Smart Places Playbook

Standards

June 2021

Table of Contents

1 BACKGROUND TO NAVIGATING STANDARDS - THE 'WHY?'

1.1 Standards, policy and legislation: understanding the connection

Standards are part of our everyday lives. From concrete structures, to the design of bridges we drive on, to the security of digital systems we use for email and storage of documents, they are making their mark. Standards are a constant feature of infrastructure - physical, digital and cyber-physical. Companies such as Amazon, Google, IBM and Microsoft adopt standards at-scale, particularly in relation to their cloud services, demonstrating their global reach and relevance.

The International Organization for Standardization (ISO), one of the pre-eminent consensus-based international standards development organisations, defines a standard as: "a document, established by a consensus of subject matter experts and approved by a recognized body that provides guidance on the design, use or performance of materials, products, processes, services, systems or persons.[1]"

Standards and smart places - an introduction

Standards can play a strong role in the creation of smart places by providing a framework to scale solutions more safely, securely and efficiently. They can help to provide the 'how' of implementation and scale, when councils, agencies, developers or other businesses might have already determined the 'why' - realising the benefits, and relevant risks, of digital adoption to smart places.

Legislation - legal requirements for smart places

Legislation provides the mandatory requirements to govern the development of smart places, and indeed all places. Legislation traditionally outlines the prescribed course(s) of action, as well as the consequences of inaction or negligence. These consequences might include corrective action, fines, or even imprisonment. In many cases, the NSW Parliament, as with other Parliaments, outlines requirements or consequences through legislation, but the specific actions needed to meet specific legal thresholds are at the discretion of business owners, councils or indeed Government agencies themselves. In short, there are the rules, but very often there is no consistent playbook, particularly when it comes to areas like infrastructure.

This is where standards can add value. For example, the Australian Privacy Principles specify principles that apply in specific circumstances for businesses, with an exemption for some small businesses (based on turnover), but the implementation of these differs. Similarly, the National Construction Code (NCC) provides a broad framework governing construction in Australia, and State legislation gives effect to it. To satisfy the requirements of this framework developers, certifiers and others can follow one of two fundamentally different approaches:

1) the performance-based process, using materials and methods they determine will meet performance requirements for buildings, or
2) the 'deemed-to-comply' pathway, which involves the use of Standards referenced in the relevant legislation and through the NCC process

The 'deemed-to-comply' pathway provides arguably greater technical specification and certainty, when used correctly.

Policy - rules and principles

Policies set broad expectations for agencies, as well as the private sector, in relation to specific areas of responsibility. While policy documents might not always stipulate specific actions or standards, they often reference these. Historic examples have included the way in which ISO/IEC 27001 was referenced in whole-of-government

[1] ISO (2021). *Standards in our world*. Retrieved from: https://www.iso.org/sites/ConsumersStandards/1_standards.html

cyber security policies, in different States and Territories. In that case, partners or companies could cite the standards they use as being consistent with policy that the Government itself set. In other cases, where policy directives are broader, for example by referencing 'good' or 'best' practice in relation to cyber security (and in the absence of other granular requirements), companies, councils or agencies can point to their adoption of standards as effectively meeting those requirements.

Standards - how to do something

Within the context of Smart Places, the family of ISO 37100 standards are often considered the building blocks of creating sustainable cities and communities, commonly referred to as 'smart cities' in the international standards community. The flagship standard ISO 37101:2016 *Sustainable development in communities,* provides an overall framework for defining sustainable development objectives as well as a roadmap to achieving them. The ISO 37101:2016 is considered a management system standard, which provides a set of policies, processes and procedures to help organisations achieve their objectives and goals. A management system standard considers the way an organisation manages different parts of its business; therefore, these standards provide guidance and recommendations to organisations on processes and procedures to meet those objectives.[2] Refer to section 1.3 for further information.

