

IoT Deployment Handbook for Social Housing – a practical, legal, and regulatory framework

Handbook developed by Intelligens Consulting Limited for Glasgow City Region

Supported by:

Professor Guido Noto La Diega, Professor of Law, Technology and Innovation at the University of Strathclyde;

Malcolm Combe, Reader, School of Law, University of Strathclyde and

Burness Paull LLP.

Final version

Contents

About this handbook **6**
Purpose 6
Scope of the handbook 7
Out of scope 8
Disclaimer 8

How the handbook works **10**
The six-step process 10
How to use this handbook 11
How the handbook supports users 13
Using this handbook in practice 13
Key principles underpinning the handbook 15

What to expect for different types of deployment **16**
Damp and mould monitoring example 16
Legionella monitoring example 17
Telecare example 18
Void management example 18

1 Step 1: Define the Problem and Identify Use Cases **21**
1.1 Define and record the use case(s) 22
1.2 Define the problem and identify the use case 25
1.2.1 Understand contributing factors 25
1.3 Use case identification guide 25
1.4 Confirm the correct use case 26
1.5 Define the data, its use and expected outcomes 27
1.6 Organisations, roles, and governance responsibilities 28
1.7 Decision point 31
1.8 Common mistakes to avoid 31
1.9 Critical control — change of purpose 31
1.10 Step 1 Outcome 32

2 Step 2 - Assess Organisation and Governance Readiness **33**
2.1 Assess organisational readiness 34
2.1.1 Purpose definition and scope 35
2.1.2 Governance and accountability 37
2.1.3 Data lifecycle and control 40
2.1.4 Supporting proportionate governance through IoT solution design 44
2.1.5 Transparency and trust 45
2.1.6 Governance readiness and safeguard capability 49
2.1.7 Organisational readiness checkpoint 52
2.2 Applying proportional governance 52
2.3 Step 2 Conclusion 53
2.3.1 Step 2 Outcome 57

3	**Step 3 - Governance Classification and Use Case Assessment**	**59**
3.1	Governance classification overview	62
3.1.1	Governance levels	62
3.1.2	Lower-impact and higher-impact use	62
3.1.3	Governance flags	63
3.1.4	Governance requirements	63
3.1.5	Legal guardrails	63
3.1.6	Consent	64
3.1.7	How these concepts are used in Step 3	65
3.2	Initial deployment context and scaling considerations	66
3.2.1	Deployment environment and tenancy context	66
3.2.2	Rollout approach and scaling	67
3.2.3	Nature of data use and potential impact on people	68
3.3	Applying use case profiles	70
3.3.1	Selecting the relevant use case profile	70
3.3.2	Interpreting governance flags in context	71
3.3.3	Confirming the governance classification	72
3.3.4	Recording the governance classification	75
3.4	Governance capability and gap assessment	77
3.4.1	Assessing governance capability	78
3.4.2	Governance capability framework	81
3.4.3	Assess current governance capability	98
3.5	Step 3 Conclusion	102
3.5.1	Step 3 Outcome	102
4	**Step 4 – Real-World Deployment Assessment and Justification**	**104**
4.1	Understanding how the use case will operate in practice	105
4.2	Identifying considerations from how the use case operates in practice	108
4.3	Considering combined or multi-faceted use within the intended deployment	109
4.4	Tenancy and legal implications	112
4.4.1	Identifying tenancy and legal governance engagement	112
4.5	Step 4 Conclusion	115
4.6	Step 4 Outputs	115
4.6.1	Step 4 Outcome	117
5	**Step 5 – Governance Definition, Readiness and Approval**	**118**
5.1	Confirming previous step outputs	121
5.1.1	Confirming Step 2 outputs	122
5.1.2	Confirming Step 3 outputs	123
5.1.3	Confirming Step 4 outputs	125
5.2	Defining governance arrangements, safeguards and responsibilities	128
5.2.1	Defining governance arrangements	128
5.2.2	Governance domain assessment outcome	129
5.2.3	Confirmation	130
5.3	Defining responsibilities and accountability	131
5.3.1	Responsibilities and accountability assessment	131
5.3.2	Responsibilities and accountability outcome	133
5.3.3	Confirmation	133
5.4	Legal, tenancy and deployment conditions	133
5.4.1	Pathway mapping guidance	134
5.4.2	Place-based pathway	138
5.4.3	Tenant affecting deployments	141

5.4.4 Health, care and telecare deployments 144
5.5 Governance and deployment decision 149
5.5.1 Confirming the assessment remains current 150
5.5.2 Recording the governance and deployment decision 153
5.6 Step 5 Conclusion 159
5.6.1 Step 5 Outcome 160
5.7 Step 5 Completion 160

6 Step 6 – Governance Review and Reassessment 161
6.1 Reviewing whether the governance position remains current 163
6.1.1 Governance position remains current check 163
6.1.2 Changes identified 164
6.1.3 Guidance 164
6.1.4 Confirmation 164
6.2 Reviewing changes to the deployment 165
6.2.1 Deployment change assessment 165
6.2.2 Changes identified 166
6.2.3 Guidance 166
6.2.4 Confirmation 167
6.3 Reviewing whether governance assumptions continue to hold 167
6.3.1 Governance assumptions review 168
6.3.2 Observations identified 169
6.3.3 Guidance 169
6.3.4 Confirmation 170
6.4 Step 6 Conclusion 171
6.5 Step 6 Outcome 171

Annex A IoT use case definitions 173
A.1 Purpose of this Annex 173
A.2 Use case families 173
A.3 Use case definitions 173
A.4 Environmental and healthy homes use case profiles 178
A.4.1 Damp and mould 178
A.4.2 Indoor air quality (IAQ) and CO_2 181
A.4.3 Leak detection 184
A.4.4 Temperature and energy monitoring 187
A.5 Fire and tenant safety use case profiles 190
A.5.1 Smoke alarms 190
A.5.2 Fire alarm systems 193
A.6 Telecare and health support use case profiles 196
A.6.1 Fall detection 196
A.6.2 Telecare systems 199
A.6.3 Voice assistants (care context) 202
A.7 Behaviour and occupancy monitoring use case profiles 205
A.7.1 Occupancy and presence detection 205
A.7.2 Noise monitoring 208
A.7.3 Appliance-level monitoring 211
A.7.4 Thermal imaging 214
A.8 Security and access control use case profiles 216
A.8.1 Internal CCTV 216
A.8.2 External CCTV 220
A.8.3 Smart locks and door entry 223

A.9 Workforce and asset management use case profiles 226
A.9.1 Asset performance monitoring 226
A.9.2 Lone worker support 229

Annex B Handbook and use case definitions 232
B.1 Governance level 232
B.2 Governance flag 233
B.3 Governance requirements 233
B.4 Legal guardrails 234

Annex C Best practices 236
C.1 Step 1 – Define the use case 236
C.2 Step 2 – Assess organisational and governance readiness 237
C.3 Step 3 – Governance classification 238
C.4 Step 4 – Assess the intended deployment 238
C.5 Step 5 – Governance definition, readiness and approval 240
C.6 Step 6 – Governance review and reassessment 240

Annex D Sources used outside GCR 242

Tables

Table 1: Problems, use cases, data use and outcomes 23
Table 2 Organisations, roles, and governance responsibilities 30
Table 3 Purpose, definition and scope 36
Table 4 Governance and accountability 38
Table 5 Data lifecycle and control 41
Table 6 Transparency and trust 46
Table 7 Governance readiness and safeguard capability 50
Table 8 Step 2 readiness checkpoint 54
Table 9 Step 2 organisational governance readiness 56
Table 10 Step 2 outcome 57
Table 11 Deployment environment 67
Table 12 Roll out approach and scaling 68
Table 13 Data use and outcomes 70
Table 14 Use case profile confirmation 72
Table 15 Governance classification for each use case 76
Table 16 Current governance capability 101
Table 17 Step 3 outcome 102
Table 18 Operating use cases 107
Table 19 Practical impacts and power imbalance considerations 109
Table 20 Combined and multi-faceted deployment of use cases 111
Table 21 Tenancy and legal governance engagement 114
Table 22 Outputs carried forward from Step 4 to Step 5 116
Table 23 Step 4 outcome 117
Table 24 Confirming Step 2 outputs 123

Table 25 Confirmation of Step 2 outputs 123
Table 26 Confirming Step 3 outputs 124
Table 27 Confirmation of Step 3 outputs 125
Table 28 Confirming Step 4 outputs 126
Table 29 Confirmation of Step 4 outputs 127
Table 30 Governance domain assessment 129
Table 31 Confirmation of governance domain assessment 130
Table 32 Responsibilities and accountability assessment 132
Table 33 Responsibilities accountability outcomes 133
Table 34 Confirmation of responsibilities accountability outcomes 133
Table 35 Place-based deployment assessment 138
Table 36 Place-based deployment assessment concerns identified 140
Table 37 Place-based deployment assessment outcome 141
Table 38 Place-based deployment assessment confirmation 141
Table 39 Tenant affecting deployment assessment 142
Table 40 Tenant affecting deployment assessment concerns identified 143
Table 41 Tenant affecting deployment assessment outcome 144
Table 42 Tenant affecting deployment assessment confirmation 144
Table 43 Health care and telecare deployment assessment 145
Table 44 Health care and telecare deployment assessment concerns identified 148
Table 45 Health care and telecare deployment assessment outcome 148
Table 46 Health care and telecare deployment assessment confirmation 149
Table 47 Assessment remains current check 151
Table 48 Assessment remains current check changes identified 152
Table 49 Assessment remains current check outcome 152
Table 50 Assessment remains current check confirmation 152
Table 51 Governance deployment decision 154
Table 52 Deployment decision 155
Table 53 Decision rationale 156
Table 54 Decision rational recording and approval 157
Table 55 Partner organisation confirmation 158
Table 56 Partner organisation confirmation recorded 158
Table 57 Step 5 outcome 160
Table 58 Step 5 completion 160
Table 59 Governance position remains current check 163
Table 60 Changes identified 164
Table 61 Confirmation of governance position 164
Table 62 Deployment change assessment 166
Table 63 Changes identified 166
Table 64 Confirmation of changes identified 167
Table 65 Governance assumptions review 169
Table 66 Governance assumptions review observations identified 169
Table 67 Governance assumptions review confirmation 170
Table 68 Step 6 outcome 172
Table 69 Step 6 outcome review record 172

About this handbook

Purpose

This handbook provides a structured, step-by-step framework to support organisations in the safe, proportionate, and effective deployment of Internet of Things (IoT) solutions in social housing.

It has been designed to guide users from the earliest stage of identifying a problem, through to defining a use case, assessing organisational readiness, applying appropriate governance, and managing deployment over time.

The primary purpose of this document is to ensure that IoT solutions are:

- driven by clearly defined needs
- aligned to service outcomes
- deployed with appropriate oversight and accountability
- compliant with legal and regulatory requirements
- proportionate to the level of risk and tenant impact

Social landlords may consider deploying IoT solutions for a wide range of operational, regulatory, strategic and service-related reasons. These may include improving damp and mould management, supporting compliance with Awaab's Law (which came into force in Scotland on 6 October 2026), managing void properties, improving asset performance, supporting tenant wellbeing, enhancing building safety, improving energy efficiency, or addressing wider housing management challenges. This handbook is designed to support organisations in applying a consistent governance approach regardless of the issue being addressed or the technology being deployed.

The handbook has also been designed to support both current and future IoT deployment use cases. As technologies, regulatory requirements, governance expectations and deployment approaches evolve, organisations should review and adapt their use of the handbook to ensure it remains relevant and effective. This document should therefore be treated as a 'living' resource that can support emerging IoT applications alongside those described within the current version.

A focus on how data is used and the decisions that result from it, rather than the technology itself is a consistent theme throughout the handbook. This ensures that governance is applied consistently, regardless of the devices or systems involved.

Governance is influenced not only by the technology deployed, but also by how deployment outputs are used, who receives or acts upon those outputs, the environment in which the deployment operates, the organisations involved, and the individuals who may be affected by resulting decisions or interventions.

Good governance is achieved when organisations can demonstrate that deployment decisions have been informed by appropriate evidence, specialist input, consideration of risks and impacts, and clear accountability for decision-making. This document has been designed to support this by helping organisations identify relevant considerations, involve appropriate stakeholders and maintain a transparent record of decisions throughout the deployment lifecycle.

Supporting organisations in identifying and applying an appropriate level of governance based on the nature of the deployment, how data will be used, the potential impact on tenants, and

the decisions that may result from deployment outputs is central to the handbook. Organisations can better identify when additional legal, regulatory, governance, privacy, cybersecurity, tenancy, safeguarding, or specialist input may be required before deployment proceeds by working their way through the handbook. This document therefore supports lawful, accountable and proportionate deployment, but does not replace the need for organisations to comply with applicable legal or regulatory requirements.

The handbook can be used to deploy:

- a single IoT solution / use case
- multiple IoT solutions / use cases
- multiple IoT solutions / combined uses cases

Scope of the handbook

This handbook applies to the use of IoT in social housing where data is collected, analysed, or used to support decision-making.

It includes use cases such as:

- monitoring property condition and environmental factors (Awaab's Law in Scotland now means landlords have to follow strict, legally binding timescale with regards to damp or mould)
- detecting safety risks and triggering alerts
- supporting tenant health or wellbeing
- understanding occupancy or behaviour
- improving operational efficiency and asset management

The handbook covers:

- the definition and validation of use cases
- the use of data generated by IoT devices and systems
- governance, accountability, and oversight
- the responsibilities of organisations and partners involved
- the lifecycle management of IoT deployments

It applies to both:

- new IoT deployments
- changes or expansions to existing deployments

The handbook was developed by **Intelligens Consulting**, on behalf of Glasgow City Region (GCR), an award-winning-winning telecoms, digital and technology management consultant. Intelligens works across the UK and internationally, supporting public authorities, operators and investors to plan, fund and implement digital infrastructure and smart connected place strategies.

The development of this handbook was supported by:

- **Professor Guido Noto La Diega**, Professor of Law, Technology and Innovation at the University of Strathclyde, with internationally recognised expertise in IoT, AI and digital regulation;
- **Malcolm Combe**, Reader, School of Law, University of Strathclyde, has expertise in property law, with interests in land law reform, public access to land, and landlord and tenant law; and
- **Burness Paull LLP**, providing practitioner review from a data protection, cyber and governance review.

Out of scope

This handbook does not:

- prescribe or encourage deployment of specific technologies, devices, or suppliers
- provide technical design or system architecture guidance
- replace existing legal, regulatory, or compliance frameworks
- define detailed procurement or commercial processes
- provide detailed data protection guidance (e.g. how to complete a DPIA)
- provide any information or cyber security assessment

Instead, the handbook:

- identifies when these processes may be required
- ensures they are applied appropriately
- supports consistent and proportionate decision-making

Where specialist input is required (e.g. legal advice, data protection assessment, technical design), this can be obtained through existing organisational processes.

Disclaimer

This handbook provides guidance to support structured decision-making and governance in the use of IoT.

It is not a substitute for:

- legal advice
- regulatory interpretation
- professional or technical expertise

Organisations remain responsible for ensuring that:

- all applicable laws and regulations are complied with
- appropriate governance processes are followed
- decisions are made based on accurate and complete information

The guidance within this document is based on established principles of good governance, risk management, and service delivery. However, it should be applied in the context of each organisation's specific circumstances.

Some IoT deployments may have implications not only for data protection and governance processes, but also for tenancy arrangements, occupancy documentation, landlord access, and service delivery responsibilities. This handbook does not provide legal advice on tenancy law, but it highlights where organisations may need to review tenancy-related arrangements and obtain legal input where appropriate.

Where there is uncertainty or ambiguity, organisations may seek appropriate advice before proceeding.

Successful IoT deployment is not driven by technology alone. It depends on:

- clearly understanding the problem
- using data appropriately
- applying governance proportionately
- ensuring accountability throughout

This handbook provides the structure needed for users and organisations to achieve this in a consistent and practical way.

How the handbook works

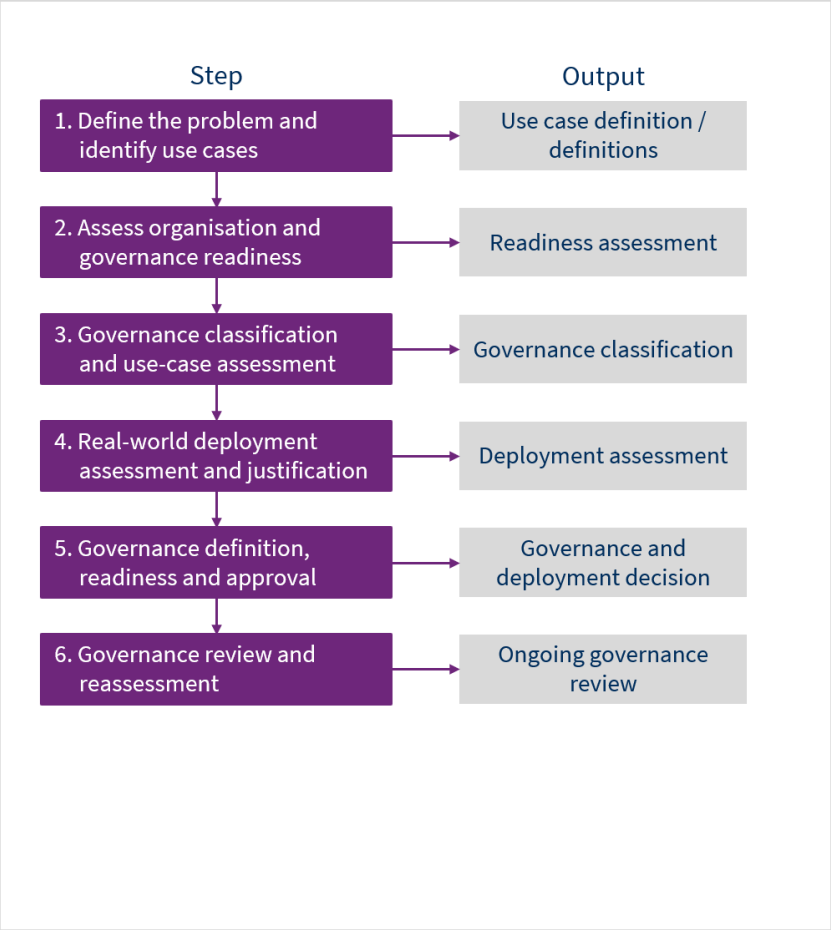
The six-step process

This document is designed as a **practical, step-by-step process** that users can follow when developing or reviewing an IoT use case.

It consists of a sequence of defined steps, each of which must be completed before moving to the next:

1. Define the problem and identify use case(s)
2. Assess organisational readiness
3. Determine governance requirements
4. Assess deployment context
5. Define governance arrangements and record the deployment decision
6. Review governance post-deployment and reassess where appropriate

Figure 1 Workflow of the six steps of the handbook



Each step produces outputs that are used in subsequent stages of the handbook. The workflow below illustrates how use case definition, readiness assessment, governance classification, deployment assessment, governance approval and ongoing review combine to form a connected governance process

The handbook also includes:

- a defined set of IoT use cases (Annex A, page 173)
- guided tools to support use case identification
- structured templates for documenting decisions and responsibilities.

How to use this handbook

This document is intended to support social landlords in making proportionate, consistent, and auditable decisions about whether and how to deploy IoT solutions.

It is not intended to replace legal advice, technical design, procurement processes, organisational governance arrangements or regulatory arrangements for social landlords (via the Scottish Housing Regulator). Instead, it provides a structured route for identifying what governance, safeguards, review, approval, communication, and deployment conditions need to be addressed before deployment proceeds.

The handbook provides guidance rather than prescriptive rules. Organisations should apply the framework in a way that reflects their own governance arrangements, operating models, risk appetite, legal obligations, tenancy arrangements, and deployment objectives. Not every deployment will require the same level of governance, documentation, specialist involvement, or approval. The framework is designed to help organisations determine what is appropriate in their specific circumstances and to apply governance proportionately.

A collaborative approach should be taken to completing this document. A lead individual or team should coordinate the process, but other internal teams, external advisers, delivery organisations, service providers, or partner organisations may need to contribute depending on the nature of the intended deployment.

This may include, where relevant:

- housing, tenancy, neighbourhood, or resident-facing teams
- asset, repairs, compliance, building safety, or property teams
- governance, risk, audit, or assurance functions
- legal advisers
- data protection, privacy, cybersecurity, or information governance specialists
- digital, technology, or operational delivery teams
- suppliers, contractors, telecare providers, service providers, or other delivery organisations
- partner organisations involved in receiving, sharing, interpreting, acting upon, or supporting the use of deployment outputs

The handbook is not prescriptive; it does not prescribe who should approve or sign off a deployment. Organisations should determine this through their own governance arrangements. This approach should ensure the level of scrutiny, specialist input, and senior review is proportionate to the governance requirements and deployment context.

Lower-impact or primarily asset-based deployments may be capable of progressing through existing governance arrangements with proportionate review.

Higher-impact deployments, person-based deployments, tenancy-affecting deployments, or deployments involving combined use cases, direct decision-making, external delivery organisations, or partner organisations are likely to require broader scrutiny, greater specialist involvement, and more senior approval before deployment proceeds. This document has been designed to support users through intended deployments of varying complexity. These may include:

- a single use case
- multiple independent use cases
- combined or integrated use cases
- sequential use of data, outputs, or decisions
- deployment across different environments or settings
- deployment involving multiple organisations

Users of this document should also consider the environment in which the deployment takes place, the handbook will help to facilitate this thinking. Governance may need to be applied differently depending on whether deployment occurs in:

- occupied homes
- new-build homes
- void or unoccupied properties
- communal or shared residential areas
- operational or staff environments
- mixed deployment settings

Users should not assume that all IoT deployments are tenancy-based. Some deployments are primarily associated with a property, building, tenancy, or access to the home.

Other deployments are primarily associated with an individual, a support service, healthcare provision, social care provision, telecare, or assisted-living support.

Some deployments may involve both place-based and person-based elements.

The governance, tenancy, legal, communication, documentation, access, safeguarding, and deployment considerations may therefore differ depending on the nature of the deployment.

Where the intended deployment is place-based, organisations may need to consider whether tenancy agreements, occupancy agreements, licences, access arrangements, tenant communications, and landlord or tenant responsibilities need to be reviewed or updated.

Where the intended deployment is person-based, organisations may instead need to consider service arrangements, commissioning arrangements, provider responsibilities, information-sharing arrangements, safeguarding requirements, and the roles of healthcare, social care, telecare, or other support providers.

Where deployments involve both place-based and person-based elements, organisations may need to consider both sets of issues.

Social landlords retain overall accountability for the deployment, accountability for governance, compliance, use of data, tenant impact, cybersecurity oversight, system integrity, and

deployment decisions cannot be transferred to suppliers, contractors, service providers, telecare providers, or partner organisations.

This document has been designed to help organisations identify:

- what the social landlord should ensure
- what delivery organisations should support or demonstrate
- where partner organisations are involved in the use of outputs
- what governance, legal, tenancy, communication, documentation, access, or deployment conditions need to be addressed before deployment proceeds
- and should also be used on the basis that governance is not static.

It is essential, that if the **purpose** of the deployment **changes**, if **use cases** are **combined** in new ways, if **new data sources** are **introduced**, if outputs are used in **new** decision-making contexts, or if **new** organisations become involved, the organisation **may** need to reassess the deployment through the relevant steps of the handbook.

How the handbook supports users

The handbook has been designed for users who may not have specialist knowledge of IoT, data governance, or regulatory frameworks.

It supports users by:

- breaking complex decisions into manageable steps
- providing guided questions and prompts
- offering a structured way to develop and test ideas
- clearly identifying when to involve other teams or specialists
- ensuring that decisions are evidence-based and documented

Completion of the handbook should involve input from individuals with responsibility for, or expertise in, the proposed deployment. Depending on the nature of the deployment, this may include representatives from housing, asset management, digital, data protection, information governance, cyber security, procurement, legal, resident engagement, operational teams and external delivery partners. Not all disciplines will be required in every case; however, organisations should ensure that decisions are informed by the appropriate expertise before progressing through approval gateways.

The level of assessment, stakeholder involvement and governance oversight should be proportionate to the nature, complexity and potential impact of the proposed deployment. Simpler, lower-risk deployments may require fewer activities, reviews and approvals than deployments involving higher levels of risk, complexity, personal data processing, tenancy impacts or multiple organisations.

Where uncertainty exists, the handbook prompts users to pause, seek input, and refine their understanding before proceeding.

Using this handbook in practice

Organisations should ensure that **ownership** exists for both the **completion** of the handbook and the **governance position** established through it. Governance remains an ongoing responsibility throughout the lifecycle of a deployment.

To use this handbook effectively:

- work through each step in sequence
- complete all required tables and records
- involve relevant colleagues as needed
- do not proceed where information is incomplete or unclear
- refer to earlier steps if conditions change

The outputs generated at each step form part of a **documented governance record**, which supports:

- internal approval
- audit and assurance
- regulatory compliance
- ongoing monitoring and review.

Key principles underpinning the handbook

A consistent governance approach for connected technology deployments in social housing has been applied to this handbook, which follow the core principles in Figure 2.

Figure 2 Principles underpinning the handbook



What to expect for different types of deployment

The following four deployment examples have been selected because they represent different governance contexts and different levels of handbook effort commonly encountered within social housing IoT deployments:

- **Damp and mould monitoring** – monitoring property conditions in occupied homes
- **Legionella monitoring** – supporting safety and compliance requirements
- **Telecare** – supporting health, wellbeing and safeguarding
- **Void management** – managing properties between tenancies and coordinating multiple organisations.

The examples help organisations understand:

- The steps involved in delivering an IoT project
- The level of effort required
- Key governance and legal considerations
- Who may need to be involved in decision-making.

They are also intended to support planning only. The full handbook should always be completed before making any deployment decisions.

Damp and mould monitoring example

Damp and mould monitoring is typically one of the simpler IoT deployments covered by the handbook. The deployment is usually focused on understanding property conditions, identifying potential damp and mould risks earlier, and supporting property management and maintenance activities.

When completing the handbook, organisations should expect particular attention to be given to:

- how monitoring will operate in occupied homes
- how outputs will be interpreted and acted upon
- tenant transparency and communication
- roles, responsibilities and accountability
- review, escalation and intervention arrangements.

Most organisations are likely to spend the greatest amount of time in:

- **Step 2** assessing organisational readiness
- **Step 4** understanding how the deployment will operate in practice
- **Step 5** defining governance arrangements and accountability.

Housing, asset management and repairs teams will normally contribute to completion of the handbook. Governance, information governance, legal and specialist colleagues may also need to be involved depending on how the deployment operates and how outputs are used.

Organisations with established governance arrangements and previous experience of deploying IoT solutions will generally complete the handbook more quickly than organisations establishing governance arrangements for the first time.

Damp and mould monitoring is generally less governance-intensive than telecare, occupancy-related monitoring or deployments that directly influence decisions affecting people. However, organisations should still expect meaningful effort in relation to governance, transparency, accountability and operational decision-making.

Legionella monitoring example

Legionella monitoring is typically focused on supporting water safety, compliance and asset-management activities. The deployment is usually intended to identify conditions that may indicate an increased risk of Legionella growth and support inspections, testing, maintenance and remediation activities.

When completing the handbook, organisations should expect particular attention to be given to:

- how monitoring supports existing compliance and safety processes
- how outputs will be interpreted and acted upon
- roles, responsibilities and accountability
- review, escalation and intervention arrangements
- operational ownership of monitoring outputs.

Most organisations are likely to spend the greatest amount of time in:

- **Step 2** assessing organisational readiness
- **Step 4** understanding how the deployment will operate in practice
- **Step 5** defining governance arrangements and accountability.

Asset management, compliance and maintenance teams will normally contribute to completion of the handbook. Governance, information governance, legal and specialist colleagues may also need to be involved depending on how the deployment operates and how monitoring outputs are used.

Organisations with established compliance, safety and governance arrangements will generally complete the handbook more quickly than organisations establishing these arrangements for the first time.

Legionella monitoring is generally less governance-intensive than telecare, occupancy-related monitoring or deployments that directly influence decisions affecting people. However, organisations should still expect meaningful effort in relation to accountability, review processes, escalation arrangements and operational decision-making.

Telecare example

Telecare deployments are typically intended to support health, wellbeing, independence, safeguarding or care-related outcomes. Deployments often involve multiple organisations and may require information to be reviewed, interpreted or acted upon by different services.

When completing the handbook, organisations should expect particular attention to be given to:

- how outputs influence decisions and actions affecting people
- responsibilities, accountability and governance arrangements
- safeguarding and wellbeing considerations
- information sharing and multi-agency working
- review, escalation and intervention arrangements.

Most organisations are likely to spend the greatest amount of time in:

- **Step 2** assessing organisational readiness
- **Step 3** understanding governance requirements
- **Step 4** understanding how the deployment will operate in practice
- **Step 5** defining governance arrangements, safeguards and accountability.

Housing, support, telecare, governance and information-governance teams will normally contribute to completion of the handbook. Healthcare organisations, social care organisations, legal advisers and other specialist stakeholders may also need to be involved depending on how the deployment operates and how outputs are used.

Organisations with existing care, support, safeguarding and governance arrangements will generally complete the handbook more quickly than organisations that need to establish these arrangements as part of the deployment.

Telecare is generally one of the more governance-intensive deployment types covered by the handbook. Organisations should expect significant effort in relation to safeguarding, accountability, information sharing, transparency, governance oversight and operational decision-making.

Void management example

Void management deployments are typically intended to support property utilisation, identify potentially unoccupied properties, reduce void periods and improve operational management of housing stock. Depending on how outputs are used, deployments may extend beyond asset management and raise additional occupancy, tenancy and governance considerations.

When completing the handbook, organisations should expect particular attention to be given to:

- how outputs are interpreted and acted upon

- occupancy, tenancy and transparency considerations
- roles, responsibilities and accountability
- review, escalation and intervention arrangements
- involvement of homelessness, temporary accommodation or support services where relevant.

Most organisations are likely to spend the greatest amount of time in:

- **Step 2** assessing organisational readiness
- **Step 3** understanding governance requirements
- **Step 4** understanding how the deployment will operate in practice
- **Step 5** defining governance arrangements and accountability.

Housing operations, tenancy management and service-owner functions will normally contribute to completion of the handbook. Governance, information-governance, legal and specialist colleagues may also need to be involved depending on how the deployment operates, how outputs are used and whether partner organisations are involved.

Organisations with established governance, accountability and review arrangements will generally complete the handbook more quickly than organisations establishing governance arrangements for the first time.

Void management is generally more governance-intensive than asset-focused monitoring deployments and similar to telecare deployments. Organisations should expect meaningful effort in relation to occupancy-related considerations, accountability, transparency, partner involvement and operational decision-making.

End of the Introduction – Move to Step 1 to start the Handbook

1 Step 1: Define the Problem and Identify Use Cases

Figure 3 Introducing Step 1's purpose, outputs and relevant principles



Step 1 establishes a clear and shared understanding of the proposed IoT deployment before any technical solution is developed or procured.

This step ensures that:

- the problem being addressed is clearly defined and evidenced
- the correct IoT use case(s) are identified using a standardised framework
- the intended use of data is explicit, controlled, and understood
- roles, responsibilities, and governance accountability are defined from the outset

Step 1 is critical because all subsequent decisions — including governance classification, approval, and deployment — depend on the accuracy and clarity of the information defined here.

By the end of this step, you should be able to clearly explain:

- what problem is being solved
- which IoT use case(s) apply
- how data and resulting outputs will be used in practice
- who is responsible for governance, decision-making, and delivery

IoT deployments must be driven by purpose and data use, rather than by technology or devices.

Refer to Annex C.1 which provides a set of best practices to assist with completing Step 1, Define the Problem and Identify Use Cases.

1.1 Define and record the use case(s)

Complete Table 1 as you work through Sections 1.2 to 1.5. The guidance in each section corresponds to one or more rows in Table 1. Return to Table 1 as needed to refine your responses.

Responses should be:

- clear and specific
- based on evidence where available
- directly aligned to the problem being addressed.

A single organisational problem may lead to several potential IoT use cases. More than one use case may apply to the intended deployment. Where this is the case, record each use case separately and carry each relevant use case through the subsequent handbook steps. Add further response columns or duplicate the table where more than two use cases are being assessed.

You should complete and refine Table 1 as you progress through this step.

Table 1: Problems, use cases, data use and outcomes

Area	What you need to define	Relevant guidance section	Use case 1 response	Use case 2 response
Problem definition	Clearly describe the issue being addressed	1.2		
Evidence of the problem	Evidence supporting the need (e.g. data, complaints)	1.2		
Contributing factors	Known or suspected causes of the problem	1.2.1		
Selected use case(s)	Use case(s) identified using the guide. Which use case(s) apply? (More than one may apply. See Annex A, page 173)	1.3 and 1.4		
Data to be collected	What data will be collected	1.5		
Data use	How data will be interpreted and used	1.5		

Area	What you need to define	Relevant guidance section	Use case 1 response	Use case 2 response
Expected outcomes	What improvement is expected (is it to benefit someone's health or safety? Or to improve building security, or energy efficiency etc.?)	1.5		

1.2 Define the problem and identify the use case

Use this section to complete the problem definition and evidence of the problem rows in Table 1, as you work through sections 1.2 through to 1.5.

Firstly, you need to clearly describe the issue you are trying to address.

Ask:

- What is happening?
- Why is it a problem?
- What evidence supports this?
- What outcome is required?

Avoid defining a solution at this stage.

Record your response in Table 1.

1.2.1 Understand contributing factors

Use this section to complete the Contributing factors row in Table 1:

- whether the problem has a single cause
- whether it involves multiple contributing factors
- the need to understand the wider context before selecting a use case.

Understanding the wider context will help ensure the correct use case is selected.

1.3 Use case identification guide

Use the Use Case Identification Guide below (A to F) to identify the most appropriate use case(s) and record the selected use case(s) in Table 1.

Start with the category that most closely reflects the problem, then identify the use case that best reflects the intended purpose and use of the data. Refer to Annex A where more detail is needed.

Select the closest option:

- Property or environmental condition → A
- Safety or immediate risk → B
- Health or wellbeing → C
- Behaviour or occupancy → D
- Security or access → E
- Operations or assets → F

A — Environmental and healthy homes

- Damp or moisture → Damp and mould
- Air quality → Indoor air quality
- Water leaks → Leak detection
- Temperature or energy → Temperature and energy monitoring

B — Fire and tenant safety

- Fire detection → Smoke alarms or fire systems
- Smoke detection → Smoke alarms

C — Telecare and health support

- Monitoring a health condition → Telecare systems
- Detecting falls → Fall detection
- Supporting daily living → Voice assistants (care context)

D — Behaviour and occupancy monitoring

- Presence or occupancy → Occupancy and presence detection
- Heat based patterns → Thermal imaging
- Noise → Noise monitoring
- Appliance use → Appliance-level monitoring

E — Security and access control

- CCTV → Internal or external CCTV
- Access control → Smart locks and door entry

F — Workforce and asset management

- Equipment monitoring → Asset performance monitoring
- Predicting faults → Asset performance monitoring
- Workforce safety → Lone worker support

1.4 Confirm the correct use case

Some ideas may appear to fit more than one use case, which occurs where the same data could be used in different ways.

Confirm that the selected use case is based on how the data and outputs will be used, rather than only on what the technology measures. Record the confirmed use case in Table 1.

Example:

- Monitoring UV levels to assess environmental conditions → Environmental use case
- Using UV patterns to infer occupancy → Behavioural use case

Where more than one use case could apply, record each potentially relevant use case and refer to Annex A (page 173). Seek appropriate input where the intended purpose or use of outputs remains unclear.

Identifying a use case is **only the first stage** of the assessment. The governance implications of a deployment may be influenced by deployment context, intended use of outputs, participating organisations, deployment environment, and how outputs are acted upon in practice. These considerations are assessed in later steps of the handbook.

1.5 Define the data, its use and expected outcomes

Complete this section in Table 1

Use the prompts below to guide your responses.

What data will be collected

Examples include:

- environmental readings
- equipment or system data
- movement or presence
- health indicators

How will the data be interpreted

- threshold-based alerts
- trends over time
- comparison with other relevant data
- analytics or automated processing

What actions will result

- alerts
- inspections
- repairs or interventions
- operational decisions
- actions affecting tenants or services

Who will receive, review, interpret, or act upon the outputs generated?

Describe the practical improvement the organisation expects to achieve by collecting, interpreting and acting upon the IoT data. The expected outcomes should address the problem identified earlier in Step 1 and should be sufficiently clear to support later evaluation.

