.

Example implementation

Case study: West of England Combined Authority

WEST OF ENGLAND Combined Authority

Use case(s):

Traffic management

Need:

West of England Combined Authority were looking at ways to better integrate public transport systems and improve citizens' travel experiences in the region by creating a Transport Data Hub and implementing their Mobility as a Service (MaaS) initiatives. To do this they needed to address various governance and policy issues related to cyber security but processes related to cyber governance, risk management and threat analysis at the organisational level were lacking and needed further support.

Solution:

The Combined Authority used the Governance in a Box resource, particularly the commission document and the cyber treatment plan, to understand the various connected places projects across their organisation. The resource has helped the Combined Authority at a project level, as they have been able to update their Project Initiation Document (PID) to incorporate more cyber and digital considerations. They have also been able to make significant revisions to their Cyber Risk Register and create a new project committee to engage stakeholders. The PID will be used for future connected places projects so their digital and technology leaders can support the delivery of their connected places projects and incorporate them further into the Combined Authority's governance processes.

Outcome:

The use of the Governance in a Box resource has been a catalyst for change for the Combined Authority who are now looking to formalise and disseminate the valuable knowledge and practices they have acquired to their local authorities to create a standardised approach to the cyber security of their connected places projects. They have started to incorporate the steering group guidance into a newly established Governance Board subgroup for connected places. In the future, the Combined Authority will use the guidance to develop a West of England Digital Charter to provide further guidelines for data-enabled transport technologies in the region and enhance their 2024 Digital, Data and Technology Strategy.

Example implementation

Case study: Newcastle City Council

Use case(s):

Community Safety, Outdoor Public WiFi

Need:

Newcastle City Council (NCC) needed to replace its aging free public Wi-Fi offering whilst also overhauling their CCTV infrastructure. To do this as well as implement their various other connected places projects, they needed to create a standardised approach across the Council, especially engaging their ICT and Digital teams to make them aware of this approach. They found that expert teams were very aware of the threats and risks associated with connected asset implementation if they were fully engaged but this could be more consistent and specific across the organisation.

Solution:

By introducing a Connected Places Steering Group Terms of Reference into their current digital processes, NCC have been able to expand the awareness key stakeholders have of connected places projects across the Council. This will also be used to form the basis for an Intranet site devoted the connected places projects so teams are able to understand where overlaps may be. They have been able to apply the security principles from the resource to the design phase of their project alongside their supplier, helping them make more secure decisions about the types of tooling they should use.

Outcome:

NCC were already implementing secure processes and solutions, but the resources have given them a standardised approach to consistently achieve a secure connected places network. By being able to view all connected places projects across the Council, it has made it easier to review collective risks and threats and improve the speed and efficiency of their projects. They have found that the resource has also been a useful tool to enhance stakeholders' understanding of connected places and how to secure them. NCC are also looking to widen their reach and share their experiences with their regional local government IT leaders' forum to help other councils reach the same level of efficiency.

Glossary of terms

Term / acronym	Definition
Architecture	The designed structuring of something e.g. an agreed set of components for IT systems
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
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
Methodology	A particular set of methods, rules, procedures employed by a discipline
NCSC	National Cyber Security Centre
Personally Identifiable Information	Information that relates to an identified or identifiable person. This can be name, phone number, IP address etc. If it is possible to identify an individual from the information then it may be personal information
Risk	A situation involving exposure to risk, harm or loss
Risk appetite	The level of risk that an organisation is willing to accept
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:	This resource will advise you on the processes and considerations needed to set up and maintain good security governance across all connected places projects.
Limitations:	By its nature, this tool has limited coverage across the principles as it focuses on governance and there are key gaps across the 'designing your connected place' group of principles.

■	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