The ISO 37101:2016 is designed to help communities **define** their sustainable development goals and create a **strategy** to achieve them. The standard sets out the broad principles that a community may wish to adopt as part of their sustainable development strategy, such as improving citizens' well-being and to consider issues such as health and mobility, to help define their sustainable development objectives. The standard is designed to be used at the community level to reflect the number of interests and stakeholders involved in real-life cities and community projects. It also encourages the creation of a group or structure to support the implementation of initiatives on behalf of the community. The focus of ISO 37101:2016 is to involve all interested parties to help define and implement a sustainable development strategy. Naturally, citizens of a community are one of the most important stakeholder groups, which is why the standard encourages a citizen-centric approach in the future design and development of a community.[3]

1.2 Should I aim for certification or just demonstrate I meet requirements in an ongoing way?

There are generally two approaches to using standards that are adopted by the market - certification (a compliance-based approach) and ongoing maturity assessment. Many people spend significant amounts of time agreeing or disagreeing on which approach to adopt, but they are both complementary and serve particular purposes. Often, the pathway adopted is shaped by contractual requirements (for example, where a company or government agency requires evidence of certification to a particular standard for a particular solution). Alternatively, there might be policy or business drivers to demonstrate maturity, aligning with corporate reputation (i.e., if a company or council wants to demonstrate that the approach they are using to risk management is broadly based on a standard accepted globally - putting them ahead of the pack in a niche area). This can be termed the maturity assessment model, and is more open than certification (usually undertaken at a point in time).

A ***compliance-based approach*** assesses performance (of an organisation, process or product) at a particular point in time via an external audit and subsequent certification (if applicable). This checks whether you have considered and acted on the technical requirements of a particular standard. As an example, ISO/IEC 27001 (information security management) requires a range of measures to be adopted to meet the requirements for certification. This

[2] ISO (2021). *Management System Standards*. Retrieved from https://www.iso.org/management-system-standards.html
[3] ISO (2016). *ISO 37101 Sustainable Development in Communities*. Retrieved from https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso_37101_sustainable_development_in_communities.pdf

means businesses often undertake a full audit to identify any gaps in their practices, and what they need to do to raise their information security posture, before they are certified as ISO/IEC 27001 compliant, by an external provider.

The ongoing ***maturity assessment model*** is for standards that don't necessarily follow a check-box logic, and that aren't able to be certified against. Examples include standards like ISO 31000 (Risk Management - Guidelines), which provides a methodology for undertaking risk assessment, so that risks are identified and can be effectively managed. The standard is clear on the approach to be used for risk assessment, but the population of data and the specific approach to documenting material will differ between organisations.

1.3 The difference between governance, management, and technical standards (i.e., device-specific)

There are a range of standards in existence, locally and internationally. Indeed, there are tens of thousands of international standards in existence. Finding the standard(s) that is fit-for-purpose is the key challenge. One way we can think about standards is to group them according to the following list, which helps to define what these standards apply to and what they do. This can help teams to think through what standard they might wish to use, for assurance purposes, for procurement, or even as evidence of commitment to quality assurance when working with partners.

Governance standards - frameworks/indicators

Governance standards provide guiding principles, frameworks and indicators to enable organisations to meet their responsibilities. These are useful for helping organisations to evaluate, monitor and measure compliance against the organisation's stated objectives. For example, ISO/IEC 27014:2020 *Information security, cybersecurity and privacy protection — Governance of information security*, provides guidance to organisations on how to evaluate and monitor information-security related processes within an organisation.

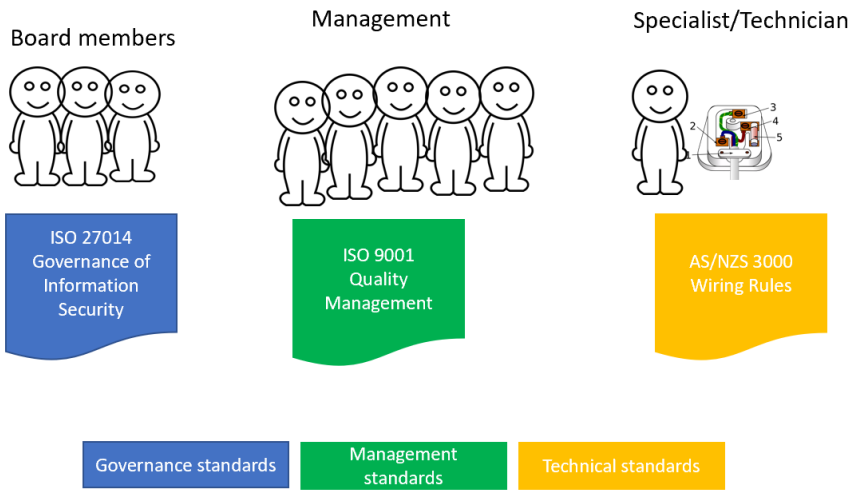
Management system standards - processes e.g., lifecycle management

Management standards provide guidance and recommendations on processes and procedures within an area or across a range of discipline. A popular management standard is the ISO 9001 *Quality Management*, which sets out processes and procedures to deliver consistent products and services to customers.