Consider:

- what improvement the organisation expects to see
- how the deployment will help address the identified problem
- whether risk is expected to reduce
- whether service delivery, operational efficiency, property conditions, safety, wellbeing or outcomes for tenants are expected to improve
- how success will be recognised in practice.

Examples may include earlier identification of damp and mould risks, faster responses to safety concerns, reduced emergency repairs, improved targeting of support or interventions, and better evidence for decision-making.

What outcomes are expected?

Describe the improvement the organisation expects to achieve from IoT data and the actions taken in response to it.

Examples may include:

- improved service delivery
- earlier identification of issues
- reduced risk
- improved property conditions
- better targeting of interventions
- improved outcomes for tenants, residents or service users.

Describe the improvement the organisation expects to achieve because of collecting, interpreting and acting upon the IoT data.

Expected outcomes should focus on the practical benefits the deployment is intended to deliver and should be directly linked to the problem identified earlier in this step.

Consider:

- what improvement the organisation expects to see
- how the deployment will help address the problem being investigated
- whether any risks are expected to be reduced
- whether service delivery, operational efficiency, property conditions, safety, wellbeing, or tenant outcomes are expected to improve
- how success will be recognised in practice.

Examples may include:

- earlier identification of damp and mould risks
- reduced property damage
- improved tenant health and wellbeing
- faster response to safety concerns
- improved targeting of support or interventions
- reduced emergency repairs
- improved operational efficiency
- better evidence for decision-making.

1.6 Organisations, roles, and governance responsibilities

Identify the internal teams and external organisations expected to support, deliver, govern, receive, interpret, share or act upon outputs from the intended deployment. Use Table 2 to record their roles and responsibilities. Example organisations and teams are provided in Table 2 below. **Only complete** the rows that apply and add additional organisations where needed.

Organisations should record all known internal teams, partner organisations, delivery organisations, service providers, advisers, or other parties that are expected to contribute to, support, receive outputs from, interpret outputs from, or act upon the intended deployment.

Guidance:

- Include all internal teams and external organisations
- Roles may include device provider, platform provider, operational teams, or governance functions
- Governance role includes responsibility for oversight, compliance, and applying controls
- Data role must identify controller and processor responsibilities
- “Responsible for acting on outputs” means responding to alerts, decisions, or actions.

Include any internal team, organisation, provider, contractor, partner, support service, telecare provider, healthcare organisation, social care organisation, or other third party that may receive, review, interpret, share, or act upon deployment outputs, or that has governance, legal, operational, support, safeguarding, or decision-making responsibilities associated with the deployment.

Key rule:

The housing provider remains accountable for governance, data use, and decisions, even where services are delivered by third parties.

Complete Table 2 below - only complete the rows that apply to the use case(s) you are planning to deploy and add additional organisations where needed. Where a listed function is not relevant, record “not applicable” or remove the row.

If any role, responsibility or organisational involvement remains unclear, pause and seek input from the appropriate operational, governance or specialist colleagues before proceeding.

Table 2 Organisations, roles, and governance responsibilities

Organisation / Team	Role in the Deployment	Key Responsibilities	Governance Role	Data Role (Controller / Processor)	Responsible for Acting on Outputs
The RSL / social housing provider you represent					
Maintenance team					
Legal team					
Data protection, risk or governance teams					
IT team					
Healthcare partner					
Social care partner					

1.7 Decision point

Before proceeding, confirm that the following are clearly defined and documented:

- the problem
- the use case(s)
- how the data will be used
- roles, responsibilities, and governance accountability

If any of the above are incomplete or unclear:

- do not proceed
- return to the relevant section in Step 1
- refine the information
- involve appropriate colleagues if required

You should only proceed to Step 2 when:

- Table 1 clearly records the problem, evidence, contributing factors, selected use case or use cases, data use and expected outcomes
- Table 2 identifies the relevant organisations, roles and responsibilities
- the information is sufficiently clear and agreed to support the readiness assessment in Step 2.

1.8 Common mistakes to avoid

- starting with a solution instead of a problem
- selecting use cases based on technology rather than purpose
- unclear or undefined data use
- failing to identify multiple use cases
- overlooking higher-impact uses such as behavioural inference

1.9 Critical control — change of purpose

A material change in the purpose for which data or outputs are used may create a new or changed use case and require reassessment.

Examples include:

- adding behavioural analysis
- combining datasets
- introducing analytics or AI
- new organisations receiving or acting upon outputs
- outputs being used to inform different decisions or interventions
- deployment being expanded into new environments or resident groups

If this occurs:

- return to Step 1
- redefine the use case
- repeat the process

1.10 Step 1 Outcome

Before moving to Step 2, confirm that:

- Table 1 is complete for every relevant use case
- Table 2 identifies the relevant organisations, roles and responsibilities
- the intended use of data and outputs is clearly described
- the information is accurate and agreed by the relevant contributors.

This forms part of the governance and approval record.

2 Step 2 - Assess Organisation and Governance Readiness

Figure 4 Introducing Step 2's purpose, outputs and relevant principles



The purpose of Step 2 is to assess whether the organisation is ready to support, govern, and operate the IoT use case(s) defined in Step 1.

Using the outputs from Step 1, this step helps determine whether the organisation has the capability, processes, responsibilities, and operational arrangements needed to:

- apply governance effectively in practice
- apply appropriate safeguards and governance consistently
- support transparency and accountability
- operate the deployment safely and consistently over time
- adapt governance appropriately if use, impacts, or operational requirements change

This step is not intended to assess whether the organisation is fully mature across all aspects of IoT governance.

Instead, it is intended to ensure that:

- governance requirements can realistically be applied
- gaps and limitations are understood
- the organisation can apply governance proportionately and consistently
- deployment decisions are evidence-based, practical, and supportable

The assessment should reflect:

- the specific use case(s) defined in Step 1
- the intended deployment approach
- the likely level of governance required
- the organisation's ability to sustain governance throughout the deployment lifecycle

Where users cannot answer an assessment question directly, they should obtain input from relevant colleagues. Depending on the use case, this may include:

- housing or operational teams
- governance or data protection teams
- IT or digital teams
- legal, procurement, or risk and compliance teams
- suppliers or delivery partners

The outputs from Step 2 will be used in subsequent steps to support:

- governance classification
- approval decisions
- governance planning and implementation
- ongoing monitoring, review, and reassessment throughout the deployment lifecycle

2.1 Assess organisational readiness

This section assesses organisational readiness across the following areas:

- Purpose definition and scope
- Governance and accountability
- Data lifecycle and control
- Transparency and trust
- Governance readiness and safeguard capability

The assessment should focus on whether the organisation is equipped to operate the use case effectively, apply governance proportionately, and support the deployment consistently over time.

Organisations are not expected to have complete maturity across all aspects of IoT governance before beginning deployment. Instead, the purpose of this step is to help organisations:

- understand what governance and operational capability is required

- identify where additional support, input, or controls may be needed
- apply governance proportionately to the intended use case
- support safe, practical, and effective deployment within organisational and regulatory expectations

The outputs from each readiness area must be used in subsequent steps including governance classification, approval, governance implementation, monitoring, review, and reassessment throughout the deployment lifecycle.

Organisations are encouraged to draw on relevant sector experience, supplier capability, peer learning, and established good practice when developing governance and operational approaches for IoT deployment.

This may include learning from:

- existing social housing deployments
- sector guidance or collaboration activities
- supplier experience supporting similar use cases
- operational approaches already established within partner organisations
- to assist in completing Step 2, Assess Organisation and Governance Readiness, refer to Annex C.2 (page 237) which provides a set of best practices.

The handbook is intended to support organisations in applying proportionate governance confidently and practically within their own operational context.

Accountability for governance decisions, operational use of IoT data, and deployment outcomes remains with the organisation.

The organisational-readiness assessment applies whether the intended deployment involves a single use case, multiple independent use cases or combined use cases. The specific implications of individual and combined use cases are considered in Steps 3 and 4.

2.1.1 Purpose definition and scope

This section assesses whether the organisation has clearly defined how success will be measured for the proposed deployment, whether the operational response to the deployment is understood and documented, and whether the organisation is prepared to identify and manage future changes in how data may be used.

This assessment helps organisations:

- define clear outcomes for the deployment
- demonstrate value and service improvement over time
- ensure operational teams understand how IoT outputs will be used in practice
- maintain appropriate governance if deployments evolve, expand, or introduce new forms of analysis

Complete Table 3 for each assessment area. Record whether the arrangement is fully in place, partially in place or not in place, then provide the information or evidence requested in the final column.

Table 3 Purpose, definition and scope

Assessment area	Why this matters	Status (Fully in place / Partially in place / Not in place)	Response / evidence (*use italicised statement for guidance*)
Outcome measures or KPIs have been identified for each use case and can be measured before and after deployment	Clearly defined KPIs help the organisation measure improvement, demonstrate value, and assess whether the deployment is achieving the intended outcome		*List the KPI(s) for each use case separately:*
Baseline KPI information has been captured, or there is a plan to capture it before deployment	Baseline information supports meaningful comparison and helps demonstrate the impact of the deployment over time		*Describe the existing baseline data or how it will be collected before deployment:*
The organisation has defined what actions, decisions, or operational processes will result from the deployment	Clearly defined operational responses help ensure alerts and insights can be managed consistently and appropriately		*Describe what actions, decisions, escalation processes, or operational responses will occur, including which teams are responsible and who will act on outputs or alerts:*
The organisation understands which teams or roles will need to support operation and oversight of the use case	Early involvement of relevant teams helps support effective governance and operational delivery		*List the teams, roles, or functions that need to be involved:*
The organisation understands how changes in use, combined use cases, data sharing, or new analysis may be identified and reassessed	Recognising changes in use early helps ensure governance remains appropriate as deployments evolve over time		*Describe how changes in use, combined use cases, data sharing, or new analysis would be identified, reviewed, and escalated:*

Changes in how data is used — including combining datasets, introducing new analysis, or applying AI or behavioural inference — may create new or higher-impact use cases.

Organisations should ensure that appropriate processes exist (such as by way of policies and training) to identify these changes and support reassessment through the framework where required.

The outputs recorded in this section must be used in subsequent steps including governance classification, approval, governance implementation, and ongoing monitoring and review.

2.1.2 Governance and accountability

Assess whether governance responsibilities, decision-making authority, accountability arrangements, and oversight processes relating to the proposed IoT deployment are sufficiently defined and operational.

This assessment helps organisations:

- ensure IoT outputs and insights are reviewed and acted on appropriately
- support effective oversight and accountability across teams and functions
- apply governance consistently and proportionately in practice
- support clear operational decision-making and escalation processes
- maintain appropriate governance as deployments evolve over time

Organisations change should consider including staff involved in the deployment who understand not only legal, procedural, and governance requirements, but also have considered the ethical and tenant-impact implications of how IoT data and outputs may be interpreted, shared, or used in practice.

This includes recognising that:

- lawful use may not always be proportionate or appropriate in every operational context
- IoT outputs should support informed human judgement rather than replace it
- inappropriate informal use of IoT insights may undermine tenant trust, confidence, and organisational accountability
- organisations should recognise that tenants and residents may not always be in an equal position to understand, challenge, or influence how IoT deployments operate in practice

Complete Table 4for each assessment area. Record whether the arrangement is fully in place, partially in place or not in place, then provide the information or evidence requested in the final column.

Table 4 Governance and accountability

Assessment area	Why this matters	Status (Fully in place / Partially in place / Not in place)	Response / evidence (*use italicised statement for guidance*)
The organisation has defined who is responsible for interpreting IoT outputs, reviewing alerts, and making operational decisions relating to the use case(s)	Clear operational ownership helps ensure IoT outputs are interpreted appropriately and acted on consistently		*Describe who is responsible for interpreting outputs, reviewing alerts, and making operational decisions:*
The organisation has defined how human oversight will be applied when acting on IoT outputs, alerts, insights, or recommendations related to the use case(s)	Human oversight helps ensure IoT outputs are considered alongside operational context and professional judgement before actions affecting tenants are taken		*Describe how human review, judgement, or approval will be applied before actions, interventions, or decisions are taken:*
Governance responsibilities and decision-making authority relating to the IoT deployment and use case(s) are clearly understood across relevant teams	Clear accountability helps ensure decisions, oversight, and operational responses relating to IoT data and outputs are managed consistently		*Describe how governance responsibilities and decision-making authority are allocated across teams or functions:*

Assessment area	Why this matters	Status (Fully in place / Partially in place / Not in place)	Response / evidence (*use italicised statement for guidance*)
The organisation understands how issues relating to the IoT deployment will be reviewed and escalated where needed	Clear escalation arrangements help organisations respond consistently where issues arise relating to IoT outputs, tenant impact, unintended use of data, safeguards, or operational concerns		*Describe how issues relating to the deployment would be reviewed, escalated, and managed:*
The organisation can evidence how decisions, actions, reviews, and approvals relating to the IoT deployment will be recorded and retained where appropriate	Maintaining appropriate records helps support operational consistency, governance assurance, learning, and review over time		*Describe what records, approvals, reviews, or evidence relating to the deployment will be maintained:*

Suppliers or delivery partners may provide assistance with governance activities, but accountability for governance decisions and oversight remains with the organisation.

The outputs recorded in this section must be used in subsequent steps including governance classification, approval, governance implementation, escalation management, audit activity, and ongoing monitoring and reassessment.

2.1.3 Data lifecycle and control

This section assesses whether the organisation can manage IoT data appropriately throughout its lifecycle, including collection, storage, access, sharing, retention, review, and ongoing control of data relating to the proposed use case(s).

For the purposes of this assessment, “IoT data” includes:

- data generated or collected through IoT devices or sensors
- alerts, outputs, or notifications generated by IoT systems
- analysis, insights, recommendations, or inferred information derived from IoT data
- operational actions or records created as part of responding to IoT outputs
- data shared or combined with other organisational or partner systems as part of the defined use case(s)

The assessment should reflect how IoT data and related outputs are used throughout the deployment lifecycle, not only the original sensor data itself.

This assessment helps organisations:

- understand how IoT data and related outputs will be managed in practice
- support effective operational use and governance of IoT data
- maintain appropriate controls over access, sharing, and use of IoT data and related outputs
- support accountability, auditability, and governance assurance
- apply safeguards proportionately as deployments evolve over time
- ensure proposed IoT solutions can support the organisation’s governance and operational requirements

Complete Table 5 for each assessment area. Record whether the arrangement is fully in place, partially in place or not in place, then provide the information or evidence requested in the final column.

Table 5 Data lifecycle and control

Assessment area, the organisation:	Why this matters	Status (Fully in place / Partially in place / Not in place)	Response / evidence (*use italicised statement for guidance*)
understands what IoT data and related outputs will be generated, how they will be used, and which systems or processes will use them	Clear understanding of data flows and usage helps support effective governance and operational management		*Describe what IoT data, alerts, insights, recommendations, or outputs will be generated, how they will be used, and which systems, platforms, or processes will access or use them:*
has considered who should have access to IoT data and related outputs for the use case(s)	Appropriate access arrangements help ensure IoT data and outputs are available to relevant teams, roles, or partner organisations while supporting proportionate governance		*Describe which teams, roles, suppliers, partners, or external organisations will require access to IoT data or related outputs:*
understands whether IoT data, alerts, insights, or outputs will be shared internally or externally as part of the deployment	Clear data-sharing arrangements help support governance, operational coordination, and partnership working		*Describe whether IoT data or related outputs will be shared and who they will be shared with:*

Assessment area, the organisation:	Why this matters	Status (Fully in place / Partially in place / Not in place)	Response / evidence (*use italicised statement for guidance*)
has identified the governance, data protection, legal, compliance, social care, healthcare, telecare, support or other internal and external organisations that need to support the deployment or act upon its outputs	Early and ongoing involvement of relevant teams or partner organisations helps support proportionate governance, operational decision-making, and appropriate safeguards throughout the deployment lifecycle		*Describe which governance, operational, partner, or specialist teams will support the deployment and when they will be involved:*
has considered how long IoT data, alerts, outputs, and related records should be retained	Appropriate retention arrangements help support operational value, governance needs, and lifecycle management of IoT data		*Describe how long IoT data, alerts, outputs, or related records are expected to be retained and why:*
can identify and review how IoT data and related outputs have been used, accessed, or acted on	Appropriate records and traceability help support operational review, governance assurance, learning, and response to issues or complaints		*Describe what records, logs, audit trails, or reporting capabilities will be available:*
understands how safeguards relating to IoT data and related outputs will be applied and maintained	Appropriate safeguards help support reliable and proportionate management of IoT data throughout the deployment lifecycle		*Describe what safeguards, controls, or governance measures will apply to the use of IoT data and related outputs:*

Assessment area, the organisation:	Why this matters	Status (Fully in place / Partially in place / Not in place)	Response / evidence (*use italicised statement for guidance*)
understands how changes to IoT data use, sharing, integration, or analysis would be identified and reviewed	IoT deployments may evolve over time, including through new integrations, analytics, AI, or combined use cases		*Describe how changes to data use, sharing, integration, or analysis would be identified, reviewed, and reassessed where appropriate:*

2.1.4 Supporting proportionate governance through IoT solution design

Organisations should consider whether the proposed IoT solution can support proportionate governance and operational control requirements in practice.

The purpose of this section is to help organisations consider whether the proposed solution can support the governance, transparency, accountability, oversight and operational requirements that may emerge through the handbook.

Governance requirements should not be treated as an activity that is applied after a solution has been selected. Organisations should consider at an early stage whether the proposed solution can support the level of governance that may ultimately be required

This may include considering whether suppliers or platforms can support:

- proportionate collection of IoT data appropriate to the use case
- configurable alerting or reporting arrangements
- role-based access to data and related outputs
- separation between raw data and operational dashboards
- appropriate audit and reporting capabilities
- data protection requirements, including reasonable assistance with data protection impact assessments, data-subject rights and the implementation of appropriate security measures
- data retention and deletion requirements
- restrictions on unnecessary access, sharing, or reuse of data.

Examples of restrictions may include:

- limiting the frequency of environmental readings where continuous monitoring is not required
- restricting access to underlying sensor data while allowing operational teams to receive alerts or exception reporting
- limiting access to sensitive or higher-impact data to authorised teams or roles only

The handbook does not prescribe technical solutions or procurement approaches. However, organisations should ensure that proposed IoT solutions can support the governance, operational, and proportionality requirements of the intended use case(s).

Organisations are not being asked to assess technical specifications or procurement solutions. Instead, they should consider whether the proposed solution is likely to support the governance, operational and accountability requirements identified through the handbook.

The considerations identified in this section should inform the readiness assessments completed in Table 3 to Table 7 and should be revisited when evaluating potential suppliers, platforms or deployment approaches.

2.1.5 Transparency and trust

This section assesses whether the organisation can support appropriate transparency, communication, engagement, consultation, and tenant trust throughout the lifecycle of the proposed IoT deployment.

This assessment helps organisations:

- explain clearly how IoT is being used and why
- support tenant understanding of the intended use case(s) and expected outcomes
- apply transparency and engagement approaches proportionately to the deployment
- support confidence, accountability, and trust throughout the deployment lifecycle
- prepare for higher levels of engagement or consultation where deployments may have greater tenant impact or governance requirements.

Complete Table 6. for each assessment area. Record whether the arrangement is fully in place, partially in place or not in place, then provide the information or evidence requested in the final column.

Table 6 Transparency and trust

Assessment area, the organisation:	**Why this matters**	**Status (Fully in place / Partially in place / Not in place)**	**Response / evidence (*use italicised statement for guidance*)**
has considered how the purpose of the IoT deployment and use case(s) will be explained to tenants, residents, or other affected groups	Clear communication helps support understanding, confidence, and transparency in how IoT is being used		*Describe how the deployment and use case(s) will be explained or communicated:*
has considered what information tenants, residents, or affected groups may reasonably expect to receive about the deployment	Different use cases and levels of impact may require different levels of explanation, communication, engagement, or consultation		*Describe what information, guidance, or communications will be provided:*
has considered whether the deployment may require enhanced engagement, targeted communication, or consultation activities	Some deployments may involve greater tenant interest, sensitivity, or impact and may benefit from more active engagement approaches		*Describe whether any additional engagement, consultation, or communication activities are planned:*
understands how transparency and engagement arrangements will continue	Ongoing transparency helps ensure tenants and affected groups remain appropriately		*Describe how tenants or affected groups would be informed about*

Assessment area, the organisation:	Why this matters	Status (Fully in place / Partially in place / Not in place)	Response / evidence (*use italicised statement for guidance*)
if the deployment evolves or changes over time	informed as deployments expand, change, or introduce new capabilities		*significant changes to the deployment or use of IoT data:*

Transparency and engagement requirements are likely to increase where deployments:

- involve monitoring within homes
- introduce behavioural analysis, inference, or AI-supported insights
- affect tenant rights, expectations, or living environments
- involve combined use cases or expanded use of IoT data over time

Lower-impact deployments may only require general awareness, clear communication, and appropriate tenant information.

Higher-impact deployments may require:

- enhanced transparency and explanation
- active engagement with tenants or representative groups
- consultation activities as part of deployment planning or governance review
- additional governance review and oversight
- ongoing communication as deployments evolve over time

Transparency should not rely solely on privacy notices or formal documentation.

Organisations should consider whether tenants and affected groups can reasonably understand:

- what the deployment is intended to do
- how IoT data and outputs will be used
- what actions or decisions may result
- what safeguards and controls are in place, including any rights to object where a deployment goes beyond a necessary repair, replacement or legally mandated installation
- how concerns, complaints, or requests can be raised

Clear, proportionate, and ongoing communication helps support tenant confidence, operational transparency, and trust in how IoT is being deployed.

Organisations should consider whether they are operationally and organisationally prepared to support the level of communication, engagement, transparency, and consultation likely to be required for the proposed deployment.

Organisations may benefit from drawing on sector experience, supplier insight, and established engagement approaches when developing tenant communication and transparency arrangements.

The handbook does not prescribe specific communication or consultation approaches. However, organisations should ensure that transparency and engagement arrangements remain appropriate to the intended use case(s), deployment context, and likely level of governance required.

The outputs recorded in this section must be used in subsequent steps including governance classification, approval, governance implementation, tenant engagement activities, and ongoing monitoring and reassessment.

2.1.6 Governance readiness and safeguard capability

This section assesses whether the organisation is prepared to apply, support, and sustain governance and safeguard measures proportionate to the proposed IoT deployment and any future change in deployment context or complexity.

This assessment helps organisations:

- understand that governance requirements may vary depending on deployment context and impact
- identify whether the organisation can support enhanced safeguards, oversight and / or escalation where required
- recognise where reassessment or additional governance review may become necessary over time
- prepare for subsequent governance classification and implementation activities within the handbook

Complete Table 7 for each assessment area. Record whether the arrangement is fully in place, partially in place or not in place, then provide the information or evidence requested in the final column.

Table 7 Governance readiness and safeguard capability

Assessment area	Why this matters	Status (Fully in place / Partially in place / Not in place)	Response / evidence (*use italicised statement for guidance*)
The organisation has considered whether it could support enhanced governance or safeguards if required by the deployment context	Some deployments may require stronger safeguards, oversight, transparency, auditability, or operational controls depending on how the deployment operates in practice		*Describe whether the organisation could support additional governance or safeguard measures if required:*
The organisation has considered whether deployment changes could require reassessment or enhanced governance over time	Governance requirements may change where deployments evolve, expand, introduce inference, combine datasets, or become more operationally relied upon		*Describe how deployment changes, increased governance requirements and escalation would be identified and reviewed:*
The organisation has considered whether additional governance, legal, specialist, tenant, or partner involvement may be required for higher-impact deployments	Some deployments may require broader organisational input or enhanced governance support before expansion or operational change		*Describe how additional governance, and / or escalation, or specialist involvement would be identified and supported:*
The organisation understands that governance review reflects the level of governance, safeguards, oversight, and	Governance classification helps determine the level of governance required and does not in		*Describe how the organisation will ensure governance decisions remain proportionate, transparent, and*

Assessment area	Why this matters	Status (Fully in place / Partially in place / Not in place)	Response / evidence (*use italicised statement for guidance*)
accountability required — not automatic permission or approval to deploy	itself determine whether a deployment is acceptable or permissible		*appropriately reviewed or escalated where required:*
The organisation has considered the environmental and sustainability implications of device deployment, replacement, and disposal	Large-scale IoT deployments may introduce sustainability, energy consumption, device lifecycle, and electronic waste considerations that should be managed appropriately throughout the deployment lifecycle		*Describe how environmental sustainability, device replacement, reuse, recycling, or disposal considerations will be managed where relevant:*

2.1.7 Organisational readiness checkpoint

Before progressing to the Step 2 readiness checkpoint, organisations should review the outcomes from Table 3 to Table 7 and determine whether they have sufficient information to assess organisational readiness and support governance proportionate to the proposed deployment.

This review should consider:

- whether the intended purpose and scope remain clearly defined and consistent with Step 1 outputs
- whether governance responsibilities and accountability arrangements are sufficiently understood
- whether any significant governance, operational, transparency, safeguarding, supplier-management, or capability gaps remain unresolved; and
- whether additional legal, governance, privacy, security, procurement, safeguarding, or specialist input may be required before proceeding

Where significant issues remain unresolved, organisations should consider addressing these before progressing to the Step 2 readiness checkpoint.

2.2 Applying proportional governance

Governance for IoT deployment should be applied proportionately to the intended purpose, operational use, deployment context and potential impact of the deployment. It is driven primarily by how IoT data and outputs are used in practice rather than by the technology itself. Governance expectations may therefore vary depending on:

- the intended purpose of the deployment;
- how outputs are interpreted or acted upon;
- the level of operational reliance on outputs;
- the potential impact on tenants, households or services;
- whether data is combined, reused or used for inference; and
- the safeguards and oversight arrangements applied in practice.

The handbook is designed to support organisations in understanding how governance expectations may increase as deployment impact, operational reliance or complexity increases.

The handbook does not replace:

- existing organisational governance arrangements;
- legal or regulatory obligations;
- information governance processes;
- security, procurement or operational frameworks
- legal advice or specialist review where required.

Governance classification is introduced in Step 3 and helps organisations understand the governance expectations associated with the intended deployment.

2.3 Step 2 Conclusion

Having completed the readiness assessments set out in Table 3 to Table 7, organisations should review and summarise their findings. Complete Table 8, which will provide a summary of the readiness assessments completed throughout Step 2.

Table 8 Step 2 readiness checkpoint

Row	Readiness consideration	Status (Yes / Partially / No)	Response / evidence
1	The intended purpose and scope of the proposed deployment are sufficiently understood (see Table 3)		
2	Governance responsibilities, accountability, operational ownership and matters requiring escalation are sufficiently understood (see Table 4)		
3	Data handling, lifecycle, sharing, retention, deletion, and exit considerations have been reviewed (see Table 5)		
4	Transparency, communication, and tenant engagement considerations have been reviewed (see Table 6)		
5	Governance, operational, transparency, oversight, safeguarding, supplier-management, resourcing, or capability gaps requiring further action have been identified and recorded (see Table 7)		

Using the outputs from Table 3 to Table 7 and Table 8, organisations should consider the wider governance, operational, assurance, and support implications of the proposed deployment.

This assessment is intended to determine whether the organisation can support and sustain governance proportionate to the proposed deployment and to identify any additional governance, capability, or specialist support requirements before progressing.

The considerations in Table 9 require organisations to draw conclusions from the assessments completed in Table 3 to Table 7 and identify any governance, capability, assurance, or specialist support requirements that may need to be addressed before progressing.

Table 9 Step 2 organisational governance readiness

Row	Readiness consideration	Status (Yes / Partially / No)	Response / evidence
1	Operational capability, governance sustainability, supplier-management, and delivery arrangements have been considered (see Table 3 to Table 8)		
2	Existing organisational governance and assurance arrangements capable of supporting the deployment have been identified (see Table 3 to Table 7)		
3	The organisation has identified where additional legal, governance, operational, procurement, safeguarding, privacy, security, or specialist support may be required (see Table 3 to Table 8)		

Before progressing to Step 3, organisations should review the outcomes recorded in Table 8 and Table 9.

Attention should be given to readiness considerations in rows 1, 2, 3 in Table 8 and row 4 in Table 9 that have been assessed as "Partially" or "No".

Organisations should not normally progress to Step 3 until:

- the intended purpose and scope of the deployment are clearly defined
- governance responsibilities, accountability, operational ownership, and escalation arrangements have been identified
- data handling, sharing, retention, deletion, and lifecycle considerations have been reviewed
- any legal, governance, privacy, security, safeguarding, procurement, operational, or specialist support requirements have been identified.

Where significant gaps remain unresolved, organisations should consider whether:

- additional review is required before deployment progresses
- existing governance or assurance functions should be engaged
- deployment scope or operational reliance should be reconsidered
- additional safeguards, transparency measures, oversight, or operational controls may be required.

2.3.1 Step 2 Outcome

Table 10 Step 2 outcome

Outcome	Recorded by	Date
Proceed to Step 3 (Governance classification and use case assessment) with readiness matters requiring further consideration		

By completing Step 2, organisations should now have:

- a clearer understanding of the intended IoT deployment and its operational purpose
- an understanding of organisational readiness, governance capability, operational sustainability, accountability, and transparency considerations associated with the proposed deployment
- reviewed existing governance, operational, assurance, legal, privacy, safeguarding, procurement, transparency, and oversight arrangements that may support the deployment
- identified any governance, operational, oversight, transparency, resourcing, skills, supplier-management, or organisational capability gaps that may affect deployment
- identified where additional governance, legal, operational, safeguarding, security, procurement, privacy, or specialist support may be required
- considered how existing organisational governance and assurance processes may need to be strengthened, adapted, coordinated, or applied to support IoT deployment appropriately

Step 2 is intended to help organisations prepare for subsequent governance classification, deployment assessment, and governance implementation activities.

Step 2 does not:

- determine governance levels or governance outcomes
- replace existing governance, legal, operational, procurement, privacy, safeguarding, or assurance processes
- determine whether deployment is appropriate, lawful, justified, or permissible
- remove the need for reassessment, escalation, or ongoing governance review over time

Step 3 introduces governance classification and use case assessment processes to help organisations understand the potential governance implications associated with the proposed IoT deployment.

3 Step 3 - Governance Classification and Use Case Assessment

Figure 5 Introducing Step 3's purpose, outputs and relevant principles



Step 3 helps organisations assess the likely governance implications associated with a proposed IoT deployment based on:

- the intended purpose of the deployment
- the operational context in which the deployment will operate
- the way IoT data and outputs may be used in practice
- the potential impact on tenants, living environments, operational decision-making, or tenancy-related activity
- whether use cases are combined, expanded, or subject to future change-of-use

This step introduces the governance classification approach used within the handbook and supports organisations in identifying the indicative level of governance, oversight, transparency, safeguards, reassessment, and organisational accountability that may become appropriate for a deployment.

This step helps organisations to:

- understand the potential governance implications associated with different IoT use cases and deployment contexts
- apply governance consistently and proportionately across deployments
- identify where governance expectations may increase due to operational context, tenant impact, combined use cases, inference, operational reliance, or evolving deployment use over time
- identify where additional governance capability, specialist input, safeguards, oversight, or reassessment may become appropriate
- support more consistent, transparent, auditable, and defensible deployment decision-making

The handbook uses Governance Levels to help organisations understand the maximum reasonably foreseeable governance exposure associated with a deployment and its intended use.

Governance Levels are intended to help organisations:

- understand the level of governance, oversight, safeguards, transparency, reassessment, and accountability that may become appropriate for a deployment
- apply governance proportionately and consistently across different deployment contexts
- identify where additional governance capability, oversight, safeguards, or specialist input may be required
- support more transparent, auditable, and defensible deployment decision-making
- work alongside existing organisational governance, legal, operational, safeguarding, procurement, privacy, and assurance processes

Governance Levels support governance planning and decision-making throughout the deployment lifecycle and should be interpreted proportionately alongside the intended purpose, deployment context, operational use, safeguards, and organisational controls applied in practice.

Governance classification is driven primarily by the intended purpose and operational use of IoT data and outputs, rather than by the sensor technology itself. The same sensor deployment may result in different governance implications depending on:

- how IoT data is interpreted or acted upon
- the operational use of IoT outputs
- whether data is used for monitoring, inference, prioritisation, enforcement, or decision-support activity
- whether deployments occur within tenanted homes, communal environments, plant rooms, offices, or mixed settings
- whether data is combined with other organisational or partner datasets
- the safeguards, controls, transparency arrangements, and oversight mechanisms applied in practice

Governance Levels associated with use case profiles reflect the maximum reasonably foreseeable governance exposure that could arise if a deployment becomes subject to greater operational reliance, expansion, combined use, different interpretation or a future change of purpose.

Actual governance implementation should remain proportionate to:

- the specific deployment context
- operational purpose and reliance
- tenant impact and expectations
- organisational governance capability
- safeguards and controls applied in practice
- transparency, oversight, and accountability arrangements

Governance escalation reflects the level of governance, oversight, scrutiny, safeguards, reassessment, and accountability likely to become appropriate for the deployment.

Step 3 consists of four stages. First, each use case is assessed to understand how it will operate in practice. Second, the relevant use case profile is applied and the governance classification confirmed. Third, the organisation assesses whether it has the governance capability required to support the classified use case. Finally, the outcomes are reviewed and recorded before progressing to Step 4. The outputs from this step will be used in Steps 4 and 5 to assess deployment context, governance arrangements, safeguards, accountability arrangements, and implementation requirements.

The following sections explain how Governance Levels are applied, how use case profiles should be used, how deployment context may affect governance expectations, and how organisations should identify governance capability gaps, reassessment triggers, and lifecycle governance considerations before proceeding to governance implementation activities.

Organisations should complete Step 3 alongside the findings recorded in Table 8 and Table 9 in Step 2. Any governance gaps, capability gaps, dependencies, governance concerns, or specialist support requirements identified in Step 2 should be considered throughout the governance classification and capability assessment process.

Refer to Annex C.3 (page 238) which provides a set of best practices to assist with completing Step 3, Governance Classification and Use Case Assessment.

3.1 Governance classification overview

This section introduces how governance is assessed for IoT use cases within this handbook. The Governance Levels, Governance Requirements, and capability areas used within this handbook **do not prescribe a specific governance structure, approval model, committee structure, organisational design, or operating model**. Instead, they describe the level of governance capability, oversight, accountability, safeguards, and assurance that organisations should be able to demonstrate. Organisations should determine how these requirements are met through their own governance arrangements.

IoT deployments can vary significantly depending on how data is collected, interpreted, and used in practice. Governance requirements therefore need to be **proportionate to the potential impact of each use case**, particularly where data may relate to homes, households, patterns of living, behaviour, or decisions affecting people.

This section defines the key governance concepts used throughout Step 3.

3.1.1 Governance levels

Governance Levels describe the **relative level of governance exposure associated with a use case**, based on:

- what the data relates to
- how the data is used
- the extent to which the use may affect people, households, or decisions about them

Governance Levels reflect the **maximum reasonably foreseeable governance exposure** associated with a use case, rather than the specific controls currently in place.

Higher Governance Levels indicate that:

- data may reveal patterns, behaviour, or vulnerability
- data may be used to make decisions or prioritise action
- outcomes may directly affect tenants, households, staff, or other individuals

Lower Governance Levels typically relate to:

- monitoring of assets, systems, or environmental conditions
- routine operational activity that does not involve decisions about people

Governance Levels are used in conjunction with use case profiles to determine the appropriate governance expectations.

3.1.2 Lower-impact and higher-impact use

The same use case may operate in **different ways in practice**, depending on how data is used.

- A **lower-impact use** is one in which data remains focused on assets, systems, environments, or routine operational activity and is not used to identify or assess people.
- A **higher-impact use** occurs where data is used in ways that may:
    - reveal patterns of behaviour, occupancy, or vulnerability
    - compare homes, households, or situations
    - support decisions, interventions, or outcomes affecting people

The distinction between lower-impact and higher-impact use is central to governance classification and is assessed in Step 3.2.

3.1.3 Governance flags

Governance flags identify the **nature of governance considerations associated with a use case**, based on how the data is used.

A governance flag indicates that a use case:

- involves a particular type of sensitivity
- may require additional scrutiny or safeguards
- may require specific expertise (for example legal, data protection, or safeguarding input)

Examples of governance flags may include use cases where data is used to:

- inform tenancy-related decisions
- support safeguarding or wellbeing activity
- identify or infer behaviour, occupancy, or vulnerability
- support system-led or automated actions

Governance flags do not determine whether a use case can proceed. Instead, they indicate the **type of governance attention required**.

3.1.4 Governance requirements

Governance requirements describe the **minimum governance arrangements expected** for a use case, based on its Governance Level and governance flags.

These may include, for example:

- data protection and legal review (including DPIA where required)
- defined oversight and accountability
- transparency and communication with tenants or stakeholders
- appropriate safeguards and human oversight
- auditability and record keeping

Governance Requirements are identified through the use-case profiles. 3.4 then assesses whether the organisation has the capability needed to meet those requirements.

3.1.5 Legal guardrails

Legal guardrails are **non-negotiable legal or regulatory constraints** that apply to a use case.

These represent:

- legal requirements that must be satisfied before deployment
- boundaries within which IoT data must be collected and used
- situations where additional legal or specialist input is required

Legal guardrails do not describe how to implement governance, but they define what **must be complied with in all cases**.

3.1.6 Consent

Consent should only be relied upon where it is genuinely required and can be obtained lawfully.

In a social housing context, consent should generally be treated as **exceptional**, because it should be:

- freely given;
- specific to the purpose;
- informed;
- unambiguous;
- and capable of being withdrawn at any time.

Where there is a clear imbalance of power between landlord and tenant, it may be difficult to demonstrate that consent has been freely given in a valid way.

For this reason, where a use case may rely on consent, this should be treated as a **trigger for enhanced governance** rather than as a presumption that the use case is permissible. This should include:

- review by a Data Protection Officer or legal specialist
- consideration of whether a DPIA is required
- enhanced transparency and clear explanation to tenants or affected individuals
- meaningful tenant engagement or consultation, where appropriate

Where a use case is only lawful if valid consent exists, organisations should ensure that they have the governance capability to obtain, manage, record, and respond to withdrawal of consent in practice.

3.1.7 How these concepts are used in Step 3

These governance concepts are applied in the following way:

- Step 3.2 identifies how each use case operates in practice, including how data relates to assets, homes, behaviour, or people
- Step 3.3 applies the relevant use case profile to determine:
    - the governance level
    - the governance flag
    - the associated governance requirements and legal guardrails
- Step 3.4 assesses whether the organisation has the governance capability in place to meet those requirements

Together, these steps ensure that IoT deployments are assessed in a way that is **proportionate, consistent, and aligned with governance and legal obligations**.

3.2 Initial deployment context and scaling considerations

This section helps you define how each IoT use case will operate in practice before applying use case profiles.

IoT deployments may involve one or more use cases operating across different environments. Each use case should be considered separately, as governance implications may differ depending on how and where it is deployed.

In this section, you will classify each use case across a set of defined deployment context areas. Organisations will also record the deployment environment, rollout approach and nature of the intended data use for each use case. These outputs provide the deployment context needed to apply the use-case profiles consistently in the following sections.

You are not being asked to assess governance requirements at this stage. Instead, you are identifying how the deployment will operate in practice so that governance classification can be applied consistently in the following steps.

For each use case, you will:

- identify the use case and its purpose
- select the level that best describes how it operates across each deployment context area
- select the highest applicable level where more than one condition applies

Complete the tables in this section separately for each use case identified in Step 1. Where a deployment contains multiple use cases, record the context of each use case rather than assuming that the same answer applies to all of them.

The outputs from this section form a structured description of each use case and will be used directly in subsequent steps to:

- apply use case profiles and determine governance classification (3.3)
- assess governance capability and identify any gaps (3.4)
- identify lifecycle considerations and reassessment triggers (3.5)

Where multiple use cases are deployed together, each should be classified individually.

3.2.1 Deployment environment and tenancy context

This section identifies where each IoT use case will operate.

Complete Table 11 for each use case identified in Step 1:

- enter the description of each use case from Table 1 in the relevant column
- review each deployment environment and record Yes against every environment in which that use case will operate
- select all environments that apply, as a use case may operate across more than one environment
- consider each use case separately, as different use cases within the same deployment may operate in different environments
- add additional use-case columns or duplicate the table where more than two use cases are being assessed.

Select all environments that are relevant. Where a use case operates across multiple environments, record all that apply. Where multiple environments include tenant-facing settings (such as homes or communal areas), this will influence governance considerations in later steps.

Table 11 Deployment environment

Deployment environment	Use Case 1	Use Case 2	Additional use cases (if required)
Use case description (from Step 1 – from Table 1)			
Tenanted homes			
New build homes (homes not yet occupied)			
Void or empty properties (temporarily unoccupied homes)			
Communal or shared residential areas			
Plant rooms or building infrastructure			
Offices or administrative environment			
Operational environments involving staff or mobile workforce – Deployment associated with organisational staff, including mobile or lone worker monitoring			

The environments selected in Table 11 will be used in Step 4 when assessing deployment context, affected individuals, organisational involvement, tenancy considerations, safeguarding considerations, and deployment-specific governance implications.

3.2.2 Rollout approach and scaling

This section identifies how each IoT use case will be introduced across properties, locations, or users. Understanding whether deployment will be phased or implemented at scale helps determine how governance arrangements may need to be established and applied.

For each use case, select the option that best reflects how the deployment will be introduced, using Table 12. Record “Yes “against the rollout approach that applies. Select one of the two options only for each use case. The rollout approach selected for each use case will be used to support interpretation of governance classification in Step 3.3

Table 12 Roll out approach and scaling

Rollout approach and scaling	Use Case 1	Use Case 2	Additional use cases (if required)
Use case description (from Table 1)			
Phased or gradual scale – Deployment is introduced in stages or on a limited basis and may be expanded over time.			
Full operational deployment – Deployment is implemented at scale across the organisation (or a large part of it) and is fully embedded in normal operational activity. The organisation expects consistent and ongoing use.			

The rollout approach identified in Table 12 will be used in Step 5 when considering whether governance arrangements, oversight arrangements, safeguards, accountability arrangements, and governance capability are proportionate to the scale and operational reliance of the deployment.

3.2.3 Nature of data use and potential impact on people

This section helps you to classify each IoT use case according to **what the data relates to** and **what type of outcome that data is used to support**.

The purpose of the use case was defined in Step 1 (from Table 1). This section does not redefine that purpose. Instead, it helps you determine whether the use of the data remains lower-impact or becomes higher-impact because of:

- what the data is about
- whether the data can reveal something about a home, household, patterns of living, behaviour, vulnerability, or occupancy
- whether the data is used only to support routine operational activity, or whether it supports decisions, prioritisation, interventions, or outcomes affecting people

This classification will be used in the next step to apply the relevant use case profile and determine the appropriate Governance Level, governance flag, and associated governance requirements. It must also be recalled that interventions which affect a tenant's legal rights – in relation to access to their home – cannot be taken without recourse to appropriate judicial processes.

Definitions of levels

- **Level 1 – Asset, system, or environmental data not used to identify or assess people.**

  Data is used to monitor assets, systems, or environmental conditions. The data is not used to identify people, infer behaviour, compare households, or support decisions about specific tenants, households, or staff. Any response to the data remains routine and operational.

- **Level 2 – Property or service-level data supporting operational judgement.**

  Data is used to understand conditions within a property, building, or service context and to support operational activity. The data may relate to a home or service setting, but it is not used to identify individuals, infer behaviour, compare households, assign relative risk between cases, or support decisions about people. Staff interpret the data alongside other information to determine an appropriate operational response.

- **Level 3 – Data revealing patterns, behaviour, occupancy, vulnerability, or comparative risk.**

  Data is used in ways that may reveal patterns of use, occupancy, behaviour, vulnerability, or comparative risk between homes, households, or situations. The data may be used to prioritise action, escalate activity, or direct attention to particular cases. At this level, the use moves beyond routine operational support and begins to relate to patterns of living, comparative judgement, or higher-risk decision-making.

- **Level 4 – Data used to support interventions, decisions, or outcomes affecting people.**

  Data is used to support interventions, decisions, or outcomes that directly affect tenants, households, staff, or other individuals. This includes use where IoT data is linked to actions relating to tenancy management, safeguarding, wellbeing, access, enforcement, or other decisions about people. At this level, the data is no longer only about assets, systems, or environments; it is being used in ways that can (where due legal process is followed) materially affect people or decisions made about them.

In Table 13- for each use case:

- enter the use case description from Step 1 (from Table 1);
- select the level (1-4) statement that best reflects how its data and outputs will be used;
- select only one level; and
- where more than one level appears relevant, select the highest applicable level.

When deciding between Level 2 and Level 3, select Level 3 if the data is used to:

- compare homes, households, or situations
- identify higher-risk cases or assign relative risk
- infer patterns of behaviour, occupancy, or vulnerability
- direct attention or resources toward specific homes or households

In some cases, particularly where it is unclear whether data may reveal behaviour, occupancy, vulnerability, or be linked to identifiable individuals, you should seek input from relevant governance specialists within your organisation (for example, a Data Protection Officer, data

governance lead, or legal advisor). This helps ensure that the classification accurately reflects the nature of the data use and the potential impact on people.

If there is uncertainty between levels, select the higher level.

Table 13 Data use and outcomes

Level	Use Case 1	Use Case 2	Additional use cases (if required)
Use case description (from Step 1 – from Table 1)			
Level 1			
Level 2			
Level 3			
Level 4			

The level selected in Table 13 will influence subsequent consideration of deployment context, governance arrangements, transparency expectations, human oversight requirements, safeguards, and accountability arrangements in Steps 4 and 5.

3.3 Applying use case profiles

This section applies the relevant use case profiles to each proposed IoT use case to determine the associated governance classification.

Use case profiles provide a structured way of identifying the governance implications of different IoT uses. Each use-case profile identifies (Annex A – page 173)

- the **governance flags** associated with the use case
- the corresponding **governance level**
- the associated **governance requirements**
- any applicable **legal guardrails**

3.3.1 Selecting the relevant use case profile

For each use case, you should identify the **use case profile that best reflects the intended purpose of the deployment and how IoT data is used in practice**.

The selected profile should align with:

- the primary purpose of the use case, as defined in Step 1 – from Table 1
- how IoT data and outputs are intended to be used
- the nature of the outcomes the use case is designed to support

Where the purpose of a use case is clear and well-defined, it should normally correspond directly to a single use case profile.

Where a use case could align to more than one profile:

- select the profile that best reflects the **main intended use**

- consider whether any **secondary uses**, combined use cases, or future expansion may require additional profiles to be taken into account

The selected use case profile should reflect the intended operational use being assessed. Possible future uses should not be included unless they form part of the defined deployment. Any later change or expansion should be reassessed through the handbook.

Selection of the appropriate use case profile should be informed by:

- those responsible for **service delivery and operational use**, who understand how the use case will function in practice
- relevant **governance specialists**, such as a Data Protection Officer, data governance lead, or legal advisor, who can interpret the potential governance implications of the data use

This helps ensure that both the **practical operation of the use case** and the **potential impact of the data use** are fully understood.

3.3.2 Interpreting governance flags in context

Use case profiles define the **governance flags** associated with each type of use. These flags indicate the **nature of the governance considerations** that may apply.

When selecting the use case profile, you should also consider whether these governance flags apply in practice, based on how the use case will operate.

You should consider whether the use of IoT data may:

- relate to tenants, households, or staff
- reveal patterns of behaviour, occupancy, or vulnerability
- be used to compare cases or identify higher-risk situations
- support decisions or actions affecting people.

Where the use case operates in ways that trigger these conditions, the corresponding governance flags should be treated as applicable. However, where there is uncertainty, the more precautionary interpretation should be taken.

Where a use case involves comparing homes or households, identifying higher-risk situations, or inferring patterns of behaviour or occupancy, you should **carefully consider** whether a profile associated with **higher-impact** use is more appropriate.

In these situations, the choice of profile is especially important, as it may significantly affect the governance classification.

For each use case, use Table 14 and enter:

- the use-case description recorded in Table 1
- the name of the selected profile from Annex A
- a brief explanation of why that profile reflects the intended purpose and use of outputs.

If additional use cases are being assessed, add further columns or duplicate the table.

Table 14 Use case profile confirmation

Use case profile selection	Use Case 1	Use Case 2	Additional use cases (if required)
Use case description (from Table 1)			
Select the use case profile			
Basis for the selection			

The **basis for selection** should briefly explain:

- why the chosen profile best reflects the intended use
- how the data is expected to be used in practice
- whether and how governance flags are considered to apply
- any relevant assumptions about behaviour, occupancy, or outcomes
- whether any secondary uses, combined uses, or future developments have been considered

The selected profile should be reviewed to ensure it accurately reflects how the use case will operate in practice. Where there is uncertainty, input from appropriate governance or legal specialists should be obtained before proceeding.

Once Table 14 has been completed, use the selected profile to confirm the Governance Level, Governance Flag(s), Governance Requirements and Legal Guardrails in Table 15.

3.3.3 Confirming the governance classification

Using the selected use case profile recorded in Table 14 and the initial interpretation of Governance Flags set out in Section 3.3.1, you should now confirm the governance classification for each use case

This step consolidates the outputs from the selected use case profile into a clear and consistent set of governance expectations.

At this stage:

- the use case profile acts as the **source of truth** for the governance classification
- your task is to **record the relevant outputs from the profile** and **confirm that they accurately reflect how the use case will operate in practice**

Confirming governance level

The Governance Level should be **taken directly from the selected use case profile**.

The Governance Level represents the **maximum reasonably foreseeable governance exposure** associated with the use case and should be interpreted as:

- the level of governance the organisation, and any delivery partners, must be prepared to operate within
- reflecting how the data is used and the potential impact on people
- not the level of governance currently in place

The Governance Level should be copied directly from the selected profile. If users conclude that the profile does not accurately reflect the intended use, they should revisit the profile selection rather than manually changing the Governance Level.

Confirming governance flags

Governance flags should be taken directly from the selected use case profile.

Each profile defines the primary governance consideration associated with that type of use. This flag should be treated as applicable for the use case.

At this stage, you are not determining whether the governance flag applies. Instead, you are confirming how that governance consideration applies in practice, based on how the use case operates.

This should be considered alongside whether the use represents a lower-impact or higher-impact application, which affects the level of governance required to address the flagged consideration.

Recording governance requirements and legal guardrails

The governance requirements and legal guardrails should be **taken directly from the selected use case profile**.

These define:

- the minimum governance arrangements expected for the use case
- any legal or regulatory constraints that must be satisfied
- where enhanced safeguards, oversight, or specialist input may be required

At this stage, you are identifying **what governance is required**, rather than assessing whether these requirements are currently in place.

Confirming lower-impact and higher-impact use in practice

Where the selected use case profile includes both lower-impact and higher-impact use scenarios, you should confirm how the use case operates in practice.

This assessment should be based on a clear understanding of:

- how IoT data is used in operational workflows
- whether data is interpreted, compared, or used to prioritise cases
- whether data may reveal patterns of behaviour, occupancy, or vulnerability
- whether outputs influence decisions or actions affecting tenants, households, or staff

Determining whether the use represents lower-impact or higher-impact use should be informed by:

- those responsible for **service delivery and operational use**, who understand how data is used in practice
- relevant **governance specialists**, such as a Data Protection Officer, data governance lead, or legal advisor, who can interpret whether the data use introduces additional governance sensitivity

This distinction cannot be made based on data collection alone and depends on how the data is used in practice.

Where the intended use involves any of the following factors:

- comparing homes or households
- identifying higher-risk situations
- inferring patterns of behaviour, occupancy, or vulnerability
- supporting decisions or actions affecting people

the use should be treated as higher impact.

Where there is uncertainty, the more precautionary interpretation should be taken.

Where the current use of IoT data differs from the purpose originally defined in Step 1, organisations should review and update the relevant Step 1 outputs before proceeding. A change in purpose may alter the governance classification, governance requirements, legal guardrails, or governance capability required to support the deployment.

The governance classification must remain consistent with the purpose, intended outcomes, and intended use of data recorded in Step 1. Where a use case has evolved, expanded, or changed in scope since Step 1 was completed, organisations should review the relevant Step 1 outputs before confirming the governance classification.

3.3.4 Recording the governance classification

You should now record the governance classification for each use case, using the selected use case profile as the basis in Table 15, using Annex A (page 173) for the inputs.

Complete Table 15 separately for each use case using the profile selected in Table 14:

- copy the use-case description from the selected use case profile
- record the Governance Level from the selected use case profile
- record the applicable Governance Flags from the selected use case profile
- identify whether the intended use reflects the use case profile's lower-impact or higher-impact example, from the selected use case profile
- summarise the applicable Governance Requirements from the selected use case profile, and
- record the relevant Legal Guardrails from the selected use case profile.

Do not change the Governance Level shown in the selected use-case profile. If the profile does not reflect the intended use, revisit Table 14 before continuing.

Table 15 Governance classification for each use case

Governance classification	Use Case 1	Use Case 2	Additional use cases (if required)
Use case description			
Selected use case profile			
Governance level			
Governance flag			
Lower-impact / higher-impact use (as applied)			
Key governance requirements (summary)			
Legal guardrails			

The governance classification recorded in this section defines the **governance expectations associated with each use case**. Table 15 provides the primary governance classification output of Step 3. The Governance Level, Governance Flags, Governance Requirements, Legal Guardrails, and lower-impact or higher-impact assessment recorded in this table must be used throughout the remainder of Step 3 and carried forward into Steps 4 and 5

These outputs establish what the organisation must be prepared to manage when deploying the use case. They will now be used in the next step 3.4 to assess whether the organisation has the **governance capability required to meet these expectations**, and to identify any gaps that must be addressed before deployment.

3.4 Governance capability and gap assessment

This section helps you assess whether your organisation has the **governance capability required** to support each proposed IoT use case.

In Section 3.3, you applied the relevant use case profiles and confirmed the governance classification for each use case, including:

- the governance level
- the governance flag
- the associated governance requirements
- any legal guardrails.

These outputs define the **level of governance exposure that the organisation, and any delivery partners, must be prepared to manage**.

The purpose of this section is to determine **whether the organisation currently has governance arrangements in place that are aligned with those requirements**

This includes assessing whether governance is:

- in place and clearly defined
- proportionate to the level of impact identified
- consistently applied in practice
- supported by appropriate oversight, safeguards, and expertise.

This section does not determine whether a deployment should proceed. Instead, it identifies:

- whether governance capability is **sufficient**
- where there are **gaps or weaknesses**
- what arrangements need to be **strengthened or established** before deployment or scaling

Governance capability should be assessed across a set of **core governance areas**, reflecting the key controls and safeguards required to support IoT deployments.

This assessment should consider:

- the Governance Level associated with each use case
- the nature of the governance flag and what it indicates about data use
- whether the use represents lower-impact or higher-impact operation in practice

Where governance capability is not aligned with what is required, actions should be identified to address those gaps. This may include:

- strengthening internal governance processes
- introducing additional safeguards or oversight
- seeking input from governance, legal, or specialist functions

The outputs from this section provide a clear view of:

- governance capability currently in place
- governance capability required
- gaps that must be addressed

These findings will be carried forward into Steps 4 and 5 when assessing the intended deployment and defining the governance arrangements required before deployment.

Any governance capability gaps identified in this section should be carried forward into Step 5. Step 5 considers how governance arrangements, oversight mechanisms, safeguards, accountability arrangements, and organisational responsibilities should be established or strengthened before deployment proceeds.

3.4.1 Assessing governance capability

This section explains how to assess whether your organisation has the **governance capability required** to support each proposed IoT use case.

Using the governance classification confirmed in Section 3.3, you should now assess whether governance arrangements are in place that are **aligned with what is required in practice**.

Scope of organisational responsibility

For the purposes of this assessment, "the organisation" should be understood to include:

- the organisation leading the deployment (for example, the housing provider or council)
- any delivery partners involved in the deployment or operation of the solution (such as technology suppliers or service providers)
- any organisations that receive, use, or act on IoT data or outputs (for example, health or social care partners)

Where IoT solutions are delivered in partnership, governance capability should be considered across the **full end-to-end use of the data**, rather than within a single organisation in isolation.

This includes considering:

- how governance responsibilities are distributed across organisations
- whether roles and accountabilities are clearly defined and agreed
- whether governance arrangements operate effectively across organisational boundaries

Approach to assessing capability

For each use case, compare the governance expectations recorded in Table 15 with the governance capability currently available across the organisations involved in the deployment.

Assessing “required” vs “current” capability

For each governance area, you should consider:

- what level of governance capability is **required**, based on the governance classification
- what level of governance capability is **currently in place across all organisations involved**
- whether there is a **gap between the two**

This comparison is critical in identifying whether the organisation, and any delivery or service partners, have the capability to:

- operate within the Governance Level identified
- address the governance considerations indicated by the governance flag
- apply appropriate **oversight, safeguards, transparency, and accountability** for how IoT data is used
- meet the governance requirements and legal guardrails associated with the use case

Considering deployment stage and scaling

When assessing governance gaps, you should consider how the use case will be deployed and scaled in practice.

Where a use case is being introduced on a **phased or limited basis**:

- it may be appropriate for certain governance capabilities to be **developed or strengthened as the deployment progresses**
- any identified gaps should be clearly defined and actively managed as part of the deployment plan

However, this is only appropriate where:

- the level of impact is proportionate
- risks are understood and controlled during early stages
- there is a clear plan to achieve the required level of governance capability before scaling

Where a use case is intended to be deployed **at scale**, or where it involves **higher-impact use**:

- governance capability should be **fully in place before proceeding with deployment**
- any gaps identified should be addressed prior to rollout

This is particularly important where the use involves:

- data relating to tenants, households, or staff
- patterns of behaviour, occupancy, or vulnerability
- decisions or actions affecting people

In all cases, organisations should ensure that governance capability evolves in line with:

- the scale of deployment
- the level of operational reliance on IoT data
- the potential impact on people and outcomes

Scope of the assessment

Governance capability should be assessed across the full range of activities required to support the use case, including:

- oversight and decision-making
- legal and data protection processes
- communication and engagement with tenants, residents, or staff
- operational use of data and decision-making processes
- monitoring, audit, and assurance
- safeguards to manage risk and prevent misuse

This assessment should reflect how the use case is expected to operate in practice, including:

- the role of IoT data in operational workflows
- the extent to which data informs, influences, or determines decisions
- the potential impact on tenants, households, staff, or outcomes relating to them

Proportionate assessment

The depth and detail of the assessment should be proportionate to:

- the Governance Level associated with the use case
- whether the use represents lower-impact or higher-impact operation
- the nature of the governance flag and what it indicates about data use

Use cases involving data that may relate to behaviour, occupancy, vulnerability, or decisions affecting people will typically require a more detailed and rigorous assessment.

Using the governance capability framework

The following section provides a structured framework for assessing governance capability across key governance areas.

You should use this framework to:

- determine the level of governance capability required
- assess the level of capability currently in place
- identify any gaps that must be addressed

This structured assessment will provide a clear and consistent view of whether governance capability is sufficient to support the proposed use case, and where further action is required before deployment or scaling.

3.4.2 Governance capability framework

This section defines the **governance capability required** to support IoT deployments across a set of core governance areas. The outcomes from this section should be captured in Table 16.

These governance areas represent the key controls, processes, and safeguards that organisations must be able to apply to operate within the governance classification recorded in Table 15.

This framework is used to:

- define what level of governance capability is **required** for each use case
- provide a consistent basis for assessing governance capability
- support the identification of governance gaps in the following section

This section does not assess whether governance capability is currently in place. It defines the **expected level of capability** that organisations must be able to meet.

Capability levels

Governance capability is defined across four levels, reflecting increasing maturity and strength of governance arrangements:

- **Level 1 – Basic capability**
  Limited or initial governance arrangements, typically associated with lower-impact use
- **Level 2 – Established capability**
  Standard governance arrangements are in place and applied consistently
- **Level 3 – Enhanced capability**
  Strong governance arrangements, including increased oversight, scrutiny, and assurance, typically associated with higher-impact use
- **Level 4 – Advanced capability**
  Comprehensive and formal governance arrangements, with the highest levels of oversight, accountability, and control

These levels should be interpreted proportionately, based on:

- the Governance Level identified in Table 15
- the governance flag and what it indicates about data use
- whether the use represents lower-impact or higher-impact operation in practice

For each use case, the governance classification confirmed in Table 15 should be used to determine the **level of capability required** across each governance area.

Data protection assessment

It is important to consider whether the organisation has established the appropriate data protection, privacy and information governance arrangements to support the use of IoT data.

This includes assessing legal obligations, identifying and documenting a lawful basis for processing, determining whether a Data Protection Impact Assessment is required, obtaining appropriate specialist input, ensuring transparency obligations are met, and maintaining appropriate governance documentation.

This includes:

- assessing whether a Data Protection Impact Assessment (DPIA) is required
- identifying and documenting a lawful basis for data processing
- obtaining appropriate input from data protection or legal specialists
- identifying where data protection privacy notices, policies and procedures may require drafting or updating prior to data processing taking place
- documenting decisions and rationale, including where a DPIA is not undertaken

This is particularly important where IoT data:

- may relate to individuals or households
- may be linked to identifiable living environments
- may reveal patterns of behaviour, occupancy, or vulnerability
- may be used to support decisions or actions affecting people

Data protection assessment – capability levels

Capture the capability level in Table 16.

- **Level 1 – Basic capability**

Data protection obligations are considered and documented. A DPIA is not normally required, but the rationale for reaching this conclusion is recorded.

  - The organisation has considered whether a DPIA is necessary and has **recorded the rationale** for not undertaking one
  - Basic data protection considerations are documented, such as minor updates to the privacy notice if lower risk personal data is processed as a result of the use case
  - No formal input from data protection or legal specialists is typically required unless the privacy notice or document requiring updates is owned by that individual in the organisation

- **Level 2 – Established capability**

The organisation undertakes a structured assessment of data protection and privacy obligations, including whether a DPIA is required. The organisation evaluates whether the use involves:

  - identifying individuals or households (directly or indirectly)
  - monitoring or observing environments associated with people
  - the potential to infer patterns of behaviour, occupancy, or vulnerability

A DPIA may be undertaken where these factors indicate potential risk. Input from data protection or governance specialists is obtained where appropriate and decisions and rationale are clearly documented, including where no DPIA is undertaken.

As is set out in the introduction section, a lawful basis for data processing will need to be identified and documented and privacy notices, policies and procedures may need to be updated.

- **Level 3 – Enhanced capability**

Formal data protection governance is typically required, including a DPIA where appropriate.

- A DPIA is undertaken to assess risks associated with the use case
- Formal input is obtained from data protection or legal specialists
- Risks relating to data use, inference, and potential impact on people are clearly assessed
- Findings are reviewed through appropriate governance processes
- Senior oversight or sign-off is typically required

- **Level 4 – Advanced capability**

Enhanced data protection governance is required, including a DPIA, formal specialist review, and ongoing oversight arrangements.

- A comprehensive DPIA is undertaken
- Detailed data protection and legal review is carried out
- Consultation under the DPIA may be required
- Risks are subject to enhanced scrutiny, particularly where data may affect individuals or outcomes relating to them
- Formal approval is obtained through senior governance structures, typically at the highest level
- Ongoing review and update of the DPIA is expected, particularly where the use case evolves, scales, or changes in nature. For example, a standing agenda item at the relevant committee within the organisation's governance / risk framework.

Oversight and approval

It is also important to consider whether the organisation has appropriate **oversight, accountability, and approval processes** in place to support the deployment and use of IoT solutions.

This includes ensuring that:

- the use case has clearly defined ownership and governance responsibility
- appropriate review and approval processes are in place
- decisions relating to the use of IoT data are formally considered and documented
- accountability is clear across all organisations involved, including delivery partners
- governance arrangements are maintained as the use case evolves or scales

This governance area is particularly important where IoT data:

- is used to inform operational decisions or prioritisation
- involves comparison between homes or households or identification of higher-risk situations
- supports decisions or actions affecting tenants, households, or staff
- is used across organisational boundaries or shared between services

Oversight and approval – capability levels

Capture the capability level in Table 16.

- **Level 1 – Basic capability**

Documented operational approval is in place (required in all cases).

  - The use case is reviewed and approved at an operational level
  - Responsibility for the use case is identified
  - Governance arrangements are documented at a basic level
  - Approval is based on standard operational processes, without formal governance or legal review

- **Level 2 – Established capability**

Governance review is in place.

  - The use case is subject to structured governance review, which may include data protection, information governance, or digital oversight functions
  - Governance responsibilities are more clearly defined
  - Decisions are reviewed through standard organisational governance processes
  - Input from governance or specialist teams is obtained where appropriate

- **Level 3 – Enhanced capability**

Legal review and senior sign-off are in place.

  - The use case is subject to formal governance processes, including consideration of outputs from relevant governance, legal, data protection or specialist reviews
  - Governance risks and implications are explicitly assessed
  - Senior stakeholders are involved in reviewing and approving the use case
  - Named accountability is established for governance and decision-making
  - Governance arrangements are clearly documented, consistently applied, and subject to periodic review

- **Level 4 – Advanced capability**

Senior accountability and formal approval structures are in place.

  - The use case is subject to formal approval through senior governance structures
  - Clear accountability is defined at a senior organisational level for how the use case operates and how decisions affecting people are made
  - Governance arrangements are designed to manage high-impact or sensitive use cases
  - Responsibilities are clearly defined and coordinated across all organisations involved
  - Ongoing oversight is maintained, including review as the use case evolves, scales, or changes in nature.

Tenant transparency

This governance area considers whether the organisation provides **clear, appropriate, and proportionate communication to tenants, residents, or other affected individuals** about how IoT technologies are used and how data relating to them may be collected, interpreted, or used.

This includes ensuring that:

- individuals are aware of the use of IoT technologies in their homes or environments
- clear information is provided about:
  - what data is collected
  - how it is used
  - how it may affect tenants, households, or outcomes relating to them
- communication is appropriate to the level of impact and sensitivity of the use case
- engagement takes place where use cases may affect tenant expectations, rights, or interests

Transparency should be maintained throughout the lifecycle of the use case. This includes both:

- initial communication at the point of deployment
- ongoing communication where IoT data is used in ways that affect tenants, households, or outcomes relating to them

Communication should also enable tenants or affected individuals to **understand how IoT data may influence decisions, actions, or outcomes relating to them**, particularly where data is used to prioritise, assess, or intervene.

Transparency is particularly important where IoT data:

- may relate to tenants or households
- may reveal patterns of behaviour, occupancy, or vulnerability
- is used to prioritise, compare, or assess outcomes
- supports decisions or actions affecting people

Transparency increases with impact, ranging from general awareness to active engagement and consultation where use cases affect tenant expectations or rights. In all cases, clear communication with tenants or affected individuals is required.

Transparency arrangements should reflect the **different needs and circumstances of tenants or affected individuals**. This includes ensuring that communication is accessible, understandable, and appropriate for a diverse range of people, including:

- those for whom English is a second language
- those with additional needs or vulnerabilities
- elderly individuals
- those living in supported or assisted environments

Transparency arrangements should also reflect the **nature of the housing or living context** in which the use case operates. This is particularly important where use cases are deployed in:

- supported housing
- temporary accommodation
- accommodation used by homeless people
- assisted living environments
- properties where occupancy or habitation may be uncertain (for example, void properties)

In these contexts, organisations should consider:

- how communication can be delivered fairly and appropriately
- whether standard tenant communication approaches are sufficient
- whether IoT data may affect people even where a formal tenancy relationship is not in place
- whether the use of IoT data to infer occupancy, presence, or patterns of habitation may have implications for individuals

Where IoT solutions are delivered or operated in partnership with other organisations, transparency arrangements should ensure that communication is **coordinated across those organisations**.

Tenants, residents, or other affected individuals should be able to understand:

- which organisation is responsible for the deployment
- which organisation collects or receives the data
- which organisation interprets or acts on IoT outputs
- who to contact if they have questions or concerns

Where multiple organisations are involved, communication should be **consistent, joined-up, and proportionate to the level of impact**.

Organisations should ensure that transparency arrangements are **clearly defined, documented, and consistently applied in practice**.

This includes identifying:

- how communication is delivered
- how different tenant groups are supported
- how ongoing communication is maintained
- how responsibilities are managed where multiple organisations are involved

Tenant Transparency – capability levels

Capture the capability level in Table 16.

- **Level 1 – Basic capability**

General awareness is provided.

  - Tenants or affected individuals are made aware that IoT technologies are in use
  - Basic information is provided, for example through notices or general communications
  - Communication explains the presence and purpose of the technology at a high level

- **Level 2 – Established capability**
    - Clear communication and explanation are provided. Information is provided about:
        - what data is collected
        - how it is used
        - the purpose of the deployment
    - Communication is clear, accessible, and relevant to the audience
    - Tenants or affected individuals can understand how IoT technologies relate to their home or environment
    - Communication is adapted, where needed, to ensure it is accessible and appropriate to different tenant groups
- **Level 3 – Enhanced capability**

Enhanced transparency and tenant engagement are in place.

- More detailed information is provided about how IoT data is interpreted and used in practice
- Communication reflects the potential for:
    - patterns of behaviour, occupancy, or vulnerability to be identified
    - prioritisation or comparison between cases
- Tenants or affected individuals are actively engaged, where appropriate, including opportunities for:
    - questions
    - feedback
- Engagement approaches reflect the needs of different tenant groups, including those who may require additional support to understand how data is used
- Communication approaches take account of different housing contexts, including supported, temporary, or unstable accommodation
- Where multiple organisations are involved, communication and engagement are coordinated so that tenants or affected individuals receive clear and consistent information about how data is used and by whom
- Ongoing communication is maintained where data use may affect tenants or households.

- **Level 4 – Advanced capability**

Active consultation and clear justification are in place.

- Tenants or affected individuals are actively consulted where the use case may affect:
  - expectations of privacy
  - how their home or behaviour is understood
  - decisions or actions affecting them
- Clear justification is provided for the use of IoT technologies and how data is used
- Consultation and engagement approaches are inclusive and designed to ensure that all tenant groups, including those who may be more vulnerable or harder to reach, are able to participate meaningfully
- Transparency arrangements explicitly address situations where occupancy, habitation, or vulnerability may be uncertain, and where IoT outputs may be used in ways that affect people outside a standard tenancy model
- Consultation and justification arrangements clearly explain the role of each organisation involved in the deployment, including who collects data, who acts on it, who is accountable for decisions or interventions affecting people, and the legal processes that will be followed before such decisions or interventions affecting people are implemented
- Ongoing communication and engagement are maintained, proportionate to the level of impact
- Transparency arrangements support trust, accountability, and informed understanding of outcomes arising from IoT data use

Human oversight

This governance area considers whether the organisation has appropriate **human review, judgement, and intervention processes** in place to ensure that decisions, actions, or outcomes informed by IoT data are **not made solely on automated outputs**, particularly where they may affect tenants, households, or staff.

This includes ensuring that:

- IoT data is interpreted and used within clearly defined operational contexts
- individuals are responsible for reviewing and acting on IoT outputs where required
- decisions are subject to appropriate **human judgement, oversight, and accountability**
- automated processes are proportionate and do not replace necessary human review
- roles and responsibilities are clearly defined across all organisations involved

Human oversight is particularly important where IoT data:

- may be used to prioritise cases or resources
- may indicate patterns of behaviour, occupancy, or vulnerability
- may trigger alerts, escalation, or intervention
- may inform decisions or actions affecting tenants, households, or outcomes relating to them

The level of human oversight required should be proportionate to:

- the Governance Level identified in Table 15
- the governance flag and what it indicates about data use
- the extent to which IoT data is relied upon in decision-making

This includes ensuring that individuals involved in interpreting and acting on IoT data have an appropriate understanding of how the data is generated, what it represents, and its limitations. This may require coordination between operational teams and governance, data protection, or legal specialists.

In all cases, organisations should ensure that:

- decisions affecting people are **understood, explainable, subject to appropriate review, and do not replace necessary judicial processes**
- individuals involved in interpreting and acting on IoT data have sufficient understanding and authority
- responsibility for oversight is clearly defined, including where multiple organisations are involved
- **decisions and the role of human oversight in those decisions are documented where appropriate**, particularly where IoT data informs actions affecting tenants, households, or staff

Human Oversight – capability levels

Capture the capability level in Table 16.

- **Level 1 – Basic capability**

Limited human oversight, proportionate to impact.

  - IoT data is used to support simple operational awareness or monitoring
  - Outputs are reviewed at a basic level where required
  - Decisions are not dependent on IoT data alone
  - Human involvement is minimal but sufficient for the level of impact

- **Level 2 – Established capability**

Routine human review is in place.

  - IoT outputs are subject to **regular review by relevant teams**
  - Clear roles are defined for interpreting and acting on data
  - Human judgement is applied to decisions informed by IoT data
  - Automated outputs do not result in actions without appropriate human consideration

- **Level 3 – Enhanced capability**

Explicit human judgement is required.