Technical standards - technical specifications e.g., how to install a device

Technical standards provide technical specifications related to a product or service. It may include specific measurements or performance requirements. The most common standard is the Electrical Wiring Rule AS/NZS 3000:2018, which provides the minimum regulatory requirements for electricians to use when installing electrical work in people's homes and offices.

Simplified view of how a standard is used in an organisation



This is only a starting point, but it helps to make sense of the world of standards. It helps to answer questions particular stakeholders might have. In infrastructure, for example, an engineer might want to ensure that a particular product or piece of work meets technical requirements, where technical standards might be relevant. For an IT project, an assurance team might want to make sure that an organisation has clear, and documented, processes to manage complaints, undertake risk assessment, etc., which most closely relates to management system standards. Finally, executive leaders might be focused on ensuring that effective governance is in place, on the part of a partner, or that globally agreed high level metrics are being reflected, which aligns with the focus of governance standards.

1.4 Using standards for procurement: good practice

Standards can be used by councils, government agencies and companies, through their procurement processes and supply chains, to drive behaviour change and introduce greater levels of quality assurance. There are three main mechanisms councils and government agencies, in particular, can adopt to ensure that standards are a core consideration in smart places-related activity: (1) mandating technical specifications, (2) asking suppliers targeted questions and (3) scoring proposals (including through weighting) in a way that takes standards into account.

1.4.1 Mandating technical specifications

A commonly used approach, across both the public and private sectors is to mandate the use of particular technical standards, through commercial contracts, when building new facilities or delivering new services, for example. This tends to be in areas such as infrastructure, where standards relating to concrete, steel or telecommunications, for example, are frequently cited. This approach tends to focus on particular technical requirements for a specific project, and is heavily focused on quality assurance, for understandable reasons - particularly where life and limb is concerned, and where governments, companies and other partners want to reduce risk(s).

Example: A local council is deploying multi-functional poles as part of an initiative to drive improvements in urban amenities and sustainability. They use a Request for Proposal (RFP) process to commence this, and the documentation includes reference to specific technical specifications, including relevant international standards. This is because the scope of work is known and there are regulatory requirements in this area. Those bidding are required to demonstrate how they meet these requirements.

1.4.2 Motivating suppliers: asking the right questions

A complementary approach involves asking suppliers open questions about their commitment to standards through EOI or other tender-related processes. For example, as part of a 'scope of work', aspiring partners might be asked to list any recognised international or Australian Standards they adopt and/or comply with, in relation to a particular product or service. This enables a company that has truly embedded standards across their business to demonstrate, in a transparent and competitive way, their track record, rather than focusing only on specific technical requirements for a particular project. As a result, you might learn more about the company's particular capabilities and how secure their underlying architecture is, in a way that is not possible with a narrower approach. This might also uncover, for technical teams, emerging standards that market leaders are adopting in relation to newer forms of smart-places related technology.

Example: A government agency is procuring smart technologies. They are looking to scan the market for capabilities, so they have an EOI process established. Instead of specifying particular standards, they instead ask those lodging EOIs what standards they adopt and how. This provides the agency with both a capability view, in terms of products and services, but equally enables them to effectively assess the way in which different partners adopt standards, across the market of potential suppliers. They can then make a more informed decision on ultimately awarding work during subsequent stages of the procurement process.

1.4.3 Scoring and assessing proposals

Both mechanisms (mandating technical specifications and asking for suppliers to demonstrate their adoption of a suite of standards) can support robust scoring and assessment of proposals. For example, a team managing a tender might, from the outset, afford a weighting of 5% or higher to all eligible applications, resulting in formal assessment of capability against this requirement. This both elevates the importance of standards in the process, but creates a business-driver for market led adoption of standards. There are other things people working in procurement can support, including making some standards-related costs allowable, so that where a provider is not yet at a particular maturity point, but has the best value offering, they are able to include certification and audit costs in relation to standards, within their proposal/bid.