  - IoT outputs are **actively interpreted by qualified or authorised individuals**
  - Decisions or actions affecting tenants, households, or staff require **explicit human judgement**
  - Clear processes are in place to ensure data is interpreted consistently and appropriately
  - **Processes support consistent and proportionate decision-making across similar cases**
  - Individuals responsible for decisions understand:
    - the limitations of IoT data
    - the potential for inference or error
    - the need to obtain a court order before certain decisions can be implemented
  - Individuals responsible for interpreting IoT data are supported with appropriate guidance, training, or input from governance, data protection, or legal specialists where required
  - Human oversight is embedded in operational workflows

- **Level 4 – Advanced capability**

Strong human oversight is in place.

  - Decisions affecting tenants, households, or staff are **not taken solely on automated outputs**
  - Robust processes ensure that all significant decisions are:
    - reviewed
    - challenged where necessary
    - clearly justified
  - Human oversight is **systematic, documented, and consistently applied**
  - Accountability is clearly defined for decision-making and intervention, including at a senior level where appropriate
  - Oversight arrangements are designed to manage:
    - high-impact use cases
    - vulnerability and safeguarding considerations
    - complex or multi-organisational deployments
  - Oversight arrangements ensure that decision-making is supported by appropriate expertise, including input from operational, governance, and legal functions where required, particularly in complex or high-impact use cases
  - Ongoing review ensures that reliance on IoT data remains proportionate as the use case evolves or scales

Audit, evidence and assurance

This governance area considers whether the organisation has appropriate arrangements in place to **record, evidence, and demonstrate how IoT use cases are governed, implemented, and operated in practice**.

This includes ensuring that:

- key decisions, actions, and governance processes are **documented**
- there is a clear and auditable record of how use cases have been:
  - defined
  - assessed
  - approved
  - implemented

- organisations can demonstrate that governance requirements have been **applied consistently and proportionately**
- records are sufficient to support:
    - internal review
    - external scrutiny
    - accountability to tenants, partners, and regulators
- responsibilities for maintaining audit and evidence processes are clearly defined, including across multiple organisations where applicable

Audit, evidence, and assurance are particularly important where IoT data:

- is used to inform decisions or actions affecting tenants, households, or staff
- involves inference, behaviour, or vulnerability
- is used across organisational boundaries or by multiple delivery partners
- may be subject to **challenge, review, or scrutiny**

Audit and evidence arrangements should cover the full lifecycle of the use case, including the definition, governance classification, approval, deployment, operation, and any subsequent changes or reassessment.

Audit and evidence arrangements should clearly define roles and responsibilities for both the design and operation of audit processes. This includes identifying who is responsible for establishing audit and evidence requirements, who is responsible for recording and maintaining evidence in practice, and who is responsible for reviewing and assuring that evidence. In many cases, this will require coordination between governance, data protection, legal, operational, digital, and assurance functions, as well as delivery partners where relevant.

In all cases, organisations should ensure that:

- governance decisions are **traceable and explainable**
- appropriate records are kept demonstrating how:
    - Governance Levels were applied
    - governance flags were considered
    - legal guardrails and requirements were addressed
- evidence reflects how the use case operates **in practice**, not just in policy or design
- decisions and the role of audit and evidence processes in supporting those decisions are documented where appropriate, particularly where IoT data informs actions affecting tenants, households, or staff

Audit, evidence and assurance – capability levels

Capture the capability level in Table 16.

- **Level 1 – Basic capability**

Basic documentation is in place.

  - Key aspects of the use case are documented at a high level
  - Decisions are recorded in a limited or informal way
  - Basic records exist to describe the purpose and operation of the use case
  - Documentation may be incomplete or not consistently applied

- **Level 2 – Established capability**

A standard audit trail is in place.

  - Decisions relating to the use case are **consistently documented**
  - A clear audit trail exists for:
    - governance classification
    - approvals
    - key actions taken
  - Documentation is maintained using standard organisational processes
  - **Responsibility for maintaining records and audit trails is clearly defined across relevant teams**, including operational and governance functions

- **Level 3 – Enhanced capability**

Strong auditability and decision records are in place.

  - Detailed records are maintained for all key governance decisions, including:
    - how IoT data is interpreted and used
    - how decisions affecting tenants or households are made
  - Documentation supports **clear traceability** between:
    - inputs (data and alerts)
    - decisions
    - actions taken
  - Records are sufficiently robust to support:
    - internal audit
    - governance review
  - Documentation is applied consistently across similar use cases
  - Documentation supports traceability from initial deployment through to operational use and decision-making
  - Responsibilities for documenting decisions and maintaining auditability are consistently applied across operational and governance teams

- **Level 4 – Advanced capability**
    - Comprehensive evidencing is in place to support scrutiny.
    - Governance and operational decisions are fully evidenced and demonstrable
    - Records are structured and maintained to support:
        - internal audit
        - external scrutiny
        - regulatory or legal challenge where required
    - Clear evidence exists to show that:
        - governance processes have been followed
        - decisions are proportionate and justified
        - safeguards have been applied appropriately
    - Documentation supports:
        - accountability at a senior level
        - assurance across multiple organisations where relevant
    - Audit and evidence arrangements are **reviewed and updated over time**, particularly as the use case evolves or scales

Safeguards

This governance area considers whether the organisation has appropriate **controls, protections, and limitations** in place to ensure that IoT technologies and data are used **safely, proportionately, and within defined boundaries**.

This includes ensuring that:

- data collection and use are **limited to clearly defined purposes**
- controls are in place to prevent **misuse, overreach, or unintended use of data**
- access to IoT data and systems is appropriately **restricted and managed**
- safeguards are applied to protect tenants, households, and staff from **harm, intrusion, or unfair impact**
- risks associated with IoT deployment are **actively managed and mitigated in practice**
- safeguards are consistently applied across all organisations involved in the deployment

Safeguards are particularly important where IoT data:

- may involve monitoring within the home or private environments
- may enable **behavioural inference or profiling**
- may relate to **vulnerability, health, or wellbeing**
- may be used to inform decisions or actions affecting people
- may be combined with other datasets or systems

In all cases, organisations should ensure that:

- safeguards are **clearly defined, documented, and proportionate** to the level of impact
- controls are in place to ensure that IoT data is **not used beyond its intended purpose**
- safeguards are actively **embedded in operational processes**, not just defined in policy
- responsibilities for implementing and maintaining safeguards are clearly defined, including across multiple organisations where relevant

Safeguards should also be supported by clearly defined **roles and responsibilities**. This includes identifying who is responsible for designing, implementing, monitoring, and reviewing safeguards in practice, and who can provide specialist advice where needed. Depending on the use case, this may require coordination between operational teams, governance and data protection functions, legal advisors, digital or technical teams, suppliers, and partner organisations.

Where IoT solutions are delivered or operated in partnership with other organisations, safeguards should be **clearly agreed, coordinated, and consistently applied across those organisations**. This includes ensuring that responsibilities are defined, controls are compatible, and all organisations involved understand how safeguards operate in practice and who is responsible for maintaining them.

Safeguards should also consider the role of **technology suppliers and system design** in determining how data is collected, processed, and used. Organisations should ensure that IoT solutions are designed and configured to support **proportionate data use**, including limiting unnecessary data collection and preventing the generation of data that could enable unintended behavioural inference or profiling.

Safeguards – capability levels

Capture the capability level in Table 16.

- **Level 1 – Basic capability**

Basic controls are in place.

  - Data collection is limited to the immediate operational purpose
  - Simple controls exist to prevent obvious misuse
  - Access to systems and data is restricted internally at a basic level
  - Safeguards are applied inconsistently or vary between use cases

- **Level 2 – Established capability**
    - Standard safeguards are in place.
    - Purpose limitation is clearly defined and applied
    - Internal access controls are implemented and consistently used
    - Basic controls exist to prevent:
        - misuse
        - unintended data sharing
    - Safeguards are supported by standard organisational processes and policies
    - Responsibility for safeguards is defined
- **Level 3 – Enhanced capability**

Enhanced safeguards are in place and actively applied.

- Safeguards are designed to address:
    - behavioural inference
    - vulnerability
    - potential impact on tenants or households
- Controls are in place to prevent:
    - unauthorised use
    - profiling or inference beyond defined purpose
    - inappropriate combination of datasets
- Safeguards are consistently applied across similar use cases
- Processes are in place to ensure safeguards are **understood and applied consistently by operational teams**
- Controls ensure that systems are configured to **limit unnecessary data collection and reduce the risk of unintended inference beyond the defined purpose**
- Safeguards are embedded into operational workflows and decision-making

- **Level 4 – Advanced capability**

Comprehensive and tightly controlled safeguards are in place.

  - Safeguards are designed to manage:
    - high-impact monitoring
    - sensitive or intrusive data use
    - vulnerability and safeguarding considerations
  - Strong controls ensure that IoT data:
    - cannot be used beyond its defined purpose
    - cannot be repurposed without reassessment
  - Safeguards are **systematically applied, reviewed, and enforced**
  - Safeguards are supported by appropriate expertise, including operational, governance, and legal input where required
  - Controls are in place across all organisations involved in the use case
  - Responsibilities for implementing, monitoring, and enforcing safeguards are clearly defined across all organisations involved, with access to appropriate operational, governance, legal, or technical expertise where required
  - Where partner organisations are involved, safeguards are **formally agreed, coordinated, and monitored across organisational boundaries**, including who is responsible for applying them, how compliance is checked, and how failures or exceptions are escalated
  - Safeguards are reflected in **system design, configuration, and supplier arrangements**, so that data collection and processing remain inherently proportionate and controlled
  - Safeguards are regularly reviewed and updated as the use case evolves or scales

The capability levels defined above provide a **common reference point**. In the next section, you will assess how these levels apply to your organisation and each identified use case. This assessment will help determine whether the governance capability available is sufficient to support the proposed deployment and identify any areas where governance arrangements, oversight mechanisms, safeguards, accountability arrangements or organisational responsibilities may need to be strengthened before deployment proceeds.

3.4.3 Assess current governance capability

This section supports you to assess whether your organisation currently has the appropriate level of governance capability in place to support each IoT use case.

You should complete this assessment separately for each use case profile identified Table 15. This ensures that governance is applied proportionately, based on the specific characteristics, intended purpose and practical implications of each use case.

The purpose of this section is to confirm, for each governance area:

- the capability level required for the use case
- the capability level currently in place in practice
- whether current capability is sufficient to support the use case
- who owns or leads that governance area within the organisation

This assessment provides a clear view of whether your organisation is currently able to support the use case at the level of governance capability required.

It is not intended to capture detailed implementation actions, full evidence logs, or complete role mapping. Where capability is not sufficient, the necessary governance arrangements, ownership and actions should be addressed in Step 5.

In some cases, a single IoT deployment may support more than one distinct operational purpose. Where those purposes have different governance implications, each purpose should be assessed separately as its own use case profile. This helps ensure that the required level of governance is assessed proportionately for each use case, rather than assuming one assessment is sufficient for all purposes.

How to complete this assessment (table 16):

- Firstly, input the use case profile name from Table 15.
- For the use case identified, review each governance area in the table and complete all columns using the capability level definitions set out in Section 3.4.2.

For each governance area, you should:

- identify the required capability level (1–4) based on:
    - the outcome of Section 3.3 which is Table 15, and
    - the nature and sensitivity of the use case
- assess the current capability level (1–4) based on what is in place in practice, rather than what is documented in policy alone
- determine whether current capability is sufficient to support the use case (Yes / No)
- identify the role or function that owns or leads this governance area within the organisation

Where you are unsure between levels, select the level that most closely reflects what is consistently achieved and can be demonstrated in practice.

When assessing current capability, you should consider how governance operates day to day, including:

- whether processes are understood and consistently followed
- whether responsibilities are clear and embedded in operational practice
- whether relevant teams can support the use case effectively

Where views differ across teams or functions, the assessment should reflect a shared position based on how capability operates in practice.

You should also consider how governance is delivered in practice, including where capability depends on:

- other internal teams or functions
- external partners or delivery organisations
- technology suppliers or service providers

Where governance relies on others, your assessment should reflect how these arrangements actually operate, not only what is expected contractually or planned. The governance owner identified should remain accountable for ensuring that these arrangements are effective in practice.

If governance ownership is unclear, this should be noted and addressed as part of implementation planning.

“Sufficient” does not mean perfect or fully mature. It means that governance arrangements are appropriate, workable and justifiable in the context of the use case.

This assessment helps you understand whether your organisation is:

- already able to support the use case with confidence, or
- likely to require further governance development or strengthening

Where capability is assessed as not sufficient, this indicates that governance arrangements may need to be clarified, strengthened or extended. This will be addressed in Step 5, where you will consider what changes or actions are required to enable deployment.

This assessment will form the basis for identifying the actions and arrangements required to support implementation in Step 5.

Complete one version of Table 16 for each use-case profile recorded in Table 15. For each governance area:

- identify the required capability level using the definitions in Section 3.4.2
- assess the current capability demonstrated in practice
- record whether current capability is sufficient
- identify the responsible governance owner or function.

Where more than one use case is being assessed, duplicate the table rather than combining different capability requirements in the same response.

The assessment in Table 16 should also take account of any governance gaps, capability gaps, governance dependencies, resourcing limitations, or specialist support requirements identified in Table 9 in Step 2. Where such issues remain unresolved, organisations should reflect these in their assessment of current capability.

Table 16 Current governance capability

Governance area	Required capability level (1–4)	Current capability level (1–4)	Is current capability sufficient? (Yes/No)	Governance owner (role/function)
Data protection assessment				
Oversight and approval				
Tenant transparency				
Human oversight				
Audit, evidence and assurance				
Safeguards				

Any governance capability gaps, ownership issues, capability limitations, dependencies, governance concerns, or specialist support requirements identified through Table 16 should be recorded and carried forward into Steps 4 and 5.

Note for users completing multiple use cases

If you are assessing more than one use case, complete a separate version of Table 16 for each use case profile identified in Table 15.

This ensures that governance capability is assessed in a way that is specific to each use case, rather than assuming the same level of governance is appropriate across all deployments.

3.5 Step 3 Conclusion

This section summarises the outputs of Step 3 and supports organisations in understanding what has been established through the governance classification and capability assessment process.

Step 3 brings together:

- the **use case profiles** and how each use case is expected to operate in practice
- the **governance classification**, including Governance Level, governance flags, and the distinction between lower-impact and higher-impact use
- the **governance requirements and legal guardrails** associated with each use case
- the organisation's **current governance capability**, and whether it is sufficient to support the proposed use cases

This section helps organisations to:

- bring together these outputs in a clear and consistent way
- understand the overall **governance position** associated with each use case
- identify where governance capability is aligned with what is required, and where gaps remain
- prepare for the next stage of the handbook, which examines how the use case will operate in practice and whether it is appropriate, proportionate, and justified in its real-world context

By completing Step 3, organisations should now have:

- a clear **governance classification** for each use case
- an understanding of the **governance requirements and legal guardrails** associated with those use cases
- an assessment of whether the organisation currently has the **governance capability required** to support the proposed use cases

These outputs should be viewed collectively and will be consolidated in the following section to support consistent and auditable decision-making. Step 4 will use these outputs to assess how the deployment will operate in practice and whether factors such as deployment context, organisational involvement, affected individuals, safeguards, and use of outputs alter the governance considerations associated with the deployment.

3.5.1 Step 3 Outcome

This section records the outcome of Step 3 and confirms whether the organisation is ready to proceed to the next stage of the handbook.

The outcome recorded below should reflect the governance classification recorded in Table 15 and the governance capability assessment recorded in Table 16.

Table 17 Step 3 outcome

Outcome	Recorded by	Date

Proceed to Step 4 – Real-world deployment assessment and justification		
Proceed to Step 4 with areas requiring further consideration (as identified in Step 3 outputs)		
Further review required before proceeding to Step 4		

The outcome recorded above reflects the organisation's position following governance classification and capability assessment.

It does not represent a final approval decision. The next step supports further assessment of how the use case will operate in practice and whether deployment is appropriate, proportionate and justified.

The outputs of Step 3 should now be used within Step 4 to assess how the deployment will operate in practice and whether deployment context, organisational involvement, affected individuals, and use of outputs alter the governance considerations associated with the use case.

4 Step 4 – Real-World Deployment Assessment and Justification

Figure 6 Introducing Step 4's purpose, outputs and relevant principles



Step 4 examines how the proposed IoT use case(s) will operate in practice and supports organisations in determining whether deployment is appropriate, proportionate and justified in a real-world context.

Building on the Governance Level, Governance Flag, Governance Requirements, Legal Guardrails and Governance Capability Assessment established in Step 3, this step considers how the governance classification, governance requirements and organisational capability apply when the use case is deployed in actual environments and operational settings. This includes recognising that the practical realities of deployment — such as where the technology is used, how IoT data is interpreted, and how outcomes are acted upon — may influence the level of impact or sensitivity associated with the use case.

In completing this step, organisations are supported to consider how IoT use may affect tenants, households, staff or living environments, and whether the way data is used in practice remains aligned with the intended purpose. This includes reflecting on the level of monitoring, the potential for behavioural inference, and whether the deployment introduces intrusion or outcomes that are not necessary to achieve the intended objective.

This step also supports organisations in identifying where real-world conditions may increase impact, including where use cases are combined, evolve over time, or interact with other data or systems. Where this occurs, governance expectations may need to be strengthened to ensure that the deployment remains proportionate and appropriate to its context.

Step 4 consists of four stages. First, the organisation assesses how the use case operates in practice and how outputs are used in day-to-day activity. Second, it considers the implications arising from how the use case operates, including impacts on people, fairness, transparency, and decision-making. Third, it assesses whether the intended deployment involves combined, multi-purpose, or coordinated use that may increase governance requirements. Finally, it considers tenancy and legal governance engagement before consolidating the outputs and preparing for Step 5.

The outputs from this step will be used in Step 5 to define governance arrangements, safeguards, accountability arrangements, oversight requirements, and implementation activities.

Organisations should complete Step 4 alongside the outputs recorded in Table 15, Table 16 and Table 17 in Step 3. Governance classifications, governance requirements, legal guardrails, governance capability assessments, capability gaps, and outcome decisions identified in Step 3 should be considered throughout this assessment.

Refer to Annex C.4 (page 238) which provides a set of best practices to assist with completing Step 4, Real World Deployment Assessment and Justification.

4.1 Understanding how the use case will operate in practice

This section supports you in identifying how each use case operates in practice once deployed. It also helps organisations test whether the practical operation of the use case is consistent with the Governance Level, Governance Flag, Governance Requirements and Legal Guardrails identified through the relevant use case profile.

You should complete this section **separately for each use case** identified in Step 1 – from Table 1. Where multiple use cases are being considered, a separate table should be completed for each one. This ensures that each use case is understood clearly and consistently before further assessment is undertaken.

The purpose of this section is not to redefine the use case, repeat earlier assessments, or describe technical system design. Instead, it focuses on the **practical effect** of the use case when it is in operation.

This section focuses on the direct operational effect of the use case as currently intended. Where the intended deployment involves combined use, multiple purposes, or wider organisational coordination, these are considered in Section 4.3.

In completing this section, you should draw on your understanding from earlier steps to describe:

- how the use case is typically identified or brought to attention in practice
- what type of operational response usually follows
- which teams, roles, or organisations are involved in responding
- who or what is typically affected by that response
- the extent to which the use case influences actions or decisions

These responses should reflect how the use case functions in day-to-day operation. You are not expected to describe technical logic, system thresholds, or supplier configuration.

To support consistency, you should select the option or options that best describe the use case in practice. Where more than one option applies, select all that apply.

The purpose of this section is to provide a clear and consistent view of how the use case affects real-world activity. This will be used in the following sections to assess whether the resulting impacts and outcomes are appropriate, proportionate and justified.

Complete one version of Table 18 for each use case recorded in Table 1. For each use case:

- enter the use-case description
- refer to the selected use-case profile in Table 14
- review each field and select every response that applies
- base the responses on how the use case is intended to operate in practice
- consider all teams and organisations involved in responding to outputs
- duplicate the table where more than one use case is being assessed.

The answers recorded in this table should reflect how the classified use case will operate in practice. Do not use Table 18 to record technical specifications, system thresholds or supplier configuration unless these are directly relevant to how outputs are used or acted upon.

The responses should reflect the current intended deployment. Any later material change in purpose or use should be reassessed through the relevant handbook steps.

Table 18 Operating use cases

Field	Guided response
Use case description	Copy from Table 1
How the use case is typically identified or brought to attention in practice	☐ Routine operational visibility ☐ Review of alerts or notifications ☐ Identification of patterns or trends ☐ Identification of exceptions, anomalies, or higher-risk situations
Type of operational response that usually follows	☐ Review or checking activity ☐ Investigation or follow-up ☐ Prioritisation of work, resources, or cases ☐ Direct intervention affecting a property, service, household, or tenant
Who is directly involved in responding to the use case outputs	☐ Housing, tenancy, neighbourhood, or resident-facing team ☐ Asset, repairs, compliance, facilities, or property team ☐ Specialist internal team (for example safeguarding, legal, governance, or data protection) ☐ External partner, contractor, service provider, or supplier
Who or what is typically affected by the response to the use case	☐ Asset, system, or building only ☐ Service delivery or operational process ☐ Home or household ☐ Tenant, occupant, staff member, or other individual
Extent to which the use case influences actions or decisions in practice	☐ Supports awareness or understanding ☐ Informs decision-making ☐ Influences prioritisation or escalation ☐ Acts as a significant basis for actions or outcomes

The responses recorded in Table 18 should be reviewed alongside the Governance Level, Governance Flags, and lower-impact or higher-impact assessment recorded in Table 15. Where there is a significant difference between the expected governance classification and how the use

case operates in practice, organisations should consider whether further review is required before proceeding.

Table 18 provides the primary operational description of how the use case functions in practice. The responses recorded here should be used when completing all subsequent assessments in Step 4.

4.2 Identifying considerations from how the use case operates in practice

This section supports you in identifying whether the way the use case operates in practice introduces any considerations that may affect how it should be reviewed, governed, or deployed. It also builds directly on Section 4.1. You are not being asked to redefine the use case or reassess its governance classification. Instead, you are considering what the **practical effect of the use case** means in terms of data use, tenant impact, fairness, and decision-making.

Attention should be given to any Governance Flags recorded in Table 15, as these indicate the specific governance considerations that may require closer examination in practice.

It also identifies the implications created by how the use case operates in practice. Section 4.3 then considers whether those implications are affected by the fact that the intended deployment is combined, multi-purpose, or relies on coordination across teams or information sources.

In completing this section, you should consider whether the way the use case operates:

- involves the use of data about homes, environments, or people
- influences decisions or actions about properties, services, or individuals
- results in actions or interventions that affect properties, services, households, or tenants
- introduces monitoring or insights about occupancy, behaviour, or living conditions
- could raise questions about fairness, transparency, or how decisions are made

These considerations are particularly important in a social housing context, where there is an inherent **power imbalance between landlord and tenant**. This means that how IoT data is used, and how decisions are made, must be carefully considered to ensure fairness, transparency, and respect for tenant rights and wellbeing.

You should select the option that best reflects how the use case operates in practice in Table 19 below, and complete one for each use case. Where helpful, you may draw on input from operational, governance, tenancy, or legal colleagues, particularly where questions of tenant impact, fairness, or decision-making arise.

Complete one version of Table 19 for each use case assessed in Table 18. For each question in Table 19 select one response:

- **No** where the consideration does not arise meaningfully;
- **Yes** where the consideration is present and should be addressed in the remaining Step 4 assessment; or
- **Yes — significant** where it may materially affect people, decisions, fairness, transparency or the level of governance attention required.

Table 19 Practical impacts and power imbalance considerations

Field	Response
Does the use case influence or contribute to decisions about people, homes, or services?	☐ No ☐ Yes ☐ Yes — significant influence on decisions or actions
Does the use case result in actions or interventions affecting a property, service, household, or tenant?	☐ No ☐ Yes ☐ Yes — significant or direct impact
Does the use case involve monitoring or generating insights from data beyond a single reading or event, including about occupancy, behaviour, or living conditions?	☐ No ☐ Yes ☐ Yes — clear or ongoing monitoring or insight
Does the use case affect tenants, households, or individuals directly?	☐ No ☐ Yes ☐ Yes — significant impact on individuals or households
Could the way the use case operates raise questions about fairness, transparency, or how decisions are made?	☐ No ☐ Yes ☐ Yes — significant concerns about fairness or transparency

The considerations identified in Table 19 should be carried forward when completing Table 20 and Table 21. Attention should be given to any responses indicating significant impacts on individuals, substantial decision influence, ongoing monitoring activities, or significant concerns relating to fairness or transparency.

The purpose of this section is not to decide about the use case. Instead, it ensures that the level of attention applied in the rest of Step 4 reflects the way the use case operates in practice and its potential implications.

4.3 Considering combined or multi-faceted use within the intended deployment

This section supports you in identifying whether the **intended use of the use case**, as defined in previous sections, already involves multiple elements that may increase its complexity and governance requirements in practice.

This builds on Sections 4.1 and 4.2. Organisations should also consider the deployment environment recorded in Table 11, rollout approach recorded in Table 12, and the nature of data use recorded in Table 13 when assessing combined or multi-faceted deployment. You are not being asked to consider hypothetical future uses, system design decisions, or changes of

purpose. Instead, you should focus only on the **use case as it is currently intended to be deployed**.

You should consider whether the intended use:

- involves more than one use case operating together
- involves data being considered alongside other information
- requires interpretation of data beyond a simple reading or event
- serves more than one purpose within the same deployment
- involves more than one team or function within the organisation
- involves more than one organisation receiving, reviewing, interpreting, sharing, or acting upon outputs?

These situations are common in real-world deployments and may increase the **level of coordination, oversight, and governance required**, even where each element appears straightforward on its own.

If the way the use case is intended to be deployed changes in the future (for example, a new purpose is introduced), this should be treated as a **change of use**, and the organisation should return to the beginning of the handbook and reassess the use case. This also applies where an existing deployment is already in operation and the organisation proposes to use the data, outputs, or deployment for a new or expanded purpose. In these circumstances, the organisation should return to Step 1 and reassess the use case before proceeding.

C**omplete Table 20 for each use case**. For each question, select one response:

- **No** where the factor does not apply;
- **Yes** where the factor applies but is not central to how the use case operates; or
- **Yes: central** where the factor is fundamental to the intended operation of the use case.

Consider only the deployment currently being assessed. Do not include hypothetical future uses. If the purpose, use of outputs or combination with other use cases later changes materially, return to the relevant earlier handbook steps.

Where multiple use cases are combined or integrated, consider both the individual use cases and how they operate together.

Table 20 Combined and multi-faceted deployment of use cases

Question	Response
Does the intended use rely on this use case being deployed together with other IoT use cases as part of the same solution or service?	☐ No ☐ Yes — deployed alongside other use cases ☐ Yes — combined deployment is central to how the use case operates
Does the intended use involve data from this use case being considered alongside other types of information as part of the same activity?	☐ No ☐ Yes — used alongside other information ☐ Yes — this combined view is central to how the use case operates
Does the intended use involve interpreting data beyond a single reading or event?	☐ No ☐ Yes — some interpretation is required ☐ Yes — ongoing or structured interpretation is central to the use case
Is the use case intended to serve more than one purpose within the same deployment?	☐ No ☐ Yes — more than one purpose exists ☐ Yes — multiple purposes are central to how the use case operates
Does the intended use involve more than one team, function, or role within the organisation?	☐ No ☐ Yes — more than one team is involved ☐ Yes — coordinated working across teams is central to delivery
Does the intended use involve more than one organisation receiving, reviewing, interpreting, sharing or acting upon outputs?	☐ No ☐ Yes — more than one organisation is involved ☐ Yes — coordinated working across organisations is central to delivery

Responses indicating Yes or Yes: central (or otherwise) should be reflected when assessing tenancy and legal governance engagement and when defining governance, accountability, coordination, safeguards and oversight arrangements in Step 5.

Where combined use, coordinated decision-making or involvement of multiple organisations is central to the deployment, organisations should ensure that roles, responsibilities and governance arrangements are considered for the deployment.

Your responses in this section help identify whether the intended deployment of the use case involves **multiple elements that increase its operational complexity and governance requirements**.

The purpose of this section is to ensure that where a use case is **not standalone**, and the organisation recognises this early and applies appropriate governance in the remaining steps.

Any governance capability gaps, ownership issues, governance dependencies, capability limitations, or specialist support requirements identified in Table 16 should be considered when assessing how the use case will operate in practice and whether additional governance measures may be required.

4.4 Tenancy and legal implications

This section is about how outputs are used in decisions or actions affecting tenants, not re-listing all possible tenancy/legal themes.

This builds on the outputs of Sections 4.2 and 4.3. This assessment should also be considered alongside the Governance Level, Governance Requirements and Legal Guardrails recorded in Table 15. You are not being asked to carry out a legal assessment or determine whether the use case is compliant. Instead, this section helps you recognise where the use case may:

- affect tenants, households, or how people use and experience their home
- involve monitoring or insight within private living spaces
- influence or inform decisions about tenants, households, or service provision
- involve the use of personal or sensitive information
- require transparency, communication, or additional safeguards

It is important to recognise where data from the use case may be used beyond observation, to support or inform actions or decisions that affect tenants (subject always to due legal process being followed).

The purpose of this section is to ensure that where tenancy or legal considerations are relevant, they are identified early and carried forward into the design of governance, safeguards, and approval decisions in the following sections.

The levels in Section 4.4 **do not replace** the Governance Level identified through the use case profile. Instead, they describe the degree to which tenancy and legal governance considerations are engaged within the intended deployment.

4.4.1 Identifying tenancy and legal governance engagement

This section supports you in identifying how the intended use of the use case, as already defined in Step 3 and refined in earlier parts of Step 4, engages tenancy and legal governance in practice.

You are not being asked to repeat the purpose of the use case, reassess its governance classification, or carry out a legal assessment. Instead, this section focuses on how data and outputs from the use case are used in decisions or actions affecting tenants or households.

The purpose of this section is to distinguish between use cases where data remains within standard operational activity, use cases where data is used to support decisions involving tenants, and use cases where data is integral to decisions or actions affecting tenants or households. This distinction determines how governance must be applied in the next step.

In completing this section:

- focus on the intended use of the use case as currently defined

- do not consider future changes or expanded use (any change of purpose should return to the beginning of the handbook)
- consider how the use case operates across the full intended deployment, including where more than one team or organisation may be involved
- where helpful, draw on input from colleagues or delivery partners involved in how the use case will operate in practice

A simple way to approach this is to consider how the outputs from the use case are used:

- if outputs are not used to inform or influence decisions about tenants, the use case is likely to fall into the first row
- if outputs are used to support or inform decisions, but are not the main basis for those decisions, the use case is likely to fall into the second row
- if outputs are used to trigger or directly inform actions or decisions affecting tenants, the use case is likely to fall into the third row

When distinguishing between the second and third rows, focus on whether the outputs are **one input among others in decision-making**, or whether they are **used as a basis for action or decision-making**. The second row applies where outputs support judgement, while the third applies where outputs are used to trigger or directly inform actions or decisions affecting tenants.

Select the row that best reflects how the use case operates in practice.

- For each use case, only **one row should normally apply**.
- Select the row that represents the **primary or most significant use of the outputs**.
- If more than one row appears to apply, select the row that best reflects how the outputs are **primarily used in practice**.

For Table 21 where more than one use case is intended to be deployed, complete the table for each use case separately, based on its intended purpose and how its outputs are used.

Where use cases operate independently, and their outputs are not combined to inform or trigger the same decisions or actions affecting tenants, each use case should be carried forward based on its own outcome.

Where use cases are combined or integrated, such that outputs from more than one use case are used together to inform, support, or trigger the same decisions or actions affecting tenants or households, you should consider how the combined use of those outputs affects decision-making in practice.

In these cases, the combined deployment may result in a higher level of tenancy and legal governance engagement than any single use case considered on its own. Where this occurs, the highest applicable level should be carried forward into the next step for that combined use.

Tick “Applies” for the selected row and select the corresponding governance level.

The governance level is determined directly by the row selected and does not require further interpretation.

When determining the appropriate tenancy and legal governance engagement level, organisations should consider the Governance Level, Governance Requirements and Legal Guardrails recorded in Table 15, together with the practical impacts identified in Table 18–Table

20. The level recorded in Table 21 is a tenancy and legal governance engagement level. It does not change or replace the Governance Level recorded in Step 3.

Complete Table 21 separately **for each use case**.

- Review the three statements
- Select **Applies** against the one statement that best reflects how outputs are primarily used
- Select **Does not apply** against the remaining statements
- Record the tenancy and legal governance engagement level corresponding to the selected statement
- Select only one level for each use case
- Where use cases are combined and their outputs are used together to inform the same decision or action, assess the combined use and apply the highest relevant level.

If the intended use cannot be classified confidently, seek appropriate tenancy, governance, data-protection or legal input before proceeding.

Table 21 Tenancy and legal governance engagement

Statement	Response
The outputs from the use case are not used to inform or influence decisions about tenants or households. Level 1 — Standard tenancy/legal engagement -	☐ Applies ☐ Does not apply
The outputs from the use case are used to support or inform decisions about tenants or households but are not the primary basis for those decisions. Level 2 — Additional tenancy/legal governance required	☐ Applies ☐ Does not apply
The outputs from the use case are used to trigger or directly inform actions or decisions affecting tenants or households. Level 3 — Tenancy/legal governance is integral	☐ Applies ☐ Does not apply

Table 21 provides the primary tenancy and legal governance output of Step 4 and should be carried forward into Step 5 when defining governance, safeguards, decision-making arrangements, transparency requirements and approval processes.

The Tenancy and Legal Governance Engagement Level recorded here in Table 21 reflects how outputs from the use case are used in decisions or actions affecting tenants or households.

You are not expected to define governance, safeguards, or decision-making processes at this stage. This will be completed in Step 5.

The level recorded in Table 21 must be used in Step 5 when defining governance arrangements, safeguards, oversight requirements, accountability arrangements, approval requirements, transparency measures, and decision-making processes.

4.5 Step 4 Conclusion

This section summarises the outputs of Step 4 and supports organisations in understanding what has been established through the real-world assessment of the use case.

Step 4 brings together:

- the defined operation of the use case in practice (Table 18)
- the practical implications of the use case, including potential impacts on people, fairness, transparency and decision-making, as recorded in (Table 19)
- the level of complexity and coordination involved in delivering the use case (Table 20)
- the role of outputs in decisions or actions affecting tenants, and the resulting level of tenancy and legal governance engagement, as confirmed in Table 21

This section helps organisations to:

- bring together these outputs in a clear and consistent way
- understand how the use case operates in practice and how it may affect tenants
- recognise how outputs are used in decision-making and what this means for governance
- prepare for the next stage of the handbook, which defines how governance, safeguards, roles, and decision-making processes must be applied

Table 18–Table 21 collectively form the primary assessment outputs of Step 4. These outputs should be reviewed together before defining governance arrangements in Step 5.

4.6 Step 4 Outputs

This section brings together the key outputs from Step 4 into a structured view for each use case.

Table 18 to Table 21 form the principal assessment outputs from Step 4. Table 22 summarises how those outputs should be carried forward into Step 5. Before recording the Step 4 outcome in Table 23, review the outputs collectively and confirm that they provide a clear and consistent account of the intended deployment.

This provides a clear and auditable record of:

- how the use case operates in practice
- the key implications identified
- the complexity and coordination involved
- the level of tenancy and legal governance engagement.

Table 22 Outputs carried forward from Step 4 to Step 5

Step 4 Output	Table sources	Used in Step 5	Why It Matters
How the use case operates in practice	Table 18	5.2	Defines operational ownership, responsibilities and oversight
Practical impacts and implications	Table 19	5.2 and 5.4	Safeguards, human oversight, transparency and governance controls
Combined use, complexity and coordination factors	Table 20	5.2 and 5.4	Governance ownership, organisational involvement and coordination arrangements
Tenancy and legal governance engagement	Table 21	5.4 and 5.5	Legal, tenancy, engagement, review and approval considerations

Before recording the outcome, ensure that all sections of Step 4 have been completed and reflected in the consolidated output.

Where the use case has been identified as Level 2 or Level 3 in Table 21, you should ensure that the outputs of Step 4 are reviewed with colleagues or organisations whose knowledge is needed to confirm the assessment before proceeding to Step 5.

This review should focus on confirming a shared understanding of:

- how the use case operates in practice
- how outputs are used in decisions or actions affecting tenants
- the implications and complexity identified in earlier sections

Depending on the nature of the use case, this may include input from housing, service, digital, governance, data protection, or legal colleagues.

The purpose of this review is not to approve or reject the use case. Instead, it is intended to ensure that the organisation has a clear and consistent understanding of how the use case will operate in practice before governance arrangements are defined in the next step.