Example: A tender process is designed and includes the usual emphasis on value for money and other considerations. The team managing the procurement process proactively decides to afford a weighting of 5% to 'evidence of standards adoption' early in the process. This means that potential suppliers who both demonstrate value for money, and technical capability, can also be recognised for their conformance with International and Australian Standards. This creates a tangible driver for standards adoption on the part of potential suppliers.

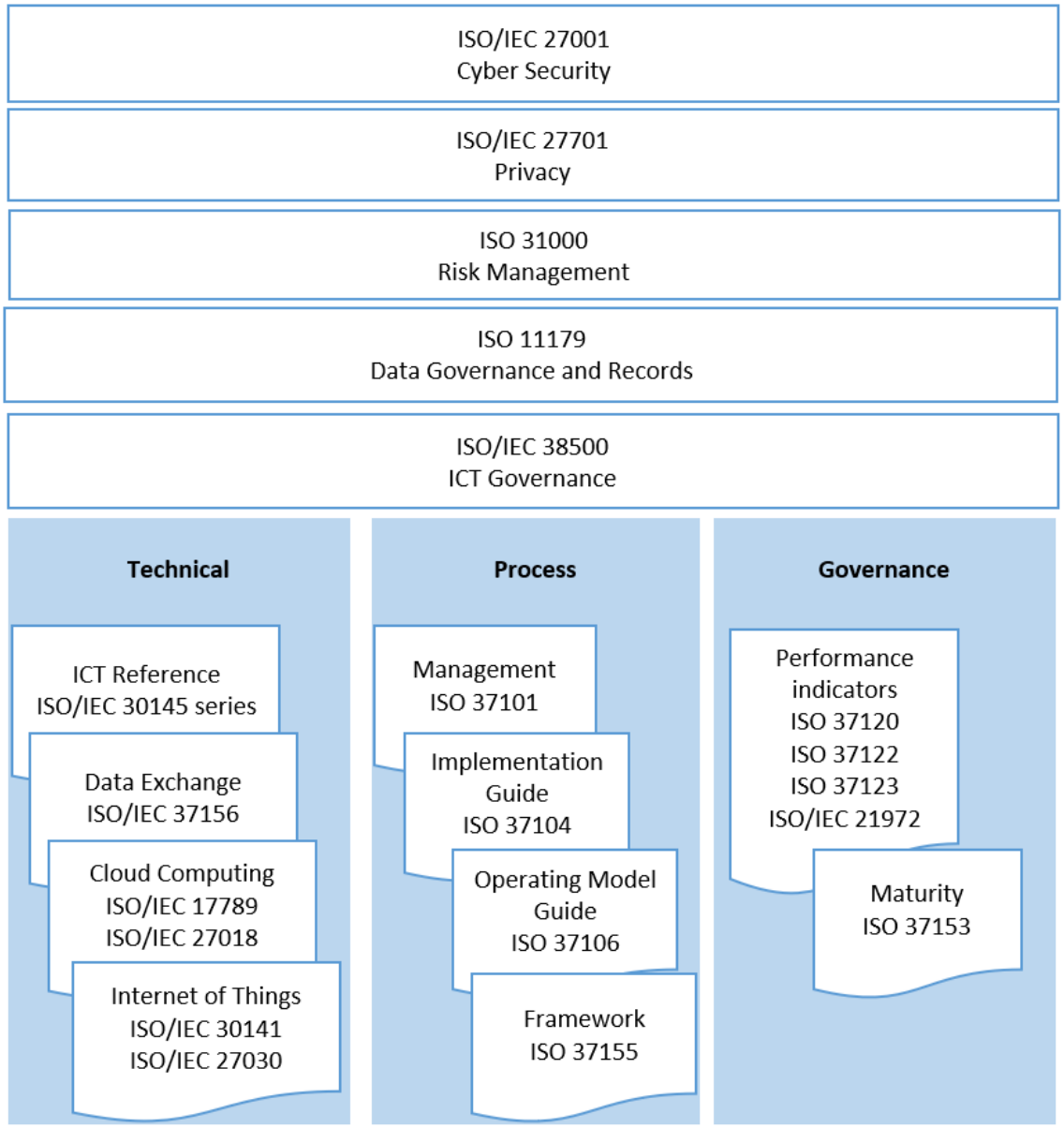
Checklist:

For your smart places project, or program of activity, have you:

- Identified how you will use standards during the procurement process, or during the subsequent implementation and activation phase?
- Consulted with colleagues, including technical teams, to distinguish the requirements you have for hardware and software, and the assurance you might need around issues such as governance in areas like privacy or risk management?

2 VISUALISING THE USE OF STANDARDS FOR SMART PLACES - A SNAPSHOT

Standards can operate at a range of levels. One way to think about standards for smart places is to think about technical and process standards for particular projects, to build and install things, and then to think about the broader systems companies might have in place to provide those services and provide assurance for customers (for example, broad all-hazards risk management, privacy and information security, for a company installing devices managing data traffic, as one example). Below, we outline how this might look in relation to smart places. One way to think about this is through a cascading model, with higher level standards leading to more specific adoption of standards in areas identified as important, following risk assessment.



Adapted from Figure 2 of ISO/IEC TS 27570:2021(en), Privacy protection — Privacy guidelines for smart cities

3 RISK MANAGEMENT FOR SMART PLACES - A STANDARDS-BASED APPROACH

Doing risk management: understanding the 'how' and identifying where to start

Any standards-based approach to smart places should involve structured and documented risk management. Risk, which refers to 'the effect of uncertainty on objectives,' is evident in all activities, but managing it effectively distinguishes mature organisations from others. The development of smart places presents many clear opportunities, and manifests some risks, particularly in relation to the adoption of technology, at-scale or particular local intensity. In this context, effective risk management can help build trust within teams designing or executing smart places projects. In particular, it can elevate specialist expertise and provide visibility to colleagues of factors that might not previously have been considered in project planning or public messaging, for example.

Risk assessment for smart places should be informed by the logic of I*SO 31000 (Guidelines - Risk Management).* ISO 31000 is an internationally recognised approach to assessing, understanding and responding to risk. It was developed following an earlier Australian/New Zealand Standard. As an International Standard it has deliberately been designed for entities of any size, making it broadly applicable and without limiting its use to large organisations or agencies alone. It is available to view, at no-cost currently, via the ISO website, here.

ISO 31000 provides principles, a framework and a process for managing risk, including the following factors:

- Leadership and commitment (including buy-in at executive level and throughout the organisation)
- Communication
- Risk identification
- Risk treatment

In the following section, we outline what some of these pillars mean in the context of smart places. In appendix A you will find an example checklist that can be used to conduct such a risk assessment exercise. Remember that your assessment, including proposed treatment, or mitigation measures, will be unique to the context in which you are operating, so you should augment this checklist with factors known to you, in addition to those provided in the attached checklist.

Whilst ISO 31000 is not a standard that an entity certifies against, there are many private companies who offer audit services, based on experience and their own templates, to assist you in using this standard for your own purposes.

Refer to Appendix B for the Risk Management Plan example.

3.1 Designing risk assessment

1. Determine the ***scope*** of your risk assessment. For example, does it apply at a project level, a program level, organisation-wide, or Board level? For smart places projects, an entity, or organisation, might want to undertake wider risk assessment if they are providing data processing services, for example, whereas the physical installation of a device from an entity that embraces risk management might warrant a narrower, project-specific assessment (i.e., at a site or neighbourhood level).

2. Define the ***context*** of your risk assessment. This should focus on both the *internal* and *external* factors that drive risk for an organisation or entity. ISO 31000 refers to factors like 'contractual relationships and commitments', and 'political, legal, regulatory, financial, technological, economic and environmental factors', as external risk factors. You might consider factors such as: where products are manufactured, where and how data is stored, and the human rights situation in countries where vendors/partners are headquartered. Internal factors are defined as data and information systems, as well as "relationships with internal stakeholders, taking into account their perceptions and values," and this might include the values of staff.

3. Agree on an approach to ***communicate*** about risk within the organisation, including consideration of the role of leadership internally. For example, who will lead the risk management program, steer the process, and how will those who participate have key information shared with them at the end of the process? Who, specifically, will be responsible for ongoing, iterative, updates to the risk management program, once the first assessment is undertaken?

3.2 Conducting risk assessment

Identify risk: This is the first logical step in any documented risk management process. It involves the development of an initial list, or register, of known risks. It should be undertaken at an executive level, with inputs from practitioners with carriage of key business areas. This should be all-hazards, meaning it covers all known risk to an entity, so that it is comprehensive and transparent. Factors might include: internal and external risk, and the sub-categories of these might include: employment (such as screening, processes), legal liabilities through commercial contracts, or supply chain security and the regulatory environment.

Analyse