If the assessment completed in Step 4 indicates that the use case will operate in a materially different way from that originally described in Step 1 or classified in Step 3, organisations should consider whether earlier steps need to be revisited before proceeding to Step 5.

4.6.1 Step 4 Outcome

This section records the overall outcome of Step 4 and confirms whether the assessed use case or use cases are ready to proceed to Step 5.

In determining the appropriate outcome, organisations should consider whether:

- the use case is sufficiently understood in practice
- any significant tenant, household, fairness, transparency, tenancy, or legal governance considerations remain unresolved
- additional governance, legal, tenancy, operational, or specialist input is required
- the deployment remains appropriate, proportionate and justified in its intended context

Select one outcome in Table 23 that best reflects the organisation's position after reviewing Tables 18 to 21. Record the name or role of the person confirming the outcome and the date of the review.

Table 23 Step 4 outcome

Outcome	Recorded By	Date
The organisation has sufficient understanding of how the use case will operate in practice and may proceed to Step 5.		
The organisation has identified deployment, tenant-impact, coordination, tenancy, or legal governance considerations that should be addressed when defining governance arrangements in Step 5.		
An additional review is required to establish how the use case will operate in practice before governance arrangements can be defined in Step 5.		

The outcome recorded in Table 23 should reflect the findings recorded in Table 18–Table 21 and any governance capability gaps, dependencies, specialist support requirements, governance concerns, or legal considerations identified through earlier steps.

It does not represent a final approval decision. The next step defines how governance, safeguards, roles, and decision-making processes must be applied in practice.

5 Step 5 – Governance Definition, Readiness and Approval

Figure 7 Introducing Step 5's purpose, outputs and relevant principles



The final step, Step 5 consists of four stages:

- Confirm previous step outputs – First, organisations confirm that any outstanding concerns arising from Steps 2, 3 and 4 have been addressed or are being appropriately managed.
- 5.2 Define governance arrangements, safeguards and responsibilities – Second, governance arrangements, safeguards, responsibilities, and accountability arrangements are defined for the intended deployment.
- 5.3 Legal, tenancy and deployment conditions – Third, any deployment-specific legal, tenancy, transparency, safeguarding, organisational, or implementation concerns are identified and reviewed through the appropriate pathway or pathways.
- 5.4 Governance and deployment decision – Finally, the organisation records the governance and deployment decision and confirms whether the deployment is ready to proceed.

The outputs from this step provide the formal governance position for the intended deployment and support ongoing governance, implementation, operation, reassessment, and review activities.

By this stage, the organisation should have:

- established the purpose of the use case or use cases

- completed governance classification and capability assessment
- assessed how the use case or use cases will operate in practice
- identified any implications, complexity factors, and tenancy or legal governance considerations associated with the intended deployment

The purpose of this step is not to reassess any use case, revisit governance classification, or repeat earlier stages of the handbook. Instead, it focuses on translating the outputs of the previous steps into a practical governance approach that supports consistent, proportionate, and auditable deployment.

This step supports organisations in:

- defining the governance arrangements required for the intended deployment
- confirming that the organisation has the capability and readiness to apply those arrangements in practice
- identifying any safeguards, oversight arrangements, responsibilities, dependencies, or conditions that should be addressed before deployment
- determining whether legal review, tenancy documentation review, tenant engagement, or other specialist input is required
- recording a clear and auditable governance decision before deployment proceeds

In completing this step, organisations should draw on:

- the governance requirements, legal guardrails, and capability assessment established in Step 3
- the operational assessment, implications, complexity factors, and tenancy and legal governance engagement identified in Step 4
- the critical baseline controls and preconditions identified in Step 2

Particular attention should be given to:

- Table 9 (Organisational Governance Readiness)
- Table 15 (Governance Classification)
- Table 16 (Current Governance Capability)
- Table 21 (Tenancy and Legal Governance Engagement)
- Table 23 (Step 4 Outcome)

These tables contain the principal governance outputs from earlier steps and should be used throughout Step 5. This step should be completed based on the use case or use cases as they are currently intended to be deployed.

Where multiple use cases are being considered, governance should be defined for both the individual use cases and the deployment as a whole. Where use cases operate independently, governance may be defined separately for each use case. Where use cases are combined or integrated, governance should reflect how those use cases operate together in practice and the combined effect of the deployment.

Governance should also reflect the environment in which deployment takes place. This may include existing occupied homes, void properties, supported accommodation, temporary

accommodation, communal areas, or new-build developments. The governance arrangements, safeguards, documentation, communication, and oversight required for deployment may differ depending on whether tenants are already in occupation and how the technology will be introduced and used in practice.

Governance requirements may not be identical across all deployment environments. For example, a use case deployed within existing occupied homes may require different engagement, communication, access, oversight, tenancy, or implementation arrangements than the same use case deployed within new-build homes, void properties, or other unoccupied environments. Organisations should therefore ensure that governance arrangements reflect not only the use case itself, but also the context in which deployment will occur.

The governance approach should not assume that one deployment environment automatically requires more or less governance than another. Instead, organisations should consider whether the deployment context creates different governance, tenancy, communication, documentation, oversight, engagement, or implementation requirements that need to be addressed before deployment proceeds.

This step is also the point at which organisations confirm whether the intended deployment is governance ready. This includes confirming that:

- governance requirements can be met
- critical baseline conditions are in place
- responsibilities and decision-making arrangements are clearly defined
- appropriate safeguards and oversight arrangements can be implemented
- any required legal, tenancy, governance, or specialist reviews have been completed or identified as conditions for deployment

The outputs of this step support organisations in defining, implementing, and documenting the governance arrangements, safeguards, responsibilities, deployment conditions, and approval records appropriate to the intended deployment.

The purpose of this step is not to assess future changes in use. Where the purpose of a use case changes, where use cases are combined in new ways, or where data is later used for new forms of analysis or decision-making, organisations should follow the reassessment requirements set out in Step 6.

By the end of this step, organisations should have:

- a clearly defined governance approach for the intended deployment
- confirmation that the organisation is ready to apply the required governance arrangements
- a clear understanding of any conditions, dependencies, or actions that must be addressed before deployment
- a recorded and auditable decision on whether the intended deployment is ready to proceed

This step supports organisations in confirming governance readiness before deployment and in defining how the intended deployment will be governed, managed, monitored, and overseen in practice.

Refer to Annex C.5 (page 240) which provides a set of best practices to assist with completing Step 5 Governance Definition, Readiness and Approval.

5.1 Confirming previous step outputs

This section supports organisations in confirming that any deployment-relevant gaps, dependencies, conditions, or actions identified in earlier steps have been addressed appropriately before governance arrangements are defined.

You are not being asked to repeat the assessments completed in Steps 2, 3 or 4. Instead, this section uses the consolidated outputs from those steps to confirm that any concerns requiring attention have either:

- been addressed
- been addressed with agreed conditions or actions
- or remain unresolved and require further work before deployment can proceed

The purpose of this section is not to determine whether deployment should proceed. Instead, it ensures that the outputs of earlier steps have been considered and that any outstanding concerns are identified before governance arrangements are defined in the following sections.

In completing this section, review the consolidated outputs from the previous steps and consider whether any deployment-relevant issues remain outstanding:

- Step 2: Has any governance-, legal-, security-, privacy-, or deployment-critical requirements, dependencies, conditions, or actions identified in Step 2 been addressed sufficiently to support the intended deployment?
- Step 3: Has any governance requirements, legal guardrails, capability gaps, dependencies, or conditions identified in Step 3 been addressed sufficiently to support the intended deployment?
- Step 4: Has any governance implications, complexity factors, deployment considerations, tenancy and legal governance considerations, or other actions arising from Step 4 been addressed sufficiently to support the intended deployment?

The following sections support you in recording the outcome of these checks.

When completing Sections 5.1.1 to 5.1.3, organisations should use the principal outputs recorded in Table 9, Table 15, Table 16, Table 21 and Table 23, together with any associated actions, conditions, dependencies, capability gaps, safeguards, governance requirements, or specialist support requirements identified in earlier steps.

5.1.1 Confirming Step 2 outputs

This section supports organisations in confirming that any unresolved concerns identified in Step 2 have been addressed, are being managed through agreed actions or deployment conditions, or remain unresolved.

Organisations should use the organisational governance readiness findings recorded in Table 9 when assessing whether unresolved concerns, dependencies, capability gaps, governance concerns, or specialist support requirements have been addressed.

You are not being asked to repeat the assessment completed in Step 2 or revisit the Step 2 readiness checkpoint. Instead, this section focuses on the status of any unresolved concerns, actions, dependencies, conditions, capability gaps, or support requirements identified through Step 2.

Where the intended deployment consists of a single use case, consider whether any unresolved concerns identified in Step 2 have been addressed sufficiently to support that deployment.

Where the intended deployment consists of multiple use cases, consider whether any unresolved concerns identified in Step 2 affect one or more of those use cases and whether they have been addressed sufficiently to support the deployment.

Where use cases are combined or integrated, consider whether any unresolved concerns identified in Step 2 affect how those use cases operate together in practice, including any governance, accountability, data-sharing, oversight, supplier-management, or coordination arrangements required to support the combined deployment.

When recording the outcome, base your assessment on the intended deployment rather than on individual use cases in isolation.

Use the following guidance when selecting a statement:

- **Step 2 outputs addressed** should be recorded where any unresolved concerns identified in Step 2 have been satisfactorily resolved and no further action is required.
- **Step 2 outputs addressed with conditions** should be recorded where unresolved concerns remain, but appropriate actions, safeguards, oversight arrangements, governance measures, deployment conditions, or specialist support have been agreed and are actively being managed. This option should only be used where those arrangements are sufficient to support the intended deployment.
- **Further action required before proceeding** should be recorded where unresolved concerns remain and appropriate arrangements have not been established to support the intended deployment.

Review each statement in Table 24 and only select one of them. The selected statement determines the outcome recorded for this section. Where more than one statement appears relevant, select the statement that best reflects the overall position.

Table 24 Confirming Step 2 outputs

Statement	Outcome
Any unresolved concerns, actions, dependencies, conditions, capability gaps, or support requirements identified in Step 2 have been addressed.	Step 2 outputs addressed ☐
Any unresolved concerns, actions, dependencies, conditions, capability gaps, or support requirements identified in Step 2 have not yet been fully addressed but are being managed through agreed actions, deployment conditions, safeguards, oversight arrangements, governance measures, or specialist support.	Step 2 outputs addressed with conditions ☐
One or more unresolved concerns, actions, dependencies, conditions, capability gaps, or support requirements identified in Step 2 remain outstanding and have not been addressed or appropriately managed.	Further action required before proceeding ☐

Confirmation

This section should be confirmed by an individual with sufficient knowledge of the concerns identified in Step 2 and the intended deployment.

Where unresolved concerns identified in Step 2 relate to governance, operational ownership, supplier management, legal, privacy, security, safeguarding, tenancy, or other specialist areas, the individual completing this section should seek appropriate input before recording the outcome.

Table 25 Confirmation of Step 2 outputs

Confirmed by	Role	Date

The individual completing this section confirms that the Consolidated Step 2 Output has been reviewed and that the outcome recorded above accurately reflects the organisation's current position.

Any agreed actions, deployment conditions, safeguards, oversight arrangements, dependencies, or unresolved issues identified through this review should be carried forward into the relevant sections of Step 5 and reflected in any governance arrangements, deployment conditions, or approval decisions.

5.1.2 Confirming Step 3 outputs

This section supports organisations in confirming that any unresolved concerns identified in Step 3 have been addressed or remain unresolved.

Use the Step 3 Outputs (Use the Governance Level, Governance Flag(s), Governance Requirements, Legal Guardrails and Governance Capability Assessment established through Step 3) when completing this section. Attention should be given to the Governance Classification recorded in Table 15 and the Governance Capability Assessment recorded in Table 16.

You are not being asked to repeat the governance classification process completed in Step 3 or revisit the assessments already recorded there. Instead, this section focuses on the status of any

actions, conditions, dependencies, capability gaps, support requirements, or further work identified through the Step 3 governance assessment.

Where the intended deployment consists of a single use case, consider whether any unresolved concerns identified in Step 3 have been addressed sufficiently to support that deployment.

Where the intended deployment consists of multiple use cases, consider whether any unresolved concerns identified in Step 3 affect one or more of those use cases and whether they have been addressed sufficiently to support the deployment .

Where use cases are combined or integrated, consider whether any unresolved concerns identified in Step 3 affect the organisation's ability to apply the governance required for the combined deployment.

When recording the outcome, base your assessment on the intended deployment in Table 26 rather than on individual use cases in isolation.

Use the following guidance when recording the outcome:

- **Step 3 outputs addressed** should be recorded where any actions, conditions, dependencies, capability gaps, support requirements, or further work identified through the Step 3 governance assessment have been satisfactorily addressed.
- **Further action required before proceeding** should be recorded where one or more actions, conditions, dependencies, capability gaps, support requirements, or further work identified through the Step 3 governance assessment remain unresolved.

Review each statement in Table 26 and only select one of them. The selected statement determines the outcome recorded for this section. Where more than one statement appears relevant, select the statement that best reflects the overall position.

Table 26 Confirming Step 3 outputs

Statement	Outcome
Any unresolved actions, conditions, dependencies, capability gaps, support requirements, or further work identified through the Step 3 governance assessment have been addressed.	Step 3 outputs addressed ☐
One or more unresolved actions, conditions, dependencies, capability gaps, support requirements, or further work identified through the Step 3 governance assessment remain unresolved.	Further action required before proceeding ☐

Confirmation

This section should be confirmed by an individual with sufficient knowledge of the Step 3 outputs and the intended deployment.

Where unresolved concerns identified in Step 3 relate to governance, legal, privacy, security, accountability, oversight, tenancy, safeguarding, organisational capability, or other specialist areas, the individual completing this section should seek appropriate input before recording the outcome.

Table 27 Confirmation of Step 3 outputs

Confirmed by	Role	Date

The individual completing this section confirms that the Consolidated Step 3 Output (Table 8, Table 9) has been reviewed and that the outcome recorded above accurately reflects the organisation's current position.

Any unresolved issues identified through this review should be addressed before proceeding further through Step 5.

5.1.3 Confirming Step 4 outputs

This section supports organisations in confirming that any unresolved concerns identified in Step 4 (Table 18 to Table 21) have been addressed, are being managed through agreed deployment arrangements, or remain unresolved.

Use the Step 4 Outputs (Table 18 to Table 21) when completing this section. Attention should be given to the Tenancy and Legal Governance Engagement Level recorded in Table 21 and the outcome recorded in Table 23.

You are not being asked to repeat the assessments completed in Step 4 or revisit how the deployment was evaluated. Instead, this section focuses on the status of any actions, dependencies, deployment activities, coordination arrangements, engagement activities, support requirements, or further work arising from Step 4.

Where the intended deployment consists of a single use case, consider whether any unresolved concerns identified in Step 4 have been addressed sufficiently to support that deployment.

Where the intended deployment consists of multiple use cases, consider whether any unresolved concerns identified in Step 4 affect one or more of those use cases and whether they have been addressed sufficiently to support the deployment.

Where use cases are combined or integrated, consider whether any unresolved concerns identified in Step 4 affect how those use cases operate together in practice, including any accountability, oversight, coordination, tenant engagement, communication, or decision-making arrangements required to support the combined deployment.

When recording the outcome, base your assessment on the intended deployment rather than on individual use cases in isolation.

Use the following guidance when recording the outcome:

- **Step 4 outputs addressed** should be recorded where any unresolved concerns arising from Step 4 have been satisfactorily resolved and no further action is required.
- **Step 4 outputs addressed with conditions** should be recorded where the governance response required by Step 4 has been defined and put in place, but supporting deployment activities, coordination arrangements, engagement activities, or other implementation actions remain ongoing and are actively being managed. This option should only be used where those arrangements are sufficient to support the intended deployment.
- **Further action required before proceeding** should be recorded where one or more governance implications, tenancy or legal governance requirements, accountability arrangements, oversight arrangements, decision-making arrangements, or other concerns arising from Step 4 remain unresolved.

Review each statement in Table 28 and only select one of them. The selected statement determines the outcome recorded for this section. Where more than one statement appears relevant, select the statement that best reflects the overall position.

Table 28 Confirming Step 4 outputs

Statement	Outcome
Any unresolved concerns arising from Step 4 have been addressed.	Step 4 outputs addressed ☐
The governance response required by Step 4 has been defined and put in place, but one or more supporting deployment activities, coordination arrangements, engagement activities, or implementation actions remain ongoing and are being actively managed.	Step 4 outputs addressed with conditions ☐
One or more governance implications, tenancy or legal governance requirements, accountability arrangements, oversight arrangements, decision-making arrangements, or other concerns arising from Step 4 remain unresolved.	Further action required before proceeding ☐

Confirmation

This section should be confirmed by an individual with sufficient knowledge of the Step 4 outputs and the intended deployment.

Where unresolved concerns arising from Step 4 relate to governance, legal, privacy, security, accountability, oversight, tenancy, safeguarding, organisational capability, tenant engagement, partner organisations, or other specialist areas, the individual completing this section should seek appropriate input before recording the outcome.

Table 29 Confirmation of Step 4 outputs

Confirmed by	Role	Date

The individual completing this section confirms that the Consolidated Step 4 Output (i.e. Table 18 to Table 21) has been reviewed and that the outcome recorded above accurately reflects the organisation's current position.

Any agreed deployment conditions, engagement activities, coordination arrangements, support requirements, dependencies, or unresolved issues identified through this review should be carried forward into the relevant sections of Step 5 and reflected in any governance arrangements, deployment conditions, or approval decisions.

5.2 Defining governance arrangements, safeguards and responsibilities

The governance arrangements defined in this section should reflect the outcomes recorded in Table 24, Table 26 and Table 28, together with any unresolved concerns, conditions, dependencies, capability gaps, support requirements, or deployment actions identified through those reviews.

This section supports organisations in defining the governance arrangements required for the intended deployment.

The purpose of this section is not to repeat earlier assessments or revisit decisions already taken. Instead, it focuses on translating the outputs of the previous steps into practical governance arrangements that can be applied before and during deployment.

This section supports organisations in:

- defining how governance will operate for the intended deployment
- establishing the safeguards required to support lawful, proportionate, and accountable deployment
- defining responsibilities, accountability, and oversight arrangements
- ensuring governance reflects the deployment context, including occupied homes, new-build homes, void properties, communal areas, and other deployment environments where relevant
- ensuring governance reflects how the deployment will operate in practice, including single use cases, multiple use cases, combined use cases, sequential use, and multi-organisation arrangements

You should not repeat information already recorded elsewhere in the handbook. Instead, use the outputs from earlier steps to define the governance arrangements required for the intended deployment.

Social landlords retain overall accountability for governance, compliance, use of data, tenant impact, cybersecurity oversight, system integrity, and deployment decisions. While suppliers, contractors, manufacturers, software providers, and partners may support delivery and demonstrate compliance with agreed requirements, accountability for the deployment cannot be transferred to them.

The outputs of this section should provide a clear and auditable governance framework for the intended deployment and will be used in the following sections to determine any legal, tenancy, documentation, engagement, deployment, and approval requirements.

5.2.1 Defining governance arrangements

This section supports organisations in confirming that they have defined how the Governance Levels identified in Step 3 will be implemented for the intended deployment.

Use the following tables to complete this section:

- Table 15
- The tables referenced in Table 22
- Table 24, Table 26 and Table 28

You are not being asked to repeat the governance assessment completed in Step 3 or revisit the deployment assessment completed in Step 4.

The Governance Levels recorded in Step 3 and the deployment assessment completed in Step 4 should already reflect the intended deployment, including any multiple use cases, combined use cases, deployment environments, participating organisations, and other deployment-specific considerations.

This section does not reassess those factors. Instead, it confirms that:

- arrangements have been defined to implement the Governance Levels identified in Step 3
- ownership has been identified for each governance domain

For each governance domain, confirm that the Governance Level identified in Step 3 will be implemented for the intended deployment and that ownership has been identified.

5.2.2 Governance domain assessment outcome

Attention should be given to the Tenancy and Legal Governance Engagement Level recorded in Table 21 and the outcome recorded in Table 23.

The governance domains assessed in Table 30 correspond directly to the governance capability areas assessed in Table 16. Any governance domain recorded as incomplete should be considered a governance readiness issue requiring resolution before deployment proceeds.

Table 30 Governance domain assessment

Governance Domain	Governance Level Identified in Step 3 Will Be Implemented for the Intended Deployment	Governance Owner Identified
Data Protection Assessment	☐ Yes ☐ No	☐ Yes ☐ No
Oversight and Approval	☐ Yes ☐ No	☐ Yes ☐ No
Tenant Transparency	☐ Yes ☐ No	☐ Yes ☐ No
Human Oversight	☐ Yes ☐ No	☐ Yes ☐ No
Audit, Evidence and Assurance	☐ Yes ☐ No	☐ Yes ☐ No
Safeguards	☐ Yes ☐ No	☐ Yes ☐ No

A governance domain should only be recorded as complete where:

- arrangements have been defined to implement the Governance Level identified in Step 3 for the intended deployment
- governance ownership has been identified

The governance owner may be:

- an individual
- a team
- a governance function
- a jointly agreed governance arrangement involving more than one organisation

The handbook does not prescribe who the governance owner should be. The organisation is responsible for determining the most appropriate governance owner for each governance domain.

Any governance domain recorded as **No** should be addressed before deployment progresses.

5.2.3 Confirmation

This section should be confirmed by an individual with sufficient knowledge of the governance requirements identified in Step 3 and the intended deployment.

Where governance arrangements involve multiple teams, specialist functions, suppliers, contractors, partners, external advisers, or other organisations, appropriate input should be obtained before recording the outcome.

Table 31 Confirmation of governance domain assessment

Confirmed by	Role	Date

The individual completing this section confirms that arrangements have been defined to implement the Governance Levels identified in Step 3 and that governance ownership has been identified for each applicable governance domain.

Any unresolved governance concerns identified through this review should be addressed before proceeding further through Step 5.

5.3 Defining responsibilities and accountability

This section supports organisations in confirming that responsibilities and accountability for the intended deployment have been understood and defined.

Use these tables when completing this section:

- Table 15
- The tables referenced in Table 22
- Table 24, Table 26 and Table 28
- Table 30.

You are not being asked to define contractual obligations, procurement requirements, technical delivery responsibilities, or detailed operating procedures.

Instead, this section focuses on confirming that the organisation understands:

- where overall accountability sits for the deployment
- where delivery organisations are involved in supporting the deployment
- where partner organisations are involved in receiving, sharing, interpreting, acting upon, or supporting the use of deployment outputs
- how those organisations support the intended deployment

The purpose of this section is to ensure that accountability and supporting responsibilities are understood before deployment proceeds.

Where the intended deployment consists of a single use case, complete this section for that deployment.

Where the intended deployment consists of multiple independent use cases, complete this section by considering all organisations involved across those use cases.

Where use cases are combined or integrated, complete this section based on the combined deployment and consider any organisations involved in delivering, supporting, receiving, sharing, interpreting, or acting upon deployment outputs.

This section should be completed for the intended deployment as a whole rather than for individual use cases in isolation.

5.3.1 Responsibilities and accountability assessment

Organisations should consider any complexity, coordination, multi-team, multi-use case, or multi-organisation factors identified in Table 20 when assessing responsibilities and accountability in Table 32.

Table 32 Responsibilities and accountability assessment

Responsibility Area	Yes	No	Not Applicable
The organisation recognises that overall accountability for governance, compliance, use of data, tenant impact, cybersecurity oversight, system integrity, and deployment decisions remains with the social landlord.			
Where technology suppliers, contractors, telecare providers, service providers, or other delivery organisations are involved, their role in supporting the intended deployment has been identified.			
Where partner organisations are involved in receiving, sharing, interpreting, acting upon, or supporting the use of deployment outputs, their role has been identified.			
Where partner organisations have a role in receiving, interpreting, sharing, reviewing, escalating, or acting upon deployment outputs, those responsibilities have been discussed and are understood by the organisations involved.			

A responsibility area should only be recorded as complete where the organisation has clearly identified the relevant accountability, support arrangements, or organisational involvement necessary to support the intended deployment.

Any applicable responsibility area recorded as **No** should be addressed before deployment progresses.

5.3.2 Responsibilities and accountability outcome

Select one of the two outcomes in Table 33.

Table 33 Responsibilities accountability outcomes

Outcome	Response
Responsibilities and accountability defined for the intended deployment	☐
Further action required before proceeding	☐

Record:

- **Responsibilities and accountability defined for the intended deployment** where all applicable responsibility areas are recorded as **Yes** or **Not Applicable** in Table 32
- **Further action required before proceeding** where one or more applicable responsibility areas are recorded as **No in** Table 32.

5.3.3 Confirmation

This section should be confirmed by an individual with sufficient knowledge of the intended deployment and the organisations involved in supporting it.

Where the deployment involves delivery organisations, partner organisations, contractors, service providers, external advisers, or other third parties, appropriate input should be obtained before recording the outcome.

Table 34 Confirmation of responsibilities accountability outcomes

Confirmed by	Role	Date

The individual completing this section confirms that responsibilities and accountability for the intended deployment have been reviewed and defined appropriately.

Any unresolved accountability, support, or organisational involvement identified through this review should be addressed before proceeding further through Step 5.

5.4 Legal, tenancy and deployment conditions

This section helps organisations identify any governance, legal, tenancy, transparency, safeguarding, accountability or deployment-related concerns that should be addressed before deployment proceeds.

Use the outputs from:

- Table 15 (Governance Classification)
- Table 21 (Tenancy and Legal Governance Engagement)
- Table 23 (Step 4 Outcome)
- the governance arrangements defined in Section 5.2.

You are not being asked to repeat earlier assessments or provide legal advice. Instead, this section helps determine whether additional review, clarification, communication,

documentation, safeguards or organisational arrangements are required before deployment proceeds.

Different deployments create different governance considerations. To support proportionate assessment, complete only the pathway or pathways that are relevant to the intended deployment.

This section should be completed for the intended deployment.

- Where the intended deployment consists of a single use case, complete this section for that deployment.
- Where the intended deployment consists of multiple independent use cases, consider each use case individually.
- Where use cases are combined or integrated, complete this section based on the combined deployment.

5.4.1 Pathway mapping guidance

Use the relevant use case profile(s), Governance Flag(s), Legal Guardrails, and deployment assessment completed earlier in the handbook to determine which pathway or pathways should be completed. Complete the:

- **Place-Based Deployment Pathway** (5.4.2) where the deployment is primarily associated with properties, buildings, assets, environmental monitoring, safety monitoring or housing management functions.
- **Tenant-Affecting Deployment Pathway** (5.4.3) where outputs may influence actions, interventions or decisions relating to tenants, households or residents.
- **Health, Care and Telecare Deployment Pathway** (5.4.4) where the deployment supports health, wellbeing, safeguarding, support services, telecare, social care or healthcare functions.

Where multiple pathways are relevant, complete each applicable pathway and consider the findings collectively when recording the governance and deployment decision. Where uncertainty remains, seek input from relevant colleagues, specialists, advisers, delivery organisations, service providers, or partner organisations before proceeding.

More detailed information on place-based, tenant affecting and health, care and telecare deployments are provided below, to assist in determining which pathways may need to be completed.

Place-based deployments

Complete the Place-Based Deployment pathway where the use case is primarily associated with:

- a property
- a building
- a residential environment
- housing management activities
- asset management activities
- environmental monitoring
- property condition monitoring
- building condition monitoring
- access management
- tenancy-related deployment activities

Examples may include:

- Damp & Mould
- CO_2 / indoor air quality (IAQ)
- Asset / Property Management
- Leak Monitoring
- Fire Alarms
- Smoke Alarms
- Temperature / Energy Monitoring where used primarily for housing, environmental, maintenance, or asset-management purposes
- External CCTV
- Smart Locks / Door Entry where used primarily for access to buildings, communal areas, contractor access, or property-management activities

The Place-Based Deployment pathway focuses on identifying concerns relating to:

- tenancy and occupancy arrangements
- communications and transparency
- access and operational arrangements
- landlord and organisational obligations
- deployment planning and delivery

Tenant affecting deployments

Complete the Tenant Affecting Deployment pathway where outputs from the deployment may influence:

- actions affecting tenants
- decisions affecting tenants
- investigations relating to tenants
- interventions involving tenants
- communications with tenants
- other responses affecting tenants

This pathway is likely to apply where the deployment may:

- indicate presence, absence, activity, behaviour, habits, or routines
- affect how a tenant uses their home
- influence decisions or actions relating to a tenant
- create privacy, transparency, accountability, safeguarding, or tenancy-related implications beyond routine property management

Examples may include:

- Occupancy / Motion Monitoring
- Appliance Monitoring
- Thermal Imaging
- Internal CCTV
- Combined deployments where outputs may be used to inform actions affecting tenants (for example external CCTV)

The Tenant Affecting Deployment pathway focuses on identifying concerns relating to:

- actions or decisions affecting tenants
- transparency and communications
- privacy and use-of-home implications
- safeguards, accountability, and human oversight
- governance implications arising from how outputs may be used

Health, care and telecare deployments

Complete the Health, Care and Telecare Deployment pathway where the use case is primarily associated with:

- telecare
- care services
- support services
- wellbeing support
- safeguarding activities
- healthcare provision
- social care provision
- services intended to monitor, support, protect, or intervene in relation to an individual's wellbeing or care needs

Examples may include:

- Telecare Support
- Fall Detection
- Voice Related Care
- other care-, support-, wellbeing-, or safeguarding-related deployments

The Health, Care and Telecare Deployment pathway focuses on identifying concerns relating to:

- service, support, or care arrangements
- safeguarding responsibilities
- provider, healthcare, social care, telecare, or support-service involvement
- information-sharing arrangements
- response, escalation, or intervention arrangements
- communication, explanation, onboarding, or expectation-setting activities

Specific guidance for smart locks / door entry

Smart Locks / Door Entry is the primary use case where pathway selection may depend significantly on deployment context and the intended use of outputs.

For example:

- where Smart Locks / Door Entry are used primarily to manage access to buildings, communal areas, contractor access, or property-management activities, the Place-Based Deployment pathway will normally be appropriate
- where Smart Locks / Door Entry are used to control access to a tenant's home, or where outputs may influence actions, decisions, investigations, interventions, or other responses affecting tenants, the Tenant Affecting Deployment pathway will normally be appropriate

Where both circumstances apply, complete both pathways.

Applying pathways in different deployment environments

The selected pathway should reflect both the use case and the deployment environment.

Particular consideration may be required where deployments operate within:

- temporary accommodation
- homeless accommodation
- supported accommodation
- other environments where occupancy may be more transient
- environments where support providers, care workers, healthcare providers, social care organisations, or partner organisations may play a significant role

In these situations, communication, engagement, onboarding, support arrangements, service coordination, accountability arrangements, and organisational involvement may differ from standard tenancy-based housing.

5.4.2 Place-based pathway

The purpose of this pathway is not to replace project planning, operational delivery planning, procurement activities, or technical implementation planning.

Instead, it focuses on concerns that may affect how the intended deployment is governed, communicated, documented, implemented, or operated within the organisation's existing legal, governance, tenancy, accountability, and organisational obligations.

Place-based deployment assessment

Table 35 Place-based deployment assessment

Concerns	Applies
Existing tenancy agreements, occupancy agreements, licences, or other documentation associated with the intended deployment should be reviewed and, where necessary, updated or adapted to reflect the intended deployment.	☐
The communication, transparency, onboarding, consultation, engagement, or expectation-setting activities appropriate to the intended deployment have been identified, taking account of the deployment environment and those affected by the deployment.	☐
The access, installation, inspection, maintenance, replacement, removal, or other operational arrangements appropriate to the intended deployment and deployment environment have been identified.	☐
The intended deployment has been reviewed to determine whether existing landlord, property, safety, housing management, or other organisational obligations create requirements that should be reflected in communications, documentation, access arrangements, operational arrangements, or other deployment activities.	☐
The Governance Flag(s), Legal Guardrails, or deployment context indicate that input from relevant internal teams, specialists, advisers, delivery organisations, or partner organisations should be obtained before deployment proceeds.	☐

Concerns	Applies
Other governance, legal, tenancy, transparency, accountability, organisational-obligation, or deployment-specific concerns should be addressed before deployment proceeds.	☐

Guidance

Communication, transparency, onboarding, consultation, engagement, expectation-setting, access, and operational arrangements may differ depending on the deployment environment.

For example:

- occupied homes may require tenant communications, engagement activity, and access arrangements
- new-build homes may require onboarding information, transparency information, and documentation to be established before occupation
- void properties may require information and arrangements to be established before re-letting
- communal areas may require arrangements appropriate to affected residents, visitors, buildings, or services

Concerns identified

For each concern identified, briefly record what should be addressed before deployment proceeds.

Table 36 Place-based deployment assessment concerns identified

Concern Identified	Action Required

Examples may include:

- review of tenancy agreements or associated documentation
- tenant information updates
- communication or engagement activities
- access arrangements for installation or maintenance
- alignment with housing condition, repairs, damp and mould, building safety, or fire safety processes
- input from relevant internal teams, specialists, advisers, delivery organisations, or partner organisations
- other governance, legal, tenancy, transparency, accountability, organisational-obligation, or deployment-specific actions

Outcome

Table 37 Place-based deployment assessment outcome

Outcome	Response
No additional concerns identified that should be addressed before deployment proceeds	☐
One or more concerns identified that should be addressed before deployment proceeds	☐

Confirmation

This section should be confirmed by an individual with sufficient knowledge of the intended deployment.

Where relevant, input should be obtained from appropriate teams, specialists, advisers, delivery organisations, service providers, or partner organisations before recording the outcome.

Table 38 Place-based deployment assessment confirmation

Confirmed by	Role	Date

The individual completing this section confirms that the intended deployment has been reviewed using the applicable 5.3 pathway and that any concerns requiring review, clarification, agreement, communication, updates, or other action before deployment proceeds have been identified and recorded.

Any concerns identified through this pathway should be carried forward into Section 5.4.

5.4.3 Tenant affecting deployments

The purpose of this pathway is not to determine how an organisation should respond to specific events, alerts, behaviours, or outcomes.

Instead, it focuses on identifying concerns that may affect how outputs from the intended deployment are interpreted, used, communicated, governed, or acted upon where those outputs may affect tenants, their use of the home, or decisions relating to them.

Tenant-affecting deployment assessment

Table 39 Tenant affecting deployment assessment

Concern	Applies
The intended deployment has been reviewed to determine whether outputs may influence actions, decisions, investigations, interventions, communications, or other responses affecting tenants.	☐
The transparency, communication, engagement, consultation, onboarding, or expectation-setting activities appropriate to the intended deployment have been identified, taking account of the deployment environment and those affected by the deployment.	☐
The intended deployment has been reviewed to determine whether tenancy rights, use of the home, privacy considerations, or other tenant-related implications should be reflected in associated communications, documentation, governance arrangements, or operational arrangements.	☐
The intended deployment has been reviewed to determine whether safeguards, human oversight, accountability arrangements, or decision-making controls should be clarified before deployment proceeds.	☐
The Governance Flag(s), Legal Guardrails, or deployment context indicate that input from relevant internal teams, specialists, advisers, delivery organisations, or partner organisations should be obtained before deployment proceeds.	☐
Other governance, legal, tenancy, transparency, accountability, safeguarding, organisational-obligation, or deployment-specific concerns should be addressed before deployment proceeds.	☐

Guidance

This pathway is particularly relevant where deployment outputs may:

- indicate presence, absence, activity, behaviour, habits, or routines
- influence actions, decisions, investigations, interventions, or communications affecting tenants
- affect how a tenant uses their home
- create privacy, transparency, accountability, safeguarding, or tenancy-related implications
- be used alongside other information to inform actions relating to tenants

Examples may include:

- Occupancy / Motion Monitoring
- Appliance Monitoring
- Thermal Imaging
- Internal CCTV
- Combined deployments where outputs may be used to inform actions affecting tenants
- Smart Locks / Door Entry where outputs may influence actions, decisions, investigations, interventions, or other responses affecting tenants

Concerns identified

For each concern identified, briefly record what should be addressed before deployment proceeds.

Table 40 Tenant affecting deployment assessment concerns identified

Concern Identified	Action Required

Examples may include:

- clarification of how outputs may be used
- transparency and tenant information requirements
- review of tenancy-related implications
- safeguards relating to interpretation of outputs
- human oversight requirements
- governance controls relating to decisions or actions affecting tenants
- clarification of accountability arrangements
- input from relevant internal teams, specialists, advisers, delivery organisations, or partner organisations
- other governance, legal, tenancy, transparency, accountability, safeguarding, organisational-obligation, or deployment-specific actions

Outcome

Table 41 Tenant affecting deployment assessment outcome

Outcome	Response
No additional concerns identified that should be addressed before deployment proceeds	☐
One or more concerns identified that should be addressed before deployment proceeds	☐

Confirmation

This section should be confirmed by an individual with sufficient knowledge of the intended deployment.

Where relevant, input should be obtained from appropriate teams, specialists, advisers, delivery organisations, service providers, or partner organisations before recording the outcome.

Table 42 Tenant affecting deployment assessment confirmation

Confirmed by	Role	Date

The individual completing this section confirms that the intended deployment has been reviewed using the applicable 5.3 pathway and that any concerns requiring review, clarification, agreement, communication, updates, or other action before deployment proceeds have been identified and recorded.

Any concerns identified through this pathway should be carried forward into Section 5.4.

5.4.4 Health, care and telecare deployments

The purpose of this pathway is not to replace service planning, care planning, safeguarding processes, operational delivery planning, procurement activities, or technical implementation planning.

Instead, it focuses on concerns that may affect how the intended deployment is governed, communicated, documented, supported, delivered, or operated within existing legal, governance, safeguarding, accountability, health, care, support, and organisational obligations.

Health, care and telecare deployment assessment

Table 43 Health care and telecare deployment assessment

Concern	Applies
Existing service arrangements, support arrangements, care-related arrangements, information-sharing arrangements, or other documentation associated with the intended deployment should be reviewed and, where necessary, updated or adapted to reflect the intended deployment.	☐
The communication, explanation, onboarding, engagement, consultation, transparency, or expectation-setting activities appropriate to the intended deployment have been identified, taking account of those affected by the deployment and the deployment environment.	☐
The intended deployment has been reviewed to determine whether service, support, safeguarding, monitoring, response, escalation, intervention, or other arrangements create governance, accountability, information-sharing, or organisational responsibilities that should be clarified before deployment proceeds.	☐
The intended deployment has been reviewed to determine whether existing safeguarding, health, care, wellbeing, support, housing support, or other organisational obligations create requirements that should be reflected in communications, documentation, service arrangements, operational arrangements, or other deployment activities.	☐
The Governance Flag(s), Legal Guardrails, or deployment context indicate that input from relevant internal teams, specialists, advisers, delivery organisations, service providers, healthcare organisations, social care organisations, telecare providers, or partner organisations should be obtained before deployment proceeds.	☐
Other governance, legal, safeguarding, accountability, information-sharing, organisational-obligation, or deployment-specific concerns should be addressed before deployment proceeds.	☐

Guidance

This pathway is particularly relevant where a deployment is intended to monitor, support, protect, assist, safeguard, or intervene in relation to an individual's wellbeing, health, care needs, safety, or support requirements.

Examples may include:

- Telecare Support
- Fall Detection
- Voice Related Care
- wellbeing monitoring deployments
- safeguarding-focused deployments
- support-service deployments
- care-related deployments

Particular consideration may be required where:

- healthcare organisations are involved
- social care organisations are involved
- telecare providers are involved
- support providers are involved
- information may be shared between organisations
- outputs may contribute to support, safeguarding, intervention, escalation, or care-related activities

Additional considerations for supported, homeless and temporary accommodation

Consideration may be required where Health, Care and Telecare deployments operate within:

- supported accommodation
- homeless accommodation
- temporary accommodation
- Housing First or other intensive support environments
- accommodation where healthcare, social care, housing support, telecare providers, third-sector organisations, or other support services are actively involved in supporting residents

In these environments, organisations should consider whether:

- support workers, key workers, healthcare providers, social care organisations, telecare providers, housing support providers, or other partner organisations should be involved in deployment planning
- communication, onboarding, engagement, transparency, and expectation-setting activities should be coordinated across the organisations supporting residents
- accountability for reviewing, interpreting, sharing, escalating, or acting upon deployment outputs has been clearly established
- information-sharing, safeguarding, wellbeing, support, or intervention arrangements should be clarified before deployment proceeds
- the intended deployment creates additional governance considerations because residents may move between accommodation, support arrangements, or service providers more frequently than in standard tenancy-based housing
- responsibilities for responding to alerts, concerns, interventions, or other outputs generated by the deployment are clearly understood before deployment proceeds

Concerns identified

For each concern identified, briefly record what should be addressed before deployment proceeds.

Table 44 Health care and telecare deployment assessment concerns identified

Concern Identified	Action Required

Examples may include:

- review of service, support, safeguarding, or care-related arrangements
- review of information-sharing arrangements
- clarification of provider, support, telecare, healthcare, or social care involvement
- communication, onboarding, or transparency activities
- clarification of governance, accountability, information-sharing, or organisational responsibilities associated with monitoring, response, escalation, intervention, or support arrangements
- input from relevant internal teams, specialists, advisers, delivery organisations, healthcare organisations, social care organisations, telecare providers, or partner organisations
- other governance, legal, safeguarding, accountability, information-sharing, organisational-obligation, or deployment-specific actions

Outcome

Table 45 Health care and telecare deployment assessment outcome

Outcome	Response
No additional concerns identified that should be addressed before deployment proceeds	☐
One or more concern identified that should be addressed before deployment proceeds	☐

Confirmation

This section should be confirmed by an individual with sufficient knowledge of the intended deployment.

Where relevant, input should be obtained from appropriate teams, specialists, advisers, delivery organisations, service providers, healthcare organisations, social care organisations, telecare providers, or partner organisations before recording the outcome.

Table 46 Health care and telecare deployment assessment confirmation

Confirmed by	Role	Date

The individual completing this section confirms that the intended deployment has been reviewed using the applicable 5.3 pathway and that any concerns requiring review, clarification, agreement, communication, updates, or other action before deployment proceeds have been identified and recorded.

Any concerns, actions, conditions, dependencies, governance concerns, legal considerations, transparency requirements, safeguards, organisational responsibilities, or specialist input requirements identified through the Section 5.3 pathways should be considered when completing Table 52 (Governance and Deployment Decision). Any concerns identified through this pathway should be carried forward into Section 5.4.

5.5 Governance and deployment decision

This section represents the primary governance decision point within the handbook. The decision recorded here should reflect the cumulative outputs of all previous steps and provide the formal governance position for the intended deployment.

The governance and deployment decision should be based on the Governance Classification recorded in Table 15, the Governance Capability Assessment recorded in Table 16, the Tenancy and Legal Governance Engagement Level recorded in Table 21, and the Step 4 outcome recorded in Table 23.

It also supports organisations in recording the governance and deployment decision for the intended deployment.

By this stage, the organisation should have:

- reviewed the outputs of the previous handbook steps
- confirmed the governance arrangements required for the intended deployment
- confirmed accountability and organisational involvement
- identified any governance, legal, tenancy, transparency, safeguarding, service, support, organisational-obligation, or other deployment concerns that should be addressed before deployment proceeds

The purpose of this section is not to repeat earlier assessments or undertake further governance analysis.

Instead, it supports organisations in:

- confirming that the handbook assessment remains current
- determining whether the intended deployment is ready to proceed
- identifying whether any concerns must first be addressed
- determining whether additional review, approval, or specialist input is required before deployment proceeds
- recording the final governance and deployment decision in Table 52 .

The decision recorded in Table 52 should reflect:

- the relevant use case profile(s), Governance Flag(s), and Legal Guardrails recorded in Table 15 (Governance Classification)
- the intended deployment context
- the governance arrangements and accountability arrangements established through Step 5
- any concerns identified through Section 5.3.

The level of review, approval, and specialist involvement should be proportionate to the intended deployment.

Lower-impact deployments may be capable of proceeding through existing governance arrangements.

Deployments involving more significant governance, legal, tenancy, transparency, safeguarding, accountability, service, support, organisational, or deployment considerations may require additional review, approval, or specialist input before deployment proceeds.

A deployment decision should only be recorded where the organisation is satisfied that the assessments completed through the handbook remain current and accurately reflect the intended deployment.

5.5.1 Confirming the assessment remains current

Before recording a governance and deployment decision, review the assessments completed through the handbook and determine whether any material changes have occurred that may affect the intended deployment.

The purpose of this section is not to repeat earlier assessments. Instead, it helps confirm that the governance and deployment decision is based on the current position and that the outputs developed through the handbook remain applicable.

Assessment remains current check

Table 47 Assessment remains current check

Since completing the relevant handbook assessments, has there been any material change relating to:	Yes	No
Legislation, regulation, guidance, policies, standards, or organisational requirements relevant to the intended deployment	☐	☐
Governance arrangements, accountability arrangements, organisational structures, or decision-making responsibilities associated with the intended deployment	☐	☐
The intended use of outputs generated by the deployment	☐	☐
The deployment scope, deployment environment, participating organisations, or delivery model	☐	☐
Data sources, technologies, integrations, analytics capabilities, AI tools, or automated processing associated with the intended deployment	☐	☐
Information-sharing, service, support, safeguarding, care, telecare, or operational arrangements associated with the intended deployment	☐	☐
Other changes that may affect the governance assessment or deployment decision	☐	☐

Guidance

Material changes may include, for example:

- changes in legislation, regulation, guidance, policies, standards, or organisational requirements
- changes to Governance Flags, Legal Guardrails, governance arrangements, or accountability arrangements
- changes to the intended use of deployment outputs
- introduction of new technologies, analytics capabilities, AI tools, or automated processing
- addition of new data sources, integrations, suppliers, partners, service providers, healthcare organisations, social care organisations, or support organisations
- changes to deployment scope, deployment environment, or participating residents
- new information-sharing, safeguarding, support, telecare, or operational arrangements

Where changes have been identified, determine whether they can be addressed within the current assessment or whether relevant earlier sections of the handbook should be revisited before a governance and deployment decision is recorded.

Changes may also arise from procurement, supplier engagement, mobilisation, implementation planning, or other organisational readiness activities taking place alongside completion of the handbook. These activities should only be considered where they create governance, legal,

tenancy, transparency, accountability, safeguarding, information-sharing, organisational, or deployment-governance implications that may affect the assessment or deployment decision.

Changes identified

If any changes have been identified, briefly record them below.

Table 48 Assessment remains current check changes identified

Change Identified	Potential Impact on the Deployment

Outcome

Table 49 Assessment remains current check outcome

Outcome	Response
No material changes identified. The handbook assessments remain current.	☐
One or more changes identified. Determine whether relevant earlier sections of the handbook should be revisited before a deployment decision is recorded.	☐

Confirmation

Table 50 Assessment remains current check confirmation

Confirmed by	Role	Date

The individual completing this section confirms that the handbook assessments have been reviewed and that the recorded outcome accurately reflects whether the assessments remain current for the intended deployment.

5.5.2 Recording the governance and deployment decision

Complete Table 51 only after Table 47-Table 50 have been completed and the assessment remains current outcome has been recorded.
Complete this section once:

- the relevant handbook assessments have been completed
- governance arrangements and accountability have been confirmed
- Section 5.4 has been completed

The purpose of this section is to record the governance and deployment decision for the intended deployment, taking account of:

- the governance classification recorded in Table 15
- the Step 4 outcome recorded in Table 23**.**

The decision recorded in this section relates only to concerns within the scope of this handbook. It does not replace organisational decisions relating to procurement, commercial arrangements, funding, project delivery, implementation planning, deployment scheduling, or other activities outside the governance, legal, tenancy, transparency, safeguarding, accountability, information-sharing, and organisational-obligation considerations addressed by the handbook.

This section does not repeat earlier assessments or undertake additional governance analysis. Instead, it records whether the organisation is satisfied that the intended deployment is ready to proceed based on the information gathered through the handbook.

When recording the deployment decision, consider whether any procurement, supplier, mobilisation, implementation, readiness, or organisational activities have introduced new governance, legal, tenancy, transparency, accountability, safeguarding, information-sharing, organisational, or deployment-governance considerations that should be reflected in the decision.

The level of review, approval, and specialist involvement should be proportionate to the intended deployment.

Governance and deployment decision

Table 51 Governance deployment decision

Decision Area	Recorded Position
Intended deployment (Table 1)	
Use case(s) covered by this decision (Table 15)	
Relevant Governance Flag(s) considered (Table 15)	
Relevant Legal Guardrails considered (Table 15)	
Recorded positions have been completed in Section 5.4 (Table 38, Table 42 and Table 46)	
Outstanding conditions, actions or dependencies arising from assessment in Section 5.4 (Table 36, Table 40 and Table 44)	
Assessment remains current, review completed (Table 47 to Table 50)	☐ Yes ☐ No

Deployment decision

Record the governance and deployment decision for the intended deployment in Table 52. Select one response in this table.

Table 52 Deployment decision

Outcome	Response
Proceed	☐
Proceed once identified concerns have been addressed	☐
Further review, approval, or specialist input required before deployment proceeds	☐

Table 52 records the primary governance and deployment decision arising from Step 5. All subsequent records, approvals, confirmations, and outcomes should be consistent with the decision recorded in this table.

Decision guidance

Record a decision of **"Proceed"** where:

- governance arrangements have been established
- accountability arrangements have been established
- assessments remain current
- no outstanding concerns remain within the scope of this handbook that should be addressed before deployment proceeds
- where the deployment affects tenants, residents, or other individuals, the organisation is satisfied that appropriate transparency, safeguards, accountability, oversight, and governance arrangements are in place and reflect the relationship between the organisation and those affected by the deployment

The organisation may continue to undertake procurement, supplier engagement, mobilisation, implementation planning, deployment planning, or other delivery activities outside the scope of the handbook, provided these do not create unresolved governance, legal, tenancy, transparency, safeguarding, accountability, information-sharing, or organisational-obligation concerns.

Record a decision of "Proceed" once identified concerns have been addressed, where:

- one or more concerns have been identified through the Section 5.3 pathway assessment(s)
- those concerns can reasonably be addressed before deployment proceeds
- the organisation remains satisfied that the intended deployment can proceed once those concerns have been addressed
- additional communication, transparency, safeguarding, accountability, oversight, documentation, governance, information-sharing, or organisational arrangements are required before deployment proceeds.

Record a decision of "Further review, approval, or specialist input required before deployment proceeds" where:

- significant governance, legal, tenancy, safeguarding, accountability, information-sharing, organisational, or deployment concerns remain unresolved
- required governance arrangements or accountability arrangements are not yet established
- required review, approval, or specialist input has not yet been obtained
- changes identified through Section 5.4.1 (Table 47, Table 48) may require earlier handbook sections to be revisited before a deployment decision can be recorded
- significant concerns remain regarding transparency, accountability, safeguards, oversight, fairness, or the appropriateness of the deployment in relation to those affected by it

Decision rationale

Briefly record the reasons for the decision.

Where relevant, include:

- how identified concerns have been addressed
- why additional review or approval is or is not required
- how transparency, accountability, safeguards, and oversight have been considered
- where the deployment affects tenants, residents, or other individuals, how the organisation has taken account of the relationship between the organisation and those affected by the deployment when reaching the decision

Table 53 Decision rationale

Decision	Rationale

Approval and review

Table 54 Decision rational recording and approval

Decision Recorded By	Role	Date
Review or Approval Obtained from	**Role**	**Date**

Where relevant, this section should reflect any governance, legal, tenancy, safeguarding, specialist, or senior review obtained before the decision is recorded.

Partner organisation confirmation

Where partner organisations have a defined role in receiving, interpreting, sharing, reviewing, acting upon, or otherwise using outputs generated by the intended deployment, record whether appropriate confirmation has been obtained that their role and responsibilities are understood.

Partner organisations may include, for example:

- healthcare organisations
- social care organisations
- telecare providers
- housing support providers
- support-worker or key-worker services
- local authority services
- third-sector organisations
- other delivery or partner organisations involved in the deployment

This section is not intended to create a contractual approval process. Instead, it helps organisations demonstrate that relevant partner organisations have been involved appropriately and that their role in the deployment is understood.

Table 55 Partner organisation confirmation

Organisation	Role in Deployment	Confirmation Obtained
		☐
		☐
		☐

Confirmation

The individual completing this section confirms that:

- the intended deployment has been reviewed using the relevant sections of the handbook
- the recorded decision reflects the current governance position for the intended deployment
- any identified concerns that should be addressed before deployment proceeds have been recorded
- the level of review and approval obtained is proportionate to the intended deployment

The decision recorded in Table 52 should be used as the formal governance and deployment decision for the intended deployment and should be carried forward into the conclusion of Step 5.

Confirmation may include, where appropriate:

- agreement on responsibilities associated with the deployment
- agreement on responsibilities relating to deployment outputs
- agreement on information-sharing arrangements
- agreement on safeguarding, support, intervention, or escalation responsibilities
- acknowledgement of accountability, governance, or operational responsibilities relevant to the deployment

The level of confirmation obtained should be proportionate to the intended deployment and the role played by the partner organisation.

Table 56 Partner organisation confirmation recorded

Decision Recorded By	Role	Date

5.6 Step 5 Conclusion

The Step 5 outcome recorded in Table 57 should reflect the governance and deployment decision recorded in Table 52 together with any associated conditions, actions, reviews, approvals, specialist input requirements, or reassessment activities identified through.

Table 52 records the governance and deployment decision. Table 57 records the formal Step 5 outcome arising from that decision.

Governance and deployment decision recorded. No further concerns identified within the scope of Step 5. should be recorded where:

- governance arrangements and accountability arrangements have been established
- the handbook assessment remains current
- any relevant review or approval has been obtained
- no outstanding concerns remain within the scope of the handbook

Governance and deployment decision recorded, subject to identified concerns being addressed before deployment proceeds. should be recorded where:

- one or more concerns have been identified through Step 5
- those concerns can reasonably be addressed before deployment proceeds
- the organisation remains satisfied that deployment can proceed once those concerns have been addressed

Further review, approval, specialist input, or reassessment is required before the governance and deployment decision can be confirmed. should be recorded where:

- significant governance, legal, tenancy, safeguarding, accountability, information-sharing, organisational, or deployment concerns remain unresolved
- required governance arrangements or accountability arrangements are not yet established
- required review, approval, or specialist input has not yet been obtained
- changes identified through Section 5.4.1 indicate that relevant earlier sections of the handbook may need to be revisited before a governance, and deployment decision can be confirmed

5.6.1 Step 5 Outcome

The governance and deployment decision recorded in Table 52, together with the Step 5 outcome recorded in Table 57, should be treated as the baseline governance position for the intended deployment and carried forward into Step 6.

Table 57 Step 5 outcome

Outcome	Response
Governance and deployment decision recorded. No further concerns identified within the scope of Step 5 (Table 52).	☐
Governance and deployment decision recorded, subject to identified concerns being addressed before deployment proceeds (Table 52).	☐
Further review, approval, specialist input, or reassessment required before the governance and deployment decision can be confirmed (Table 47, Table 52).	☐

5.7 Step 5 Completion

The outputs of Step 5, including the governance and deployment decision recorded in Table 52 and the Step 5 outcome recorded in Table 57, should be carried forward into Step 6 and used as the baseline governance position for the intended deployment.

Table 58 Step 5 completion

Completed By	Role	Date

The individual completing this step confirms that:

- the Step 5 governance activities have been completed;
- the recorded outcome reflects the organisation's current governance position;
- any required actions, conditions or approvals have been recorded; and
- the outputs are ready to be carried forward into Step 6.

6 Step 6 – Governance Review and Reassessment

Figure 8 Introducing Step 6's purpose, outputs and relevant principles



Step 6 consists of three stages. First, organisations review whether the governance position established through Steps 1 to 5 remains current. Second, organisations assess whether the deployment has evolved from the deployment originally assessed and approved. Third, organisations review whether the governance assumptions established through the handbook continue to hold in practice. The outputs from these reviews help determine whether the current governance position remains appropriate or whether relevant earlier sections of the handbook should be revisited.

The purpose of this step is not to manage day-to-day operations, technical maintenance, contractor performance, or service delivery activity. Instead, it focuses on whether any changes or issues have arisen that affect the governance, legal, accountability, transparency, safeguarding, information-sharing, or organisational-obligation assumptions on which the deployment decision was based. Partner and third-party changes remain in scope for lifecycle governance review.

This step should be used to confirm whether:

- the governance and deployment decision recorded in Step 5 remains current
- the intended use of outputs remains the same as originally assessed
- governance arrangements, accountability arrangements, and organisational responsibilities remain appropriate
- any changes in legislation, regulation, guidance, policy, technology, data use, deployment scope, delivery model, participating organisations, or deployment environment create a need for review or reassessment
- any issues affecting the reliability, accuracy, completeness, or trustworthiness of deployment outputs create governance implications that should be reviewed
- any changes or issues mean that relevant earlier sections of the handbook should be revisited

This step should not be used to repeat the full handbook assessment where no relevant changes or issues have emerged. Instead, it provides a proportionate way for organisations to determine whether the governance position established through the handbook still holds, or whether reassessment is required.

The focus of this step is governance review and reassessment, not operational performance management.

For example, this step is not intended to ask whether devices are being maintained appropriately or whether operational processes are being followed in general. However, where operational issues create governance implications — for example because outputs are unreliable, false positives or false negatives are occurring, inappropriate interventions are being triggered, or safeguards are no longer operating as intended — those issues should be considered in this step.

This section should be completed by an individual with sufficient knowledge of the deployment and its governance arrangements. Where appropriate, input should be obtained from other teams, specialists, service providers, partner organisations, or advisers. The effectiveness of this review depends upon the organisation maintaining appropriate ownership of the governance position established through Steps 1 to 5

This step should be completed with reference to the recorded outputs of Step 5 and any changes, events, issues, or developments that have occurred since the governance and deployment decision was recorded. **Step 6 should be completed** with reference to the governance and deployment decision recorded in Table 52 and the Step 5 outcome recorded in Table 57.

By the end of this step, the organisation should have reviewed whether:

- the governance position established through Steps 1 to 5 continues to remain current
- the deployment continues to operate in the manner originally assessed and approved
- governance assumptions continue to hold in practice
- any changes or observations indicate that relevant earlier sections of the handbook should be revisited

The purpose of Step 6 is therefore to ensure that governance remains proportionate, current, and appropriate throughout the lifecycle of the deployment, and that organisations have a clear route back into the handbook where changes or issues require further review.

Refer to Annex C.6 (page 240) which provides a set of best practices to assist with completing Step 6 Governance Review and Reassessment.

6.1 Reviewing whether the governance position remains current

This section supports organisations in reviewing whether the governance position established through Steps 1 to 5 remains current.

Using the outputs from the handbook and any changes that have occurred since the governance and deployment decision was recorded, determine whether any material changes have occurred that may affect the governance position established through the handbook.

This review should be completed with appropriate input from relevant individuals, teams, specialists, advisers, service providers, or partner organisations where required.

This section should be completed whenever material changes arise that may affect the governance position established through the handbook and should also be completed at review intervals determined by the organisation, taking account of the nature, complexity, and sensitivity of the deployment.

6.1.1 Governance position remains current check

Review each statement in Table 59 and record whether a material change has occurred since the governance and deployment decision was recorded (which took place at the end of Step 5).

Table 59 Governance position remains current check

Governance position check	Yes	No
Legislation, regulation, guidance, policy, standards, or organisational requirements relevant to the deployment	☐	☐
Governance arrangements, accountability arrangements, organisational structures, or decision-making responsibilities associated with the deployment	☐	☐
The intended use of outputs generated by the deployment	☐	☐
The deployment scope, deployment environment, participating organisations, or delivery model	☐	☐
Data sources, technologies, integrations, analytics capabilities, AI tools, or automated processing associated with the deployment	☐	☐
Information-sharing, service, support, safeguarding, care, telecare, or organisational arrangements associated with the deployment	☐	☐
Other changes that may affect the governance position established through the handbook	☐	☐

Table 59 provides the primary governance review output for Step 6 and should be considered alongside the deployment review and governance assumptions review completed later in this step.

6.1.2 Changes identified

If any changes have been identified, briefly record them below.

Table 60 Changes identified

Change Identified	Potential Governance Impact

6.1.3 Guidance

Material changes may include:

- changes in legislation, regulation, guidance, policy, standards, or organisational requirements
- changes in governance arrangements, accountability arrangements, or organisational involvement
- changes in the intended use of outputs generated by the deployment
- changes in deployment scope, deployment environment, participating organisations, or delivery arrangements
- changes in technologies, data sources, integrations, analytics capabilities, AI tools, or automated processing
- changes in information-sharing, safeguarding, care, telecare, support, or organisational arrangements
- other changes that may affect the governance position established through the handbook

Where changes are identified, consider whether they affect the governance position established through Steps 1 to 5 and whether further review or reassessment may be required.

This section is not intended to trigger full reassessment automatically whenever a change occurs. Instead, it helps organisations determine whether any identified change may affect the governance position established through the handbook and whether additional review is required.

6.1.4 Confirmation

Table 61 Confirmation of governance position

Confirmed by	Role	Date

The individual completing this section confirms that the governance position established through Steps 1 to 5 has been reviewed and that the recorded outcome accurately reflects whether that governance position remains current.

6.2 Reviewing changes to the deployment

This section supports organisations in identifying whether the deployment has evolved, or is intended to evolve, from the deployment that was originally assessed and approved through the handbook.

Organisations should also consider whether the Tenancy and Legal Governance Engagement Level recorded in Table 21 continues to reflect how the deployment operates in practice.

The purpose of this section is not to determine whether reassessment is required. Instead, it helps organisations identify changes to the deployment that may mean it no longer operates in the manner originally assessed through Steps 1 to 5.

This section should be completed with reference to:

- the use case(s) originally assessed (Table 1)
- the deployment context originally assessed (Table 1)
- the governance and deployment decision recorded in Step 5 (Table 52)
- any current or proposed changes to how the deployment operates in practice

This review should be completed with appropriate input from relevant individuals, teams, specialists, advisers, service providers, or partner organisations where required.

6.2.1 Deployment change assessment

Consider whether the deployment has evolved, or is intended to evolve, in any of the following ways. When completing this assessment, organisations should compare the current deployment against the use case definition established in Step 1 and the operational assessment recorded in Step 4.

Compare the current deployment with the deployment originally assessed through the handbook and identify any changes that apply and record in Table 62.

Table 62 Deployment change assessment

Consider whether:	Applies
The purpose of the deployment has changed or expanded beyond what was originally assessed through the handbook.	☐
Outputs generated by the deployment are being used, shared, interpreted, combined, or acted upon differently from the approach originally assessed.	☐
Additional organisations, teams, providers, partners, contractors, or individuals are involved in receiving, reviewing, interpreting, sharing, or acting upon deployment outputs.	☐
Governance ownership, accountability arrangements, organisational responsibilities, decision-making responsibilities, or oversight arrangements associated with the deployment have changed.	☐
The deployment has expanded beyond the properties, buildings, resident groups, services, locations, or deployment environments originally assessed through the handbook.	☐
The deployment is operating, or is intended to operate, within additional environments that were not originally assessed through the handbook.	☐
Additional technologies, use cases, data sources, integrations, analytics capabilities, AI tools, automated processing, or monitoring capabilities have been introduced or combined with the deployment.	☐
Previously separate use cases, technologies, datasets, or outputs are now being combined, linked, analysed together, or used together in ways not originally assessed through the handbook.	☐
Other changes have occurred that mean the deployment no longer operates in the way originally assessed and approved through the handbook.	☐

Changes identified through Table 62 should be assessed carefully, as they may indicate that the deployment no longer reflects the deployment originally assessed and approved through the handbook.

6.2.2 Changes identified

If any changes have been identified, briefly record them below.

Table 63 Changes identified

Change Identified	Description of the Changes

6.2.3 Guidance

Examples may include:

- deployment outputs being used for an additional purpose
- deployment outputs being shared with additional teams, organisations, or partner organisations
- new service providers, telecare providers, healthcare organisations, social care organisations, housing support providers, or other partner organisations becoming involved
- changes to governance ownership, accountability arrangements, organisational responsibilities, or oversight arrangements
- deployment expanding into additional properties, services, resident groups, locations, or deployment environments
- deployment expanding into supported accommodation, temporary accommodation, homeless accommodation, Housing First environments, or other previously unassessed environments
- additional technologies, use cases, data sources, integrations, analytics capabilities, AI tools, automated processing, or monitoring capabilities being introduced
- previously separate use cases, technologies, systems, datasets, or outputs being used together

This section is intended to identify whether the deployment differs materially from the deployment originally assessed and approved through the handbook.

The implications of any identified changes, including whether additional review, reassessment, or other action is required, are considered later in Step 6.

6.2.4 Confirmation

Table 64 Confirmation of changes identified

Confirmed by	Role	Date

The individual completing this section confirms that the deployment has been reviewed and that the recorded outcome accurately reflects whether the deployment has evolved, or is intended to evolve, from the deployment originally assessed and approved through the handbook.

6.3 Reviewing whether governance assumptions continue to hold

This section supports organisations in reviewing whether the governance assumptions established through Steps 1 to 5 continue to hold in practice.

The purpose of this section is not to assess operational performance, manage incidents, assign responsibility for resolving issues, or determine whether reassessment is required. Instead, it helps organisations identify whether there are indications that the governance, legal, accountability, transparency, safeguarding, information-sharing, or organisational assumptions on which the deployment was originally approved may no longer be operating as intended.

This section should be completed with reference to:

- the governance and deployment decision recorded in Table 52

- experience gained through operating the deployment
- feedback received from relevant teams, service providers, partner organisations, tenants, residents, service users, or other stakeholders
- any concerns, observations, issues, reviews, complaints, audits, investigations, or other relevant information that has emerged since deployment.

This review should be completed with appropriate input from relevant individuals, teams, specialists, advisers, service providers, or partner organisations where required.

6.3.1 Governance assumptions review

Consider whether there are indications that any of the following assumptions may no longer fully reflect how the deployment operates in practice. Consider whether the governance assumptions established through the handbook continue to reflect how the deployment operates in practice and complete Table 65.

This assessment should be undertaken with reference to the governance arrangements established through Table 30 and the responsibilities and accountability arrangements established through Table 32 and Table 33.

Table 65 Governance assumptions review

Consider whether:	Applies
There are indications that the reliability, accuracy, completeness, or trustworthiness of deployment outputs may no longer be consistent with the assumptions made when the deployment was originally approved.	☐
There are indications that deployment outputs may be producing unexpected, misleading, inconsistent, or unintended outcomes that were not originally anticipated.	☐
There are indications that outputs are being interpreted, reviewed, shared, communicated, or acted upon differently from what was originally understood or intended.	☐
Governance ownership, accountability arrangements, organisational responsibilities, decision-making responsibilities, or oversight arrangements are no longer operating in the way originally understood or intended.	☐
Transparency, communication, engagement, consultation, onboarding, or expectation-setting arrangements are no longer operating in the way originally envisaged.	☐
Information-sharing, safeguarding, support, care, telecare, intervention, escalation, or organisational arrangements are no longer operating in the way originally understood or intended.	☐
Governance controls, safeguards, approval arrangements, or oversight arrangements may no longer be operating as originally intended.	☐
Concerns, complaints, disputes, challenges, reviews, investigations, audits, regulatory engagement, legal review findings, or similar concerns have emerged that call into question assumptions made when the deployment was originally approved.	☐
Other observations, experiences, or information indicate that the governance position established through the handbook may no longer fully reflect how the deployment operates in practice.	☐

6.3.2 Observations identified

If any observations have been identified, briefly record them below.

Table 66 Governance assumptions review observations identified

Observation Identified	Description

6.3.3 Guidance

Examples may include:

- recurring false positives or false negatives
- outputs that appear inconsistent, unreliable, incomplete, or difficult to interpret
- outputs being interpreted differently by different teams or organisations
- accountability or governance ownership becoming unclear in practice
- safeguards or governance controls not operating as originally intended
- information-sharing arrangements not operating as expected
- telecare, support, safeguarding, intervention, or escalation responsibilities becoming unclear
- complaints, concerns, investigations, audits, or challenges relating to the deployment
- legal advice identifying concerns regarding how outputs are being used
- regulatory feedback, enquiries, engagement, or challenge
- audit findings affecting governance assumptions
- concerns regarding compliance with organisational policies or governance requirements
- concerns regarding information-sharing arrangements
- concerns regarding transparency, accountability, safeguarding, or decision-making arrangements
- transparency commitments not being delivered in the way originally envisaged
- stakeholders expressing concerns regarding how outputs are being used in practice.

This section is intended to identify whether experience gained during deployment suggests that governance assumptions established through the handbook may require further consideration.

It does not determine whether reassessment is required or whether the deployment should continue unchanged. Those considerations are addressed later in Step 6.

6.3.4 Confirmation

Table 67 Governance assumptions review confirmation

Confirmed by	Role	Date

The individual completing this section confirms that the deployment has been reviewed and that the recorded outcome accurately reflects whether there are indications that the governance assumptions established through Steps 1 to 5 continue to hold in practice.

Where reassessment is required, organisations should return to the earliest step affected by the identified change or observation. For example:

- changes to purpose, intended outcomes, or use of outputs should normally result in a return to Step 1
- changes affecting organisational readiness, governance capability, or governance requirements should normally result in a return to Step 2 or Step 3
- changes affecting how the deployment operates in practice should normally result in a return to Step 4
- changes affecting governance arrangements, safeguards, accountability arrangements, or deployment decisions should normally result in a return to Step 5.

6.4 Step 6 Conclusion

Step 6 should be revisited whenever material changes or governance-impacting observations arise, and at review intervals determined by the organisation. Where such changes or observations are identified, organisations should consider whether relevant earlier sections of the handbook should be revisited.

Step 6 is intended to support ongoing lifecycle governance rather than repeated reassessment. Organisations should revisit earlier handbook steps only where identified changes, observations, concerns, or governance issues indicate that the governance position established through the handbook may no longer remain valid.

The handbook does not require organisations to repeat all earlier steps whenever a change or observation is identified. Any review or reassessment should be proportionate to the nature of the change or observation identified.

6.5 Step 6 Outcome

The outcome recorded in Table 68 should reflect the findings recorded in Table 59, Table 62 and Table 65 and should take account of any identified governance impacts, deployment changes, observations, concerns, or unresolved issues arising from this review.

The identification of an action does not automatically require reassessment of earlier handbook steps. Reassessment should only be considered where the action arises from a material change, deployment change, governance concern, or observation that affects the governance position originally established through the handbook.

When determining the outcome of Step 6 (Table 68), organisations should consider whether:

- the governance position established through Steps 1–5 remains valid
- the deployment continues to operate in the manner originally assessed and approved
- governance assumptions continue to hold in practice
- any identified changes, observations, concerns, or actions materially affect the governance position established through the handbook.

Select the outcome in Table 68 that best reflects the findings of the Step 6 review.

Table 68 Step 6 outcome

Outcome	Response (select one outcome)
Governance position remains current. No further review required at this time	☐
Governance position remains current subject to identified actions being completed	☐
Relevant earlier sections of the handbook should be revisited	☐

Governance position remains current and no further review is required at this time should be selected where no material governance issues, changes, or concerns have been identified.

Governance position remains current, subject to identified actions being completed should be selected where actions have been identified but the governance position remains valid and reassessment is not required.

Reassessment of one or more earlier handbook steps is required should be selected where identified changes, observations, concerns, or governance issues mean that the governance position established through the handbook may no longer remain valid.

Table 69 Step 6 outcome review record

Reviewed by	Role	Date

The individual completing this review confirms that the governance position established through the handbook has been reviewed and that the recorded outcome accurately reflects the organisation's current position.

Annex A IoT use case definitions

A.1 Purpose of this Annex

This annex provides the **standard set of IoT use cases** to be used throughout the handbook (see Annex A.3 (page 173) for definitions associated with fields used in the use cases).

It ensures that:

- IoT deployments are described consistently
- use cases are clearly understood and applied
- governance decisions are based on a shared definition
- ambiguity and misinterpretation are reduced

How to use this annex

- Use **Step 1** – from Table 1 to identify the relevant use case(s)
- Refer to this annex where:
    - further detail or clarification is needed
    - there is uncertainty between similar use cases
    - multiple use cases may apply

Core principle

Use cases are defined by:

the purpose of the data and the decision it supports — not the sensors or technology used

A.2 Use case families

Use cases are grouped to support navigation and reflect housing functions.

Governance classification is determined by how the data is used — not by its category

The six use case families are:

1. Environmental and healthy homes
2. Fire and tenant safety
3. Telecare and health support
4. Behaviour and occupancy monitoring
5. Security and access control
6. Workforce and asset management

A.3 Use case definitions

Field	Content
Use Case	Name of the use case

Field	Content
Family	The family of the use cases
Governance Level	White, Green, Amber or Red
Governance Flag	The governance flag provides a concise description of the nature of the use case and the type of data and oversight it involves. It helps users quickly understand what kind of considerations apply (e.g. environmental, behavioural, safety, or operational) before working through the governance requirements
Purpose	The core definition of the use case: • what problem it solves • what the landlord is trying to achieve • what decisions or actions it supports This section ensures that: • the use case is clearly bounded • purpose is defined before data is collected or used • it aligns with the core principle: governance is driven by purpose, not technology
Tier Rationale	The maximum impact classification of the use case→ derived from Phase 3 and validated through Phase 4. The maximum reasonably foreseeable governance exposure associated with the use case, derived from the intended purpose, operational use, tenant impact, inference potential, tenancy implications, and potential severity of outcomes The Governance Level sets the baseline governance expectations associated with the use case profile, while actual governance implementation remains proportionate to deployment context, safeguards, and operational controls applied in practice. A short explanation of why the use case reaches this tier Reference to: Inference in-home monitoring health/vulnerability tenancy impact severity of outcomes What it means in practice ▪ Represents the maximum foreseeable impact ▪ Sets the baseline level of governance required Does not change based on how simple the deployment is
Legal Context	A high-level summary of the legal frameworks most relevant to this use case What it should include Key legislation and regulatory frameworks

Field	Content
	Human rights (where applicable) GDPR considerations (high-level, not detailed) What it means in practice Signals to the landlord which legal areas are engaged Ensures: early legal awareness appropriate escalation where needed
Governance Requirements	The minimum governance actions required for this use case What it should include: DPIA requirement (or not) Lawful basis requirement Need for auditability Requirement for human oversight Ownership and accountability Tenant consultation (where appropriate) is required as a separate activity from DPIA. Security and access control must be defined, including: user access management removal of access (e.g. former tenants) What it means in practice Translates the tier into required governance actions Ensures: consistency proportionality This is where the profile becomes instructional
Legal Guardrails	The non-negotiable boundaries that must never be crossed What it should include: Universal constraints (e.g.): no coercion no bypassing tenancy rights no restriction of access Any additional use case-specific constraints (if applicable) What it means in practice Defines:“ What must NEVER happen, regardless of benefit or justification” Applies:

Field	Content
	across all deployments regardless of tier
Lower-Impact Use	Two variations are provided, lower and higher-impact use cases. - A simple illustration of how governance intensity varies in practice. Helps landlords understand: “same use case, different governance intensity ”Reinforces: governance depends on how it is used, not just what it is- A simple illustration of how governance intensity varies in practice. Helps landlords understand: ▪ “same use case, different governance intensity – ”Reinforces: governance depends on how it is used, not just what it is Lower-impact: Typical or intended use Lower inference Operational outcomes Simpler governance
Higher-Impact Use	More complex or sensitive application Greater reliance on inference Use in more impactful contexts
Key Safeguards	The practical controls required to manage risk Safeguards drawn from the five families: Transparency (clear communications with tenants, active consultation where impact is significant) data lifecycle control governance & accountability technical assurance human oversight Only the most relevant safeguards for the use case What it means in practice Translates governance into: “What must actually be put in place ”Ensures: risks are controlled decisions are auditable tenant trust is maintained

Field	Content
	Safeguards must be enforceable through: tenancy agreements policies operational procedure

A.4 Environmental and healthy homes use case profiles

A.4.1 Damp and mould

Field	Content
Use Case	Damp & Mould
Family	Environmental & Health
Governance Level	Red
Governance Flag	Presence detection +potential behavioural inference + in-home monitoring
Purpose	Identify damp and mould risks to: - support housing standards - support timely maintenance and intervention - reduce risks to tenant health and safety
Tier Rationale	This use case can: - involve monitoring within the home (Article 8) - capture environmental conditions over time - indicate ventilation patterns and use of space - potential behavioural or occupancy inference - identify sustained conditions that may affect tenant health - create insight into how a property is being maintained or used Risk increases where: - data is interpreted to infer tenant behaviour (e.g. ventilation or lifestyle) - conditions are used to suggest tenant responsibility or fault - patterns are used to assess vulnerability without clear purpose - data is combined with other datasets (e.g. occupancy, energy use) - outputs are used in tenancy or enforcement decisions Risk increases where data is interpreted or used beyond its environmental or operational purpose.
Legal Context	Public task (housing management, health and safety) GDPR: - may involve personal data where linked to identifiable households - may involve inferred vulnerability - DPIA may be required Human rights considerations: - Article 8 (private and family life) engaged due to in-home monitoring
Governance Requirements	This use case requires enhanced governance aligned to its high impact profile Use must be: - clearly defined (property condition and health risk monitoring)

Field	Content
	- proportionate to intended purpose - limited to necessary scope Clear definition of purpose (environmental monitoring only) DPIA may be required depending on deployment All deployments must include: - clear tenant transparency - defined ownership and accountability - audit trail of monitoring and resulting actions - controls on interpretation of environmental data - human oversight where actions affect tenants The assigned tier reflects the maximum foreseeable impact of the use case. Governance applied in practice depends on how the use case is deployed. Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - infer behaviour beyond environmental purpose - attribute responsibility or fault to tenants without appropriate investigation - use data for tenancy enforcement without reassessment - combine with other datasets to create behavioural profiles without escalation Use must remain limited to environmental and property condition purposes. Any change of purpose requires reassessment of the use case and governance requirements.
Lower-Impact Use	Monitoring humidity and environmental conditions to: - identify damp risk - support maintenance and repairs Results in simpler governance.
Higher-Impact Use	Damp and mould data is: - analysed to infer behaviour or lifestyle - used to assess vulnerability or tenant responsibility - combined with other datasets - used in tenancy or enforcement decisions Results in enhanced governance required.
Key Safeguards	Clear tenant transparency regarding monitoring Strict purpose limitation (environmental and property condition only) Controls on interpretation and inference Separation from tenancy enforcement decisions Human oversight of actions affecting tenants

Field	Content
	Proportionate data collection and retention Auditability of monitoring and decision-making Safeguards must be documented, auditable, and enforceable through policies, tenancy agreements, and operational procedures, and regularly reviewed.

A.4.2 Indoor air quality (IAQ) and CO_2

Field	Content
Use Case	CO2 / IAQ
Family	Environmental & Health
Governance Level	Amber
Governance Flag	Environmental monitoring + potential behavioural inference + moderate oversight
Purpose	Monitor indoor air quality (e.g. CO_2 levels) to: - support healthy living environments - identify ventilation issues - reduce risks to tenant health - inform maintenance and housing quality interventions
Tier Rationale	This use case can: - monitor environmental conditions within the home (Article 8) - indicate ventilation quality and air conditions -potential behavioural or occupancy inference over time - support assessment of health-related risks - involve potential behavioural inference rather than direct behavioural monitoring Risk increases where: - data is interpreted to infer occupancy or behaviour - patterns are analysed beyond environmental purpose - data is linked to individuals or other datasets - outputs are used in tenancy or enforcement decisions Risk increases where data is interpreted or used beyond its environmental or operational purpose. Risk remains limited where the use case is confined to environmental monitoring and does not involve behavioural or tenancy-level decision-making
Legal Context	Public task (housing quality, health and safety) GDPR: - may involve personal data where linked to identifiable households - does not typically involve special category data - DPIA may be required Human rights considerations: - Article 8 (private and family life) engaged due to in-home monitoring
Governance Requirements	This use case requires enhanced governance aligned to its moderate impact profile Use must be: - clearly defined (environmental monitoring) - proportionate to intended purpose

Field	Content
	- limited to necessary scope Clear definition of purpose (air quality monitoring only) DPIA may be required depending on deployment All deployments must include: - clear tenant transparency - defined ownership and accountability - audit trail of data use - controls on interpretation of environmental data - human oversight where actions affect tenants Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - infer behaviour or lifestyle beyond environmental purpose - use data for tenancy enforcement without reassessment - combine with other datasets to create behavioural profiles without escalation - repurpose air quality data for behavioural monitoring Use must remain limited to environmental and health-related purposes Any change of purpose requires reassessment
Lower-Impact Use	Monitoring air quality to: - detect ventilation issues - support property improvements Results in simpler governance.
Higher-Impact Use	Air quality data is: - analysed to infer occupancy or behaviour - combined with other datasets - used to assess vulnerability or lifestyle - used in tenancy or enforcement decisions Results in enhanced governance required.
Key Safeguards	Clear tenant transparency Strict purpose limitation (environmental only) Controls on interpretation and inference Separation from tenancy enforcement Human oversight of decisions Proportionate data collection and retention Auditability of data use

Field	Content
	Safeguards must be documented, auditable, and enforceable through policies, tenancy agreements, and operational procedures, and regularly reviewed.

A.4.3 Leak detection

Field	Content
Use Case	Leak monitoring
Family	Asset & Infrastructure Monitoring
Governance Level	Amber
Governance Flag	Event-based environmental monitoring + minimal inference + asset-focused
Purpose	Monitor for the presence of water leaks within properties to: - prevent property damage - identify maintenance issues early - reduce risk of structural deterioration - support efficient asset management
Tier Rationale	This use case: - detects specific environmental events (presence of water or moisture) - operates as an event-based system (leak detected / not detected) - does not inherently monitor behaviour, routines, or activity - focuses on property condition rather than tenant activity - introduces minimal behavioural or privacy risk - requires little or no interpretation of data - operates within a clearly bounded purpose Risk may increase where: - data is combined with other systems to infer presence or absence - monitoring is interpreted beyond leak detection purpose Risk remains limited where the use case remains strictly asset- or safety-focused. This use case remains low impact only where data is not used to infer occupancy or behaviour
Legal Context	Public task (housing management, property maintenance) GDPR: - may not involve personal data where purely environmental - may involve limited personal data where linked to properties - does not involve special category data Human rights considerations: - minimal Article 8 impact due to narrow scope Important legal contexts for consideration - Housing (Scotland) Act 2001 - Building safety and housing condition regulations

Field	Content
Governance Requirements	This use case requires enhanced governance aligned to its moderate impact profile Use must be: - limited to leak detection and maintenance - proportionate to risk being mitigated - clearly defined Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope All deployments should include: - defined ownership (asset or maintenance teams) - basic audit trail of alerts and responses - proportionate tenant transparency - human oversight of any actions DPIA may be required depending on deployment Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - infer occupancy or behaviour from water-related data - repurpose data for tenancy or behavioural assessment - combine with other datasets for profiling Use must remain limited to leak detection and maintenance purposes Any change of purpose requires reassessment of the use case and governance requirements.
Lower-Impact Use	Use of leak detection to: - trigger maintenance alerts - detect water presence Results in simpler governance.
Higher-Impact Use	Leak detection data is: - combined with other datasets - analysed to infer presence or behaviour - used beyond maintenance purposes Results in enhanced governance required.
Key Safeguards	Strict purpose limitation (leak detection only) Proportionate transparency Basic auditability of alerts and actions Controls to prevent reuse or inference Separation from tenancy or behavioural decisions

Field	Content
	Safeguards must be documented, auditable, and enforceable through policies, tenancy agreements, and operational procedures, and regularly reviewed.

A.4.4 Temperature and energy monitoring

Field	Content
Use Case	Temperature / energy monitoring
Family	Environmental & Health
Governance Level	Red
Governance Flag	Environmental monitoring + behavioural inference + potential vulnerability impact
Purpose	Monitor temperature and/or energy usage within properties to: - support safe and healthy living conditions- identify risks such as under-heating or overheating - improve energy efficiency and asset performance - enable targeted support interventions (e.g. fuel poverty support)
Tier Rationale	This use case can: - monitor environmental conditions within the home (Article 8) - capture patterns of heating or energy use over time- behavioural and potential vulnerability inference - suggest behavioural patterns linked to energy usage - identify conditions that may indicate vulnerability (e.g. prolonged low temperatures) - operates at a moderate level of intrusion - creates risk where interpretation extends beyond environmental purpose Risk increases where: - temperature or energy patterns are used to infer behaviour or routines - data is used to assess vulnerability without clear purpose - outputs are used in tenancy or enforcement decisions - data is combined with other monitoring systems Risk increases where data is interpreted or used beyond its environmental or operational purpose.
Legal Context	Public task (housing management, health and safety, energy efficiency) GDPR: - may involve personal data where linked to identifiable households - does not typically involve special category data - may involve inferred vulnerability - DPIA may be required depending on deployment Human rights considerations: - Article 8 (private and family life) engaged due to in-home monitoring Important legal contexts for consideration - Housing (Scotland) Act 2001 - Fuel poverty and housing standards obligations - ECHR Article 8 and A1P1

Field	Content
Governance Requirements	This use case requires enhanced governance aligned to its high-impact profile Governance requirements depend on how the use case is deployed in practice, including context of use Use must be: - clearly defined (environmental monitoring and support) - proportionate to intended purpose - limited to necessary scope Clear definition of purpose (temperature and energy monitoring only) DPIA may be required depending on deployment All deployments must include: - clear tenant transparency - defined ownership and accountability - audit trail of data use and resulting actions - controls on interpretation of patterns - human oversight where actions affect tenants Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - infer behaviour or lifestyle beyond environmental purpose - assume tenant behaviour based on temperature or energy data - use data for tenancy enforcement without reassessment - combine with other datasets to create behavioural profiles without escalation Use must remain limited to environmental and support purposes Any change of purpose requires reassessment of the use case and governance requirements.
Lower-Impact Use	Use of temperature or energy monitoring to: - detect heating issues or inefficiencies - support maintenance and asset management - identify environmental risks Results in simpler governance.
Higher-Impact Use	Temperature or energy data is: - analysed to infer behaviour or occupancy patterns - used to assess vulnerability or lifestyle - combined with other datasets - used in tenancy or enforcement decisions Results in enhanced governance required.

Field	Content
Key Safeguards	Clear tenant transparency regarding monitoring Strict purpose limitation (environmental only) Controls on interpretation and inference Separation from tenancy enforcement decisions Human oversight of actions affecting tenants Proportionate data collection and retention Auditability of data use Safeguards must be documented, auditable, and enforceable through policies, tenancy agreements, and operational procedures, and regularly reviewed.

A.5 Fire and tenant safety use case profiles

A.5.1 Smoke alarms

Field	Content
Use Case	Smoke alarms
Family	Fire & tenant safety
Governance Level	Green
Governance Flag	Life-safety alerting + statutory compliance + event-based detection + potential remote monitoring risk
Purpose	Detect smoke and fire risks to: protect life and property enable timely response to smoke or fire events support landlord fire safety and housing compliance obligations provide assurance that smoke detection systems are installed, maintained, and functioning appropriately
Tier Rationale	This use case is primarily safety-critical and compliance-led. Standard smoke alarm deployment involves event-based detection and does not normally involve behavioural monitoring, occupancy analysis, or decision-making about tenants. Governance risk remains relatively contained where smoke alarms are used only for smoke/fire detection, alerting, testing, maintenance, and compliance assurance. Risk increases where: - alarms are remotely monitored and linked to identifiable tenants, households, or properties - event data is retained and analysed beyond safety and compliance purposes - alarm data is combined with other systems, such as occupancy monitoring, access control, CCTV, or tenancy records - outputs are used to infer behaviour, property use, tenant responsibility, or non-compliance - system faults, disabling, or non-response create safety, accountability, or compliance risks
Legal Context	Important legal contexts for consideration may include: - fire safety legislation and associated housing safety obligations - statutory requirements relating to smoke detection, maintenance, testing, and inspection - landlord repairing, housing condition, and safety obligations - data protection obligations where remotely monitored alarms generate data linked to identifiable properties, households, residents, or events - human rights and privacy considerations where alarm data is repurposed or linked with wider monitoring systems - Fire safety legislation and housing regulations

Field	Content
	Housing (Scotland) Act 2001 GDPR: - minimal personal data in standard deployments - accountability and system management remain applicable
Governance Requirements	This use case requires governance aligned to its safety and compliance role. Use should be: - clearly defined as smoke/fire detection, alerting, testing, maintenance, and compliance assurance - proportionate to the safety risk being managed - limited to event-based smoke/fire detection unless further assessment is undertaken Governance arrangements should address: - defined ownership and accountability for installation, testing, maintenance, fault management, and response - auditability of alarm status, testing, maintenance, alerts, faults, and remedial actions - clear escalation arrangements where alarms fail, are disabled, or require replacement - reliability and resilience of alarm operation - proportionate resident or tenant transparency regarding the purpose and operation of connected smoke alarms - access controls for alarm data and system management - review of additional governance requirements where alarm systems are remotely monitored, integrated, or linked to other datasets Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT-enabled smoke alarms should not be used to: - extend beyond smoke/fire safety, maintenance, testing, alerting, or compliance purposes without reassessment - infer behaviour, occupancy, property use, tenant responsibility, or lifestyle - use alarm data for tenancy, enforcement, behavioural, or non-fire-safety decisions without further governance review - bypass established statutory safety, inspection, maintenance, testing, or response obligations - rely on connected functionality in a way that reduces resilience, safety, or access to emergency response Any change of purpose, remote monitoring expansion, integration with other systems, or use of alarm data for non-safety purposes should trigger reassessment through the handbook.
Lower-Impact Use	Smoke alarm data is used only for: - detection of smoke/fire events

Field	Content
	- triggering alarms - supporting safety response - testing, maintenance, fault monitoring, and compliance assurance This results in simpler governance, provided use remains limited to smoke/fire safety and compliance purposes.
Higher-Impact Use	Smoke alarm data is: - remotely monitored and linked to identifiable households or individuals - combined with other systems or datasets - analysed to infer behaviour, occupancy, property use, or tenant responsibility - used in tenancy, enforcement, investigation, or non-fire-safety decision-making This results in enhanced governance requirements.
Key Safeguards	Clear purpose limitation: smoke/fire safety and compliance only Defined accountability for installation, testing, maintenance, monitoring, and response Reliable, resilient, and fail-safe alarm operation Documented testing, inspection, maintenance, fault handling, and replacement arrangements Controlled access to alarm data and system controls Proportionate transparency for tenants, residents, staff, and building users Separation between smoke/fire safety monitoring and tenancy/enforcement decision-making Reassessment before integration, expanded monitoring, or repurposing of alarm data Safeguards must be documented, auditable, and enforceable, and subject to regular review

A.5.2 Fire alarm systems

Field	Content
Use Case	Fire alarms
Family	Fire & tenant safety
Governance Level	Green
Governance Flag	Life-safety monitoring + statutory compliance + event-based alerting + potential integration risk
Purpose	Detect and respond to fire risks across buildings to: - protect life and property - enable coordinated emergency response - support statutory fire safety and housing compliance obligations - support safe evacuation and system-level safety assurance
Tier Rationale	This use case is primarily safety-critical and compliance-led. It normally involves event-based detection rather than behavioural monitoring or continuous monitoring of individuals. Governance risk is generally lower where the deployment is limited to fire detection, alerting, maintenance, and emergency response. However, governance requirements increase where fire alarm data is remotely monitored, integrated with other systems, linked to identifiable households or individuals, or used for purposes beyond fire safety. Risk increases where: - alarm data is linked to identifiable tenants, households, or occupancy records - alarm events are analysed beyond immediate safety and compliance purposes - outputs are combined with access control, CCTV, occupancy, or tenancy records - outputs are used to infer behaviour, property use, or tenant responsibility - system failures could affect tenant safety or access to emergency response
Legal Context	Important legal contexts for consideration may include: - fire safety legislation and associated building safety requirements - housing condition, landlord compliance, and statutory safety obligations - health and safety obligations relating to building users, staff, contractors, and residents - data protection obligations where alarm data is linked to identifiable people, households, properties, or events - human rights and privacy considerations where monitoring is extended beyond event-based fire safety use - Fire safety legislation and building safety regulations - Housing (Scotland) Act 2001 Statutory compliance obligations for fire detection systems GDPR: - minimal personal data in standard deployments

Field	Content
	- accountability and system management remain applicable
Governance Requirements	This use case requires governance aligned to its life-safety and compliance profile. Use should be: - clearly defined as fire detection, alerting, emergency response, testing, maintenance, and compliance assurance - proportionate to the fire safety risks being managed - limited to event-based fire safety purposes unless further assessment is undertaken Governance arrangements should address: - defined ownership and accountability for system operation, maintenance, testing, inspection, monitoring, and response - clear escalation and response arrangements for fire events - auditability of testing, maintenance, alerts, faults, and responses - resilience, reliability, and fail-safe arrangements - proportionate resident, tenant, staff, or building-user transparency - access controls for alarm data, system controls, and event records - human review where outputs inform actions affecting tenants, residents, staff, or building users - review of additional governance requirements where systems are remotely monitored, integrated, or linked with other datasets Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT-enabled fire alarm systems should not be used to: - extend monitoring beyond fire safety, emergency response, testing, maintenance, or compliance purposes without reassessment - infer behaviour, occupancy, tenant responsibility, or property use without a clearly justified and reassessed purpose - use alarm data for tenancy, enforcement, behavioural, or non-fire-safety decisions without further governance review - bypass statutory fire safety, maintenance, inspection, testing, or emergency response obligations - rely solely on automated outputs where human review or emergency response judgement is required Any change of purpose, system integration, remote monitoring expansion, or linkage with other datasets should trigger reassessment through the handbook.
Lower-Impact Use	Fire alarm data is used only for: - detection of fire events - triggering alarms - supporting evacuation and emergency response

Field	Content
	- maintenance, testing, fault monitoring, and compliance assurance This results in simpler governance, provided use remains limited to fire safety and compliance purposes.
Higher-Impact Use	Fire alarm data is: - remotely monitored in a way that links events to identifiable households or individuals - integrated with access control, CCTV, occupancy, or tenancy systems - analysed to infer behaviour, occupancy, property use, or tenant responsibility - used in tenancy, enforcement, investigation, or non-fire-safety decision-making
Key Safeguards	Clear purpose limitation: fire safety and compliance only Defined accountability for system operation, testing, maintenance, alert response, and compliance assurance Reliable, resilient, and fail-safe system design Documented testing, inspection, maintenance, and fault management Defined escalation and emergency response arrangements Controlled access to alarm data and system controls Proportionate transparency for tenants, residents, staff, and building users Separation between fire safety monitoring and tenancy/enforcement decision-making Reassessment before system integration, expanded monitoring, or repurposing of alarm data Safeguards must be documented, auditable, and enforceable, and subject to regular review

A.6 Telecare and health support use case profiles

A.6.1 Fall detection

Field	Content
Use Case	Fall detection
Family	Telecare & Health Support
Governance Level	Red
Governance Flag	Health monitoring + vulnerability detection + real-time intervention
Purpose	Use sensors or wearable devices to: - detect falls or sudden changes in movement - identify potential injury or risk events - trigger alerts to staff, carers, or emergency services - support timely intervention and tenant safety
Tier Rationale	This use case can: - involve monitoring within the home (Article 8) - detect events linked to health and physical wellbeing - generate real-time alerts requiring intervention - indicate vulnerability, mobility issues, or health status - directly relates to individual health and safety - may operate continuously or in real time - triggers intervention or response actions affecting the tenant Risk increases where: - fall data is used to assess ongoing vulnerability or independence - monitoring is continuous and linked to broader behavioural data - outputs are used in care, housing, or tenancy decisions - systems operate without appropriate human oversight These risks remain even in simple or initial deployments
Legal Context	Public task (safeguarding, care and support services) GDPR: - involves personal data - involves special category data (health) - requires Article 9 processing condition - DPIA likely required Human rights considerations: - Article 8 (private and family life) engaged due to in-home monitoring - heightened duty of care due to vulnerability

Field	Content
	Important legal contexts for consideration - Adult Support and Protection (Scotland) Act 2007 - Health and social care legislation - Housing (Scotland) Act 2001 GDPR: - special category data - Article 9 health and social care conditions - ECHR Article 8
Governance Requirements	This use case requires enhanced governance aligned to its high-impact profile Governance requirements depend on how the use case is deployed in practice, including context of use Use must be: - clearly justified (safety and wellbeing) - proportionate to the level of monitoring - aligned with tenant support needs Clear definition of purpose (fall detection and response only) DPIA may be required depending on deployment All deployments must include: - clear tenant communication and, where appropriate, agreement - defined ownership (care or support teams) - audit trail of alerts and responses - clear escalation and response processes - strong human oversight of any decisions Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - infer broader health conditions without justification - monitor behaviour beyond fall detection purpose - use data to assess tenancy suitability or independence without review - replace professional judgement in care decisions Use must remain limited to defined safety and support purposes Any change of purpose requires reassessment of the use case and governance requirements. This use case may involve processing that requires valid consent. In a social housing context, reliance on consent should be treated as exceptional because of the potential power imbalance between landlord and tenant. Where consent may be relevant, this should trigger enhanced governance, including legal or data protection review, DPIA

Field	Content
	consideration, and meaningful tenant communication or consultation, rather than being treated as a presumption of permissibility.
Lower-Impact Use	Use of fall detection for: - event-based alerts only - immediate response to incidents - defined safety monitoring Results in simpler governance.
Higher-Impact Use	Fall detection data is: - used to assess ongoing vulnerability or independence - combined with other datasets (e.g. telecare, occupancy) - analysed for behavioural or health patterns - used in care or tenancy decisions Results in enhanced governance required.
Key Safeguards	Clear tenant transparency and communication Explicit recognition of vulnerability and safeguarding responsibilities Strict purpose limitation (fall detection only) Strong human oversight of alerts and decisions Defined response and escalation protocols Controls on use of health-related data Proportionate data retention Safeguards must be documented, auditable, and enforceable through policies, care agreements, and operational procedures, and regularly reviewed.

A.6.2 Telecare systems

Field	Content
Use Case	Telecare support
Family	Telecare & Health Support
Governance Level	Red
Governance Flag	Continuous monitoring + health and wellbeing data + vulnerability and dependency risk
Purpose	Use connected telecare devices (e.g. sensors, alarms, wearables) to: - support tenant health, safety, and wellbeing - monitor for risk events (e.g. inactivity, distress) - enable timely intervention and support - facilitate independent living for vulnerable individuals
Tier Rationale	This use case can: - involve continuous or near-continuous monitoring within the home (Article 8) - capture patterns of activity, inactivity, and daily routines - indicate health status, vulnerability, or changes in condition - trigger alerts leading to intervention by staff, carers, or third parties - creates ongoing monitoring of daily life within the home - generates sensitive information about wellbeing and independence - introduces dependency on monitoring systems and response services Risk increases where: - monitoring data is analysed to infer behaviour or lifestyle - data is combined with other datasets (e.g. tenancy, health records) - outputs are used in care, housing, or eligibility decisions - systems operate without sufficient human oversight These risks remain even in simple or initial deployments
Legal Context	Public task (care provision, safeguarding responsibilities) GDPR: - involves personal data - involves special category data (health and wellbeing) - requires Article 9 processing condition - DPIA required Human rights considerations: - Article 8 (private and family life) strongly engaged due to continuous monitoring - heightened obligations due to vulnerability Important legal contexts for consideration - Adult Support and Protection (Scotland) Act 2007

Field	Content
	- Health and social care legislation - Housing (Scotland) Act 2001 GDPR: - special category data - Article 9 health and social care conditions - ECHR Article 8
Governance Requirements	This use case requires enhanced governance aligned to its high-impact profile Governance requirements depend on how the use case is deployed in practice, including context of use Use must be: - clearly justified in relation to care and support needs - proportionate to the level and intensity of monitoring - aligned with tenant wellbeing, dignity, and autonomy Clear definition of purpose (care and wellbeing support only) DPIA may be required depending on deployment All deployments must include: - clear tenant communication and, where appropriate, informed agreement - defined ownership (care providers or housing support teams) - audit trail of monitoring, alerts, and interventions - clear protocols for response and escalation - strong human oversight of all decisions affecting tenants Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - monitor behaviour beyond what is necessary for care and wellbeing - infer lifestyle or habits without explicit justification - be used for tenancy enforcement or behavioural assessment - replace professional judgement in care or safeguarding decisions - operate as general surveillance of vulnerable individuals Use must remain limited to defined care and support purposes Any change of purpose requires reassessment of the use case and governance requirements. This use case may involve processing that requires valid consent. In a social housing context, reliance on consent should be treated as exceptional because of the potential power imbalance between landlord and tenant. Where consent may be relevant, this should trigger enhanced governance, including legal or data protection review, DPIA

Field	Content
	consideration, and meaningful tenant communication or consultation, rather than being treated as a presumption of permissibility.
Lower-Impact Use	Use of telecare devices for: - specific risk-based monitoring (e.g. alerts) - event-based triggers rather than continuous analysis - clearly defined care pathways Results in simpler governance.
Higher-Impact Use	Telecare data is: - continuously analysed to infer behaviour or lifestyle - combined with other datasets - used to assess fitness for independent living - used to inform tenancy or eligibility decisions - relied upon without sufficient human oversight Results in enhanced governance required.
Key Safeguards	Clear and accessible tenant transparency Explicit recognition of vulnerability and safeguarding responsibilities Strict purpose limitation (care and wellbeing only) Strong human oversight of decisions and interventions Controls to prevent misuse of sensitive health data Defined response protocols and accountability Proportionate data retention Safeguards must be documented, auditable, and enforceable through policies, care agreements, and operational procedures, and regularly reviewed.

A.6.3 Voice assistants (care context)

Field	Content
Use Case	Voice related care
Family	Telecare & Health Support
Governance Level	Red
Governance Flag	In-home interaction + continuous listening + behavioural and contextual inference
Purpose	Use voice-enabled devices to: - support tenant independence and daily living - enable interaction with services (e.g. reminders, alerts, assistance requests) - provide access to information and communication tools - support care or wellbeing through voice interaction
Tier Rationale	This use case can: - involve ongoing presence of listening-enabled devices within the home (Article 8) - capture spoken interaction and contextual audio signals - infer behaviour, routines, and personal circumstances - indicate vulnerability or wellbeing through interaction patterns - generate insights from frequency, tone, or engagement patterns - introduces risk of unintended data capture (e.g. background conversations) - may create a perception of surveillance within private space - may involve third-party processing of voice data Risk increases where: - interactions are analysed to generate behavioural or health insights - data is stored or combined with other datasets - outputs are used in care, tenancy, or service decisions - systems operate without clear user awareness or control These risks remain even in simple or initial deployments
Legal Context	Public task may apply (care provision, supported housing) GDPR: - involves personal data - may involve special category data through inferred health or vulnerability - likely to require DPIA - may involve third-party data processors Human rights considerations: - Article 8 (private and family life) strongly engaged due to presence in the home Important legal contexts for consideration - Health and social care legislation

Field	Content
	- Housing (Scotland) Act 2001 - ECHR Article 8 GDPR: - personal and potentially special category data - consent may arise but is high-risk in housing contexts
Governance Requirements	This use case requires enhanced governance aligned to its high-impact profile Governance requirements depend on how the use case is deployed in practice, including context of use Use must be: - clearly defined (assistive support, not surveillance) - proportionate to intended purpose - transparent and understandable to tenants Clear definition of purpose (interaction and assistance only) DPIA may be required depending on deployment All deployments must include: - clear tenant communication - explicit explanation of when devices are listening or processing data - defined ownership and accountability (including third parties) - strong controls on data storage and sharing - human oversight of any decisions affecting tenants Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - monitor or record private conversations beyond defined functionality - infer behaviour or personal characteristics without justification - use interaction data for tenancy enforcement - operate without user awareness or control - rely on automated interpretation without human review Use must remain limited to assistive and service purposes Any change of purpose requires reassessment of the use case and governance requirements. This use case may involve processing that requires valid consent. In a social housing context, reliance on consent should be treated as exceptional because of the potential power imbalance between landlord and tenant. Where consent may be relevant, this should trigger enhanced governance, including legal or data protection review, DPIA consideration, and meaningful tenant communication or consultation, rather than being treated as a presumption of permissibility.

Field	Content
Lower-Impact Use	Use of voice assistants to: - provide reminders or alerts - support user-initiated commands - avoid storage or analysis of interaction history Results in simpler governance.
Higher-Impact Use	Voice data is: - analysed to infer behaviour or wellbeing - stored to build profiles of usage patterns - combined with other datasets - used in tenancy, care, or eligibility decisions - processed extensively by third parties Results in enhanced governance required.
Key Safeguards	Clear tenant transparency regarding how devices operate Explicit user control (e.g. mute, disable) Strict purpose limitation (assistive use only) Strong controls on data storage and third-party processing Separation between assistive functionality and decision-making Controls to prevent unintended capture or profiling Human oversight of any decisions Safeguards must be documented, auditable, and enforceable through policies, care agreements, and operational procedures, and regularly reviewed.

A.7 Behaviour and occupancy monitoring use case profiles

A.7.1 Occupancy and presence detection

Field	Content
Use Case	Occupancy / motion
Family	Behaviour & Occupancy
Governance Level	Red
Governance Flag	Presence detection + behavioural inference + in-home monitoring
Purpose	Use occupancy or motion sensors to: - detect presence or absence within a property - support safety, energy efficiency, or asset management - identify patterns of activity - trigger alerts or operational responses
Tier Rationale	This use case can: - presence detection + continuous behavioural inference (Article 8) - generate patterns of occupancy over time - indicate daily routines and activity levels - provide insight into how a property is used - introduces behavioural inference through repeated monitoring - does not directly capture identity or detailed activity Risk increases where: - occupancy patterns are analysed to identify routines or behaviour - data is linked to individuals or combined with other datasets - outputs are used in tenancy or enforcement decisions - monitoring becomes continuous or highly granular These risks remain even in simple or initial deployments
Legal Context	Public task (housing management, safety, energy efficiency) GDPR: - involves personal data where linked to identifiable individuals - may enable behavioural profiling through inference - DPIA may be required depending on deployment Human rights considerations: - Article 8 (private and family life) engaged due to in-home monitoring Important legal contexts for consideration - Housing (Scotland) Act 2001 - ECHR Article 8 and A1P1

Field	Content
Governance Requirements	This use case requires enhanced governance aligned to its high-impact profile Use must be: - clearly defined (safety, efficiency, or operational purpose) - proportionate to the level of monitoring - limited to necessary scope Clear definition of purpose (presence detection only) DPIA may be required depending on deployment All deployments must include: - clear tenant transparency - defined ownership and accountability - audit trail of data use and interpretation - controls on how patterns are analysed - human oversight of decisions affecting tenants Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - infer behaviour beyond defined purpose - monitor tenants covertly or continuously without justification - use occupancy data for tenancy enforcement without reassessment - combine with other datasets to create behavioural profiles without escalation Use must remain limited to defined operational purposes Any change of purpose requires reassessment of the use case and governance requirements. Where presence / behaviour / habitation is inferred, this use case may involve processing that requires valid consent. In a social housing context, reliance on consent should be treated as exceptional because of the potential power imbalance between landlord and tenant. Where consent may be relevant, this should trigger enhanced governance, including legal or data protection review, DPIA consideration, and meaningful tenant communication or consultation, rather than being treated as a presumption of permissibility.
Lower-Impact Use	Use of occupancy sensors to: - detect presence for operational purposes (e.g. heating, lighting) - trigger simple alerts or automation Results in simpler governance.
Higher-Impact Use	Occupancy data is: - analysed to infer routines or behaviour - combined with other datasets

Field	Content
	- used to monitor individuals over time - used in tenancy or enforcement decisions Results in enhanced governance required.
Key Safeguards	Clear tenant transparency regarding monitoring Strict purpose limitation (presence detection only) Controls on analysis of patterns and inference Separation between monitoring and tenancy decision-making Strong human oversight of decisions Proportionate data collection and retention Auditability of data use and interpretation Safeguards must be documented, auditable, and enforceable through policies, tenancy agreements, and operational procedures, and regularly reviewed.

A.7.2 Noise monitoring

Field	Content
Use Case	Noise monitoring
Family	Behaviour & Occupancy
Governance Level	Red
Governance Flag	Behavioural detection + enforcement risk + in-home monitoring
Purpose	Use noise monitoring devices to: - detect elevated noise levels within properties - support management of anti-social behaviour (ASB) - identify disturbances affecting other residents - trigger alerts or interventions where thresholds are exceeded
Tier Rationale	This use case can: - monitor activity within the home based on sound levels (Article 8) - detect patterns of noise associated with behaviour or occupancy - indicate potential anti-social behaviour - be used as supporting evidence - does not record identifiable audio content (in typical deployments) - operates at a moderate level of intrusion - introduces behavioural monitoring through indirect signals Risk increases where: - noise patterns are analysed to infer behaviour or activity - data is linked to individuals or combined with other datasets - outputs are used as evidence in tenancy or enforcement decisions - monitoring becomes continuous or highly sensitive These risks remain even in simple or initial deployments
Legal Context	Public task (housing management, ASB prevention) GDPR: - involves personal data where linked to identifiable properties or individuals - may involve inference of behaviour - DPIA required Human rights considerations: - Article 8 (private and family life) engaged due to in-home monitoring - tenancy and enforcement implications Important legal contexts for consideration - Housing (Scotland) Act 2001 - Anti-social behaviour legislation

Field	Content
	- ECHR Article 8 and A1P1
Governance Requirements	This use case requires enhanced governance aligned to its high-impact profile Governance requirements depend on how the use case is deployed in practice, including context of use Use must be: - clearly justified (ASB or disturbance management) - proportionate to the issue being addressed - limited to defined thresholds and conditions Clear definition of purpose (noise level detection only) DPIA may be required depending on deployment All deployments must include: - clear tenant transparency regarding monitoring - documented lawful basis - defined ownership and accountability - audit trail of alerts and actions - controls on interpretation of data - human oversight of decisions affecting tenants Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - record or analyse actual audio content without explicit justification - infer behaviour beyond noise thresholds - operate covertly or without transparency - use noise data as sole evidence for enforcement decisions - combine with other datasets to create behavioural profiles without escalation Use must remain limited to noise-level monitoring for defined purposes Any change of purpose requires reassessment of the use case and governance requirements. Where behaviour or lifestyle is implicated, this use case may involve processing that requires valid consent. In a social housing context, reliance on consent should be treated as exceptional because of the potential power imbalance between landlord and tenant. Where consent may be relevant, this should trigger enhanced governance, including legal or data protection review, DPIA consideration, and meaningful tenant communication or consultation, rather than being treated as a presumption of permissibility.
Lower-Impact Use	Use of noise monitoring to: - detect threshold breaches only - support early intervention for disturbances - avoid recording or storing detailed data

Field	Content
	Results in simpler governance.
Higher-Impact Use	Noise data is: - analysed to infer behaviour or activity - used as evidence in disputes or enforcement - combined with other datasets - used to monitor tenants over time Results in enhanced governance required.
Key Safeguards	Clear tenant transparency regarding monitoring Strict purpose limitation (noise thresholds only) Controls to prevent audio capture or content analysis Separation between monitoring and tenancy enforcement Strong human oversight of decisions Proportionate thresholds and deployment Auditability of alerts and actions Safeguards must be documented, auditable, and enforceable through policies, tenancy agreements, and operational procedures, and regularly reviewed.

A.7.3 Appliance-level monitoring

Field	Content
Use Case	Appliance monitoring
Family	Behaviour & Occupancy
Governance Level	Red
Governance Flag	In-home behavioural monitoring + routine/lifestyle inference + potential vulnerability signals
Purpose	Monitor usage of household appliances (e.g. kettles, cookers, fridges) to: - understand patterns of activity within the home - support safety, maintenance, or energy efficiency - identify changes or anomalies in behaviour - support wellbeing monitoring where appropriate
Tier Rationale	This use case can: - involve continuous or repeated monitoring within the home (Article 8) - capture detailed patterns of appliance usage over time - infer daily routines, habits, and lifestyle patterns - indicate presence, absence, and activity levels within the home - generate behavioural insights without direct observation - enables reconstruction of how a home is lived in - may indicate vulnerability or changes in wellbeing - introduces high behavioural inference potential Risk increases where: - appliance data is analysed to identify behavioural patterns - data is interpreted to detect vulnerability or need for intervention - outputs are used in tenancy, care, or service decisions - multiple data streams are combined to build profiles These risks remain even in simple or initial deployments
Legal Context	Public task may apply (housing management, safety, wellbeing monitoring) GDPR: - involves personal data when linked to identifiable households - capable of behavioural profiling through inference - may involve special category data where vulnerability is inferred - DPIA likely required Human rights considerations: - Article 8 (private and family life) engaged due to in-home monitoring Important legal contexts for consideration

Field	Content
	- Housing (Scotland) Act 2001 - ECHR Article 8
Governance Requirements	This use case requires enhanced governance aligned to its high-impact profile Governance requirements depend on how the use case is deployed in practice, including context of use Use must be: - clearly defined and justified - proportionate to the level of monitoring - limited to necessary scope Clear definition of purpose (specific monitoring objective only) DPIA may be required depending on deployment All deployments must include: - clear tenant transparency about what is monitored - explicit acknowledgement of behavioural inference potential - defined ownership and accountability - audit trail of data use and interpretation - controls on how inference is generated - human oversight of decisions affecting tenants Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - monitor behaviour beyond defined purpose - infer lifestyle or personal characteristics without justification - be used for tenancy enforcement or behavioural judgement - combine data sources to create behavioural profiles without escalation - present the use as low-risk where significant inference exists Use must remain limited to clearly defined, proportionate purposes Any change of purpose requires reassessment of the use case and governance requirements. Only apply this guardrail where the use is clearly beyond routine housing / building management. This use case may involve processing that requires valid consent. In a social housing context, reliance on consent should be treated as exceptional because of the potential power imbalance between landlord and tenant. Where consent may be relevant, this should trigger enhanced governance, including legal or data protection review, DPIA consideration, and meaningful tenant communication or consultation, rather than being treated as a presumption of permissibility.
Lower-Impact Use	Monitoring individual appliances to: - detect faults or maintenance issues

Field	Content
	- record simple usage events - support energy efficiency without behavioural analysis Results in simpler governance.
Higher-Impact Use	Appliance data is: - analysed to infer routines or lifestyle - used to detect vulnerability or behaviour change - combined across multiple devices - linked with other datasets - used in care or tenancy decisions Results in enhanced governance required.
Key Safeguards	Clear and accessible tenant transparency Explicit acknowledgement of behavioural inference risks Strict purpose limitation Controls to prevent profiling or over-interpretation Separation between monitoring and tenancy/enforcement decisions Strong human oversight Proportionate data collection and retention Strong auditability of data use Safeguards must be documented, auditable, and enforceable through policies, tenancy agreements, and operational procedures, and regularly reviewed.

A.7.4 Thermal imaging

Field	Content
Use Case	Thermal imaging
Family	Behaviour & Occupancy
Governance Level	Red
Governance Flag	In-home monitoring + behavioural inference without direct observation
Purpose	Use thermal imaging sensors to: - detect heat patterns - identify occupancy and movement within a property - support safety, security, or building management functions
Tier Rationale	This use case can: - involve monitoring within the home (Article 8) - detect presence, movement, and activity indirectly through heat patterns - infer occupancy, routines, and behaviour without direct visual capture - create insight into how a home is used over time - enables behavioural inference from non-visual data - may operate continuously or repeatedly within private residential space - introduces significant privacy risks despite lower perceived intrusiveness than cameras Risk increases where: - thermal data is analysed to identify patterns of behaviour or lifestyle - outputs are used to assess occupancy or compliance - data is combined with other monitoring systems - insights inform tenancy or enforcement decisions These risks remain even in simple or initial deployments
Legal Context	Public task (housing management, safety, or operational monitoring) GDPR: - involves personal data where linked to identifiable individuals - capable of behavioural inference - does not typically involve special category data unless additional interpretation is applied Human rights considerations: - Article 8 (right to private and family life) is strongly engaged due to in-home monitoring Important legal contexts for consideration - Housing (Scotland) Act 2001 - ECHR Article 8 and A1P1 GDPR:

Field	Content
	- inferred personal and behavioural data - potential for intrusive monitoring
Governance Requirements	This use case requires enhanced governance aligned to its high-impact profile Governance requirements depend on how the use case is deployed in practice, including context of use Use must be: - clearly defined (e.g. safety, asset protection) - proportionate to the level of monitoring - limited to the minimum necessary scope Clear definition of purpose (specific operational objective, not general behavioural monitoring) DPIA may be required depending on deployment All deployments must include: - clear tenant transparency - defined ownership and accountability - audit trail of monitoring and use - controls on interpretation of thermal data - human oversight of any decisions affecting tenants Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - infer or analyse behaviour beyond the defined purpose - monitor tenants covertly or without clear transparency - use thermal data for tenancy enforcement or behavioural assessment - combine with other datasets to create behavioural profiles without governance escalation Use must remain limited to defined operational or safety purposes Any change of purpose requires reassessment of the use case and governance requirements. Where this use case relates to occupants, presence, or body-based inference rather than building fabric only, this use case may involve processing that requires valid consent. In a social housing context, reliance on consent should be treated as exceptional because of the potential power imbalance between landlord and tenant. Where consent may be relevant, this should trigger enhanced governance, including legal or data protection review, DPIA consideration, and meaningful tenant communication or consultation, rather than being treated as a presumption of permissibility.
Lower-Impact Use	Use of thermal imaging to: - detect general occupancy patterns at a low level

Field	Content
	- support asset or safety monitoring No behavioural analysis or profiling Results in simpler governance.
Higher-Impact Use	Thermal data is: - analysed to infer routines or behaviour - combined with other datasets (e.g. occupancy, access, appliance) - used to monitor individuals over time - used in tenancy or enforcement contexts Results in enhanced governance required.
Key Safeguards	Clear and accessible tenant transparency Strict purpose limitation (no behavioural monitoring beyond defined use) Controls on data interpretation and inference Separation between monitoring and tenancy decision-making Strong human oversight of any decisions or interventions Proportionate data collection and retention Strong auditability of data use Safeguards must be documented, auditable, and enforceable through policies, tenancy agreements, and operational procedures, and regularly reviewed.

A.8 Security and access control use case profiles

A.8.1 Internal CCTV

Field	Content
Use Case	Internal CCTV
Family	Security & Surveillance
Governance Level	Red
Governance Flag	Direct in-home surveillance + high intrusion + behavioural monitoring
Purpose	Use internal CCTV systems to: - monitor activity within a property - support safety or safeguarding - detect incidents or risks within indoor environments
Tier Rationale	This use case can: - involve direct visual monitoring within the home (Article 8) - capture identifiable individuals and their behaviour - record continuous or intermittent footage of private living space - generate detailed insight into behaviour, routines, and personal activity

Field	Content
	- represents one of the most intrusive forms of monitoring in residential settings - creates high risk of surveillance and loss of privacy - may impact dignity, autonomy, and tenant rights Risk increases where: - monitoring is continuous or extensive - footage is analysed for behavioural or compliance purposes - data is retained or shared beyond immediate safety use - outputs are used in tenancy or enforcement decisions These risks remain even in simple or initial deployments
Legal Context	Public task may apply in limited safeguarding contexts GDPR: - involves personal data and likely special category data - may involve highly sensitive contextual information - triggers a strong likelihood of DPIA requirement Human rights considerations: - Article 8 (right to private and family life) is strongly engaged - particularly high threshold for justification Important legal contexts for consideration - Housing (Scotland) Act 2001 - ECHR Article 8 and A1P1 Equality and safeguarding law GDPR: - personal data - potential criminal data - Data Protection Act requirements
Governance Requirements	This use case requires enhanced governance aligned to its high-impact profile Governance requirements depend on how the use case is deployed in practice, including context of use Use must be: - clearly justified (e.g. safeguarding, extreme risk scenarios) - proportionate and necessary - limited in scope and duration Clear definition of purpose (specific safeguarding or safety objective) DPIA will typically be required due to the high-impact nature of the use case All deployments must include:

Field	Content
	- explicit and clear tenant communication - strong legal justification - defined ownership and accountability - strict access controls and audit logging - defined retention and deletion policies - strong human oversight of all decisions Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - conduct general surveillance of tenants within their home - monitor behaviour for tenancy enforcement - operate without clear justification and transparency - replace human judgement in decision-making - retain or reuse footage beyond defined purpose Use must remain limited to clearly justified safeguarding or safety purposes Any change of purpose requires reassessment of the use case and governance requirements. This use case may involve processing that requires valid consent. In a social housing context, reliance on consent should be treated as exceptional because of the potential power imbalance between landlord and tenant. Where consent may be relevant, this should trigger enhanced governance, including legal or data protection review, DPIA consideration, and meaningful tenant communication or consultation, rather than being treated as a presumption of permissibility.
Lower-Impact Use	Use of internal CCTV for: - specific safeguarding situations - time-limited monitoring - clearly defined and agreed circumstances Results in simpler governance.
Higher-Impact Use	Internal CCTV is: - used continuously or broadly within the home - used to monitor behaviour or compliance - combined with other datasets - used in tenancy or enforcement decisions Results in enhanced governance required.
Key Safeguards	Explicit and clear tenant transparency and agreement Strict purpose limitation (safeguarding only) Strong access controls and auditability of footage

Field	Content
	Clear retention and deletion policies Separation between monitoring and tenancy decision-making Strong human oversight Controls to prevent misuse or overreach Safeguards must be documented, auditable, and enforceable through policies, tenancy agreements, and operational procedures, and regularly reviewed.

A.8.2 External CCTV

Field	Content
Use Case	External CCTV
Family	Security & Surveillance
Governance Level	Red
Governance Flag	Surveillance in shared spaces + identification risk + potential enforcement use
Purpose	Use CCTV systems to: - monitor external and communal areas - support safety and security - deter and detect crime or anti-social behaviour - provide evidence for incident investigation where required
Tier Rationale	This use case: - can capture identifiable individuals in external or communal residential areas -can monitor movement and activity around buildings - can create records of behaviour over time - can support investigation of incidents and security concerns - can operate outside the private interior of the home - can introduce identification and surveillance risk in shared environments - may influence decisions relating to safety or tenancy - may involve criminal offence data depending on use (e.g. incident investigation) Risk increases where: - individuals are tracked or monitored over time - footage is analysed to identify behavioural patterns - data is combined with other systems (e.g. access control, tenancy records) - outputs are used in tenancy or enforcement decisions These risks remain even in simple or initial deployments
Legal Context	Public task (community safety, housing management) GDPR: - involves personal data where individuals are identifiable - may involve criminal offence data depending on use (e.g. incident investigation) - surveillance and security regulations - DPIA likely required Human rights considerations: - Article 8 (private and family life) may be engaged in residential contexts Important legal contexts for consideration - Housing (Scotland) Act 2001

Field	Content
	- Anti-social behaviour legislation - ECHR Article 8
Governance Requirements	This use case requires enhanced governance aligned to its high-impact profile Governance requirements depend on how the use case is deployed in practice, including context of use Use must be: - clearly justified for safety or security purposes - proportionate to the risks being addressed - limited to appropriate locations Clear definition of purpose (security and safety monitoring only) DPIA may be required depending on deployment All deployments must include: - clear and visible signage and tenant communication - documented lawful basis - defined ownership and accountability - audit trail for access and use of footage - strict access controls - human oversight of decisions affecting tenants Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - conduct general behavioural surveillance of tenants - monitor areas where there is a reasonable expectation of privacy - use footage as the sole basis for tenancy enforcement decisions - repurpose surveillance data for unrelated purposes Monitoring must remain limited to defined external or communal areas Any change of purpose requires reassessment of the use case and governance requirements.
Lower-Impact Use	Use of CCTV to: - monitor entrances, exits, and shared areas - support incident detection and investigation - operate with restricted access and retention Results in simpler governance.
Higher-Impact Use	CCTV data is: - actively monitored or analysed to identify behaviour - combined with other datasets

Field	Content
	- used to track individuals over time - used in tenancy or enforcement decisions Results in enhanced governance required.
Key Safeguards	Clear and visible transparency (e.g. signage and tenant communication) Strict purpose limitation (security only) Strong access controls and audit logging Defined retention and deletion controls Separation between surveillance and tenancy decision-making Controls to prevent tracking or profiling of individuals Proportionate deployment (camera positioning and coverage) Safeguards must be documented, auditable, and enforceable through policies, tenancy agreements, and operational procedures, and regularly reviewed.

A.8.3 Smart locks and door entry

Field	Content
Use Case	Smart locks / door entry
Family	Security & Access Control
Governance Level	Red
Governance Flag	Access control + behavioural data (entry/exit) + high tenant impact
Purpose	Control and manage access to properties using connected systems (e.g. smart locks, keyless entry, or door entry systems) to: - improve security and safety - manage access for tenants, staff, and authorised third parties - provide auditability of access events - support operational processes (e.g. maintenance access, void management)
Tier Rationale	This use case can: - control or restrict access to a tenant's home - record entry and exit events over time - indicate occupancy, presence, and routines - generate logs that may be linked to individuals - affect how and when a tenant can access their home It may: - introduce behavioural inference (e.g. access patterns) - create dependency on system availability for access - impact tenancy rights and quiet enjoyment Risk remains even where systems are used for operational access control, due to the inherent ability to control and record access to the home Risk increases where: - access logs are analysed to infer behaviour or routines - access is remotely controlled without adequate safeguards - data is combined with other datasets (e.g. occupancy, CCTV) - access events are used in tenancy or enforcement decisions - system failure impacts tenant access or safety
Legal Context	Public task (housing management, property access, safety) GDPR: - involves personal data (access logs linked to individuals) - may involve behavioural inference DPIA likely required depending on deployment Human rights:

Field	Content
	- Article 8 (private life and home) engaged - A1P1 (peaceful enjoyment of property) relevant where access control is affected
Governance Requirements	This use case requires enhanced governance aligned to its high-impact profile. Use must be: - clearly defined (access control and security only) - proportionate to the risks being managed - designed to ensure tenants retain reliable and fair access to their home DPIA may be required depending on deployment All deployments must include: - clear tenant transparency about: - how access is controlled - what data is recorded - defined ownership and accountability - audit trail of access events and system actions - strong access controls (who can grant / revoke access) - resilience and fallback mechanisms (e.g. manual override) - human oversight of decisions affecting tenant access Systems must include fail-safe mechanisms to ensure tenants are not prevented from accessing their home Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - restrict or control tenant access without lawful justification - analyse access patterns to monitor behaviour without reassessment - use access data for tenancy enforcement without governance escalation - combine access data with other datasets to create behavioural profiles - rely solely on automated processes to grant or deny access Only apply this guardrail where the use is clearly beyond routine housing / building management: This use case may involve processing that requires valid consent. In a social housing context, reliance on consent should be treated as exceptional because of the potential power imbalance between landlord and tenant. Where consent may be relevant, this should trigger enhanced governance, including legal or data protection review, DPIA consideration, and meaningful tenant communication or consultation, rather than being treated as a presumption of permissibility.
Lower-Impact Use	Door entry systems controlling access to communal areas only Smart locks used for: - temporary maintenance access

Field	Content
	- time-limited use cases Access logs: - not retained beyond operational need - not analysed for behavioural insight Results in simpler governance (still RED baseline, but lower intensity)
Higher-Impact Use	Continuous logging and analysis of entry/exit patterns Remote control of tenant access Integration with: - CCTV - occupancy data Use of access data in: - tenancy enforcement - behaviour monitoring Results in significantly enhanced governance requirements
Key Safeguards	Clear and accessible tenant transparency Strict purpose limitation (access control only) Strong authentication and access management controls Separation between: - access control - tenancy decision-making Resilience and fail-safe access (critical) Human oversight of access decisions Proportionate data retention and auditability Controls preventing behavioural profiling Safeguards must be documented, auditable, and enforceable, and subject to regular review

A.9 Workforce and asset management use case profiles

A.9.1 Asset performance monitoring

Field	Content
Use Case	Asset / Property Management
Family	Workforce & Asset
Governance Level	White
Governance Flag	Asset monitoring + operational data + limited tenant impact
Purpose	Monitor landlord-owned assets and property conditions to: - ensure safe and functional housing infrastructure - support maintenance, compliance, and efficiency - identify issues such as equipment failure, heating system malfunction, void properties, and water-system risks (e.g. legionella)
Tier Rationale	This use case: - focuses on property condition and asset performance - may involve non-personal or low-sensitivity data - does not inherently involve behavioural monitoring - supports operational decisions rather than tenancy or enforcement action - involves minimal inference and limited tenant impact This use case does not involve behavioural monitoring or inference when used solely for asset and infrastructure purposes However: - risk increases where data is repurposed - or linked to tenancy, behavioural or occupancy insights Any linkage to tenant behaviour, occupancy, or decision-making requires reassessment of the use case and governance level
Legal Context	Housing (Scotland) Act 2001 Building safety and housing condition regulations Water safety regulations (including legionella management) GDPR: - may involve non-personal data; where no personal data is processed, GDPR does not apply - purpose limitation and accountability remain applicable
Governance Requirements	This use case requires baseline governance aligned to its limited impact profile Use must be proportionate to the intended purpose and balanced against tenant rights and potential impact Clear and bounded definition of purpose (asset-focused use only) Documented lawful basis where personal data is involved

Field	Content
	Audit trail for maintenance and operational decisions Defined ownership (e.g. asset / maintenance teams) Human oversight for any decisions affecting tenants or property access Tenant communication must be clear where systems are deployed within or affecting the home DPIA may be required depending on deployment This classification applies only where the use case remains strictly asset-focused and does not involve inference about occupancy, behaviour, or tenancy decisions. Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - infer tenant behaviour or occupancy without justification - repurpose asset data for tenancy or behavioural assessment - combine with other datasets to create profiles without reassessment - use asset data for enforcement decisions Use must remain limited to property and infrastructure purposes Any change of purpose requires reassessment
Lower-Impact Use	Monitoring infrastructure and assets (faults and maintenance): - boilers, lifts, ventilation systems - water systems (including legionella risk at infrastructure level) - temperature thresholds and system performance Operational use only Results in simpler governance
Higher-Impact Use	Data combined with other datasets Asset data is: - linked to occupancy or behavioural inference - combined with other datasets - used in tenancy or enforcement decisions Results in enhanced governance required.
Key Safeguards	Strict purpose limitation (asset condition, not tenant behaviour) Clear separation of: - asset management - tenancy decision-making Tenant transparency and communication: - tenant consultation may be required depending on impact - consultation is distinct from DPIA

Field	Content
	Controls to prevent: - unintended inference - reuse beyond defined purpose Proportionate use of data at all times Safeguards must be documented, auditable, and enforceable through policies, tenancy agreements, and operational procedures, and regularly reviewed.

A.9.2 Lone worker support

Field	Content
Use Case	Lone-worker use cases
Family	Workforce & Asset
Governance Level	Amber
Governance Flag	Staff safety monitoring + location tracking + limited behavioural inference
Purpose	Use connected devices (e.g. wearables, mobile apps) to: - support the safety of staff working alone - enable emergency alerts and rapid response - monitor location during high-risk activities - provide assurance and duty-of-care capability
Tier Rationale	This use case can: - monitor location and movement of individuals in a work context - capture real-time or periodic safety-related data - detect events such as distress, inactivity, or emergency alerts - introduce some level of behavioural visibility through movement data - monitoring occurs in a workplace rather than domestic context - behavioural inference is limited and purpose-specific - operates at a moderate level of intrusion Risk increases where: - location data is used to assess performance or behaviour - monitoring extends beyond defined safety purposes - data is retained beyond immediate operational need - data is combined with other workforce datasets Risk increases where data is interpreted or used beyond its safety purpose.
Legal Context	Legitimate interest / public task (staff safety and duty of care) GDPR: - involves personal data (location, activity) - does not typically involve special category data - DPIA may be required depending on deployment Human rights considerations: - privacy applies but expectation differs in workplace context - lower Article 8 impact compared to in-home monitoring Important legal contexts for consideration - Health and safety legislation - Employment and workforce protection requirements

Field	Content
Governance Requirements	This use case requires enhanced governance aligned to its moderate impact profile Use must be: - clearly justified (staff safety) - proportionate to the risks being managed - time-bound where possible Clear definition of purpose (safety monitoring only) DPIA may be required depending on deployment All deployments must include: - clear staff transparency and communication - defined ownership and accountability - audit trail of alerts and use - controls on access to monitoring data - human oversight of any actions affecting staff Use must be clearly defined, proportionate to the intended purpose, and limited to the necessary scope
Legal Guardrails	IoT must not be used to: - monitor or assess employee performance using tracking data - track individuals beyond what is necessary for safety - retain or analyse data beyond defined safety needs - repurpose data for disciplinary or behavioural assessment Use must remain limited to staff safety purposes Any change of purpose requires reassessment of the use case and governance requirements.
Lower-Impact Use	Use of lone worker devices for: - emergency alert functions - time-bound location tracking during high-risk tasks - event-based monitoring Results in simpler governance.
Higher-Impact Use	Lone worker data is: - continuously tracked over extended periods - analysed to assess behaviour or productivity - combined with other employee data - used in performance or disciplinary contexts Results in enhanced governance required.
Key Safeguards	Clear staff transparency and communication

Field	Content
	Strict purpose limitation (safety only) Controls on access and use of location data Proportionate monitoring (time-bound and risk-based) Separation between safety monitoring and performance management Human oversight of decisions affecting staff Proportionate data retention Safeguards must be documented, auditable, and enforceable through policies, employment agreements, and operational procedures, and regularly reviewed.

Annex B Handbook and use case definitions

The governance level associated with each use case profile reflects the maximum reasonably foreseeable governance impact that could arise from the deployment, depending on how IoT data and outputs are used, combined, interpreted, or operationalised.

Actual governance implementation should remain proportionate to the intended deployment purpose, operational context, applied safeguards, organisational controls, and level of operational reliance.

B.1 Governance level

Defines the maximum reasonably foreseeable governance exposure associated with the use case and its intended operational use. The governance levels were determined as part of a separate deliverable and as an input to this handbook. This deliverable was also developed by Intelligens Consulting Limited.

The handbook uses four Governance Levels to provide a consistent indication of the maximum reasonably foreseeable governance exposure associated with a use case.

- White – Primarily asset, infrastructure or operational uses with limited governance exposure and limited impact on individuals.
- Green – Lower-impact uses where governance requirements remain relatively straightforward and are typically associated with safety, compliance or operational monitoring.
- Amber – Moderate governance exposure where data use, operational context or potential impacts on individuals require increased governance attention, oversight or safeguards.
- Red – Higher governance exposure where deployments may directly affect individuals, involve behavioural inference, health or wellbeing considerations, significant monitoring, tenancy implications, safeguarding considerations or decision-making affecting people.

The colour associated with a Governance Level provides a quick visual indication of the governance attention likely to be required. However, governance implementation should always remain proportionate to the intended purpose, deployment context, safeguards and organisational controls applied in practice.

The Governance Level:

- reflects the baseline level of governance expectation associated with the use case profile
- supports proportional governance planning and decision-making
- helps organisations understand where additional governance, oversight, safeguards, reassessment, transparency, or specialist input may become appropriate.

The Governance Level does not automatically determine:

- whether deployment is appropriate or permissible
- the final governance implementation outcome

- the exact safeguards required in practice.

Actual governance implementation should remain proportionate to:

- deployment context
- operational use
- safeguards and controls applied in practice
- tenant impact and expectations
- organisational governance capability and oversight arrangements.

B.2 Governance flag

Provides a concise description of the nature of the use case and the type of governance considerations typically associated with it.

The Governance Flag helps organisations quickly understand:

- the types of governance considerations likely to apply
- whether the deployment may involve:
    - environmental monitoring
    - behavioural inference
    - health or wellbeing considerations
    - tenancy-related implications
    - operational prioritisation
    - safeguarding considerations
    - AI-supported analysis
    - enhanced transparency or oversight expectations

The Governance Flag supports early governance awareness before organisations assess detailed governance requirements.

B.3 Governance requirements

Defines the minimum governance expectations typically associated with the use case.

Governance requirements help organisations understand:

- the types of governance activity likely to become appropriate
- the level of governance oversight expected
- where additional safeguards, auditability, transparency, reassessment, or human oversight may be required
- where legal, privacy, safeguarding, procurement, operational, or specialist involvement may become necessary

Governance requirements support:

- consistency,
- proportionality,

- transparency,
- and defensible deployment decision-making.

Governance requirements should be interpreted proportionately alongside:

- deployment purpose,
- operational context,
- safeguards applied,
- organisational capability,
- and operational reliance on IoT outputs.

B.4 Legal guardrails

Defines the non-negotiable legal, ethical, governance, and tenancy boundaries that must not be crossed regardless of deployment context or operational benefit.

Legal guardrails help organisations understand:

- where additional legal awareness or escalation may be required
- where organisational accountability or tenant protections must remain preserved
- where certain operational approaches may be inappropriate regardless of intended benefit

Legal guardrails apply across all deployment stages and should continue to be considered throughout reassessment and lifecycle governance activities.

Use case profiles identify the maximum reasonably foreseeable governance exposure associated with a deployment.

Actual governance implementation should remain proportionate to:

- the intended purpose of the deployment
- the way IoT data and outputs are used in practice
- operational reliance on IoT outputs
- safeguards and controls applied
- organisational governance capability
- tenant impact and deployment context

Governance exposure may increase where deployments:

- expand,
- combine use cases,
- introduce behavioural inference,
- increase operational reliance,
- or evolve beyond the original intended purpose over time.

This will become one of the most important interpretive principles in the entire handbook.

Annex C Best practices

The sections that follow provide a set of best practices, aligned to the sections in the handbook. that can be referred to by users. For more detailed information, please refer to the sources or contact the relevant organisation.

C.1 Step 1 – Define the use case

Best Practice	Why It Matters	Source
Start with the outcome to be achieved, not the technology.	Deployments are more successful when framed around housing, safety, compliance or tenant outcomes rather than introducing sensors.	NG Homes; Glasgow stakeholder engagement.
Clearly define how data will be used and what it will not be used for.	Strong purpose limitation reduces governance uncertainty and helps build tenant trust.	North Lanarkshire; HSCP; Aico.
Distinguish property-focused monitoring from tenant affecting monitoring.	Governance requirements can change significantly depending on how outputs are used.	LOTI Damp & Mould Report.

C.2 Step 2 – Assess organisational and governance readiness

Best Practice	Why It Matters	Source
Identify who owns the alert-to-action process.	Projects often fail when alerts are visible but no-one is accountable for acting on them.	Aico; Archangel; NG Homes, LOTI Information Processes
Embed IoT into existing processes and workflows.	Existing repairs, compliance and housing processes are often more scalable than creating separate IoT processes.	Craigdale Housing; Bield & Care; LOTI Information Governance Processes.
Start small, learn, then scale.	Pilots help organisations understand governance, access and operational challenges before wider deployment.	Barrhead; SSA Partners; Information Governance Processes
Plan for organisational change alongside technical deployment.	IoT often requires changes to workflows, responsibilities and decision-making arrangements.	HSCP; SSA Partners; Information Governance Processes
Establish governance, legal, privacy and accountability arrangements before scaling.	Organisations may encounter delays, uncertainty and inconsistent decision-making where controller, processor, accountability or review arrangements are not defined early. Consider developing reusable governance artefacts, such as DPIAs, decision logs and assurance documentation, that can be adapted across future deployments.	North Lanarkshire; HSCP; ARC Technical Guidance
Ensure sensors, platforms and monitoring arrangements are capable of producing reliable and technically defensible data.	Governance decisions, repairs interventions and tenant engagement activities should be based on data that is accurate, appropriately located, maintained and periodically verified.	UK Housing Retrofit Technical Guidance (BPE Guide); industry good practice.
Establish governance, legal, privacy and accountability arrangements before scaling.	Organisations may encounter delays, uncertainty and inconsistent decision-making where controller, processor, accountability or review arrangements are not defined early. Consider developing reusable governance artefacts, such as DPIAs, decision logs and assurance documentation, that can be adapted across future deployments.	North Lanarkshire; HSCP; ARC Technical Guidance

C.3 Step 3 – Governance classification

Best Practice	Why It Matters	Source
Apply governance proportionately to the purpose and impact of the deployment.	Governance needs often increase where outputs affect people rather than property.	Intelligens research; LOTI Damp & Mould Report; Information Governance Processes
Reuse governance artefacts where appropriate.	Shared DPIAs, governance approaches and assurance models can reduce duplication.	North Lanarkshire; HSCP; Archangel; Aico; Information Governance Processes
Consider modular governance approaches for connected IoT ecosystems.	Common platforms may support multiple use cases with shared governance foundations.	North Lanarkshire; Information Governance Processes
Where possible, use recognised housing and building standards when defining risk thresholds.	Aligning monitoring and reporting approaches with recognised housing, building and ventilation standards can reduce subjectivity and support more consistent decision-making.	Approved Document F (England & Wales); housing-sector good practice.

C.4 Step 4 – Assess the intended deployment

Best Practice	Why It Matters	Source
Define alert thresholds, ownership and response pathways before deployment.	Unclear response processes can create unnecessary workload and inconsistent interventions.	Craigdale Housing; Bield & Care; HSCP; Information Governance Processes
Treat sensor outputs as indicators requiring review rather than automatic evidence of a problem.	Environmental sensors typically identify conditions associated with risk rather than confirming causation. Outputs should be interpreted alongside inspections, property information, resident engagement and operational context.	LOTI Damp & Mould Sensor Report.
Align installation activity with existing tenant access opportunities.	Existing visits can improve installation success and reduce tenant disruption.	Barrhead; SSA Partners; LOTI; Information Governance Processes
Avoid assuming tenants are responsible for issues identified by sensors.	Issues may be influenced by building condition, fuel poverty or wider circumstances.	LOTI Damp & Mould Report; Glasgow stakeholder engagement; Information Governance Processes

Best Practice	Why It Matters	Source
Consider supported accommodation, temporary accommodation and homelessness settings separately.	Communication, accountability and support pathways may differ from standard tenancy settings.	HSCP; SSA Partners; Information Governance Processes
Define how sensor outputs will be validated before interventions are triggered.	Sensors should support decision-making rather than replace professional judgement. Organisations should understand what additional checks, inspections or contextual information are required before action is taken.	LOTI Damp & Mould Sensor Report; Craigdale Housing; Bield & Care.
Deploy sensors in locations consistent with recognised technical guidance.	Poor sensor placement may generate misleading readings, increase false positives and reduce confidence in data quality.	UK Housing Retrofit Technical Guidance (BPE Guide).
Consider calibration, maintenance and ongoing assurance of sensor performance.	Sensor accuracy may deteriorate over time. Periodic verification against known-good equipment can improve trust in outputs and support evidence-based decision-making.	UK Housing Retrofit Technical Guidance (BPE Guide).

C.5 Step 5 – Governance definition, readiness and approval

Best Practice	Why It Matters	Source
Confirm who receives, reviews, interprets and acts on outputs.	Accountability should be clear before deployment proceeds.	Craigdale Housing; Bield & Care; HSCP;
Keep accountability with the social landlord.	Suppliers may support delivery, but accountability remains with the landlord.	Information Governance Processes
Ensure partner organisations understand their role.	Multi-agency deployments require agreed responsibilities and escalation arrangements.	HSCP; Bield & Care; Information Governance Processes
Use tenant communications that are accessible and practical.	Understanding and trust are improved through simple, transparent communications.	Aico; Barnet; LOTI Damp & Mould Report; Information Governance Processes
Treat transparency as an ongoing activity rather than a one-off exercise.	Changes in purpose, organisations involved or use of outputs may require further engagement.	LOTI Information Governance Review Guidance.
Define in advance what outcomes will be measured and how success will be evaluated.	Organisations should understand whether deployments are improving housing conditions, tenant outcomes, operational performance or compliance activity, rather than simply generating additional data.	LOTI; Glasgow stakeholder engagement.
Ensure monitoring approaches support housing and regulatory obligations rather than creating alternative standards.	IoT solutions should support compliance, evidence gathering and proactive intervention, but should not replace existing legal, regulatory or professional obligations.	Scottish Housing Regulator Damp & Mould indicators; housing regulatory guidance

C.6 Step 6 – Governance review and reassessment

Best Practice	Why It Matters	Source
Review governance when deployments expand or change.	New purposes, users, technologies or data sharing arrangements may change governance requirements.	LOTI Information Governance Review Guidance; Information Governance Processes

Best Practice	Why It Matters	Source
Test whether processes work before scaling.	Testing helps identify governance, workflow and data quality issues before wider deployment.	LOTI Testing Guidance; Information Governance Processes
Review whether the original purpose remains valid.	Reassessment may be needed if purposes or stakeholders change over time.	LOTI Information Governance Review Guidance; Information Governance Processes
Capture and share lessons learned.	Shared learning can reduce duplication and support more effective deployments across the sector.	North Lanarkshire; HSCP; Archangel; Aico; Information Governance Processes
Periodically review whether monitoring thresholds, assumptions and response pathways remain appropriate.	Experience gained after deployment may identify false positives, missed risks or unintended operational impacts that require adjustment.	LOTI Testing Guidance; LOTI Information Governance Review Guidance

Annex D Sources used outside GCR

How to Undertake an Information Governance Review for a Project or Process, loti.London

Drivers, foundations and data protection considerations for damp & mould-related data projects, loti.London

Information Governance Considerations for System or Process Testing, loti.London

Internet of Things (IoT) Sensors for Damp and Mould, loti.London

UK Housing Retrofit Technical Guidance (BPE Guide)

HomeLINK Resident Leaflet, Aico (Barnet Homes)

Approved Document F (England & Wales); housing-sector good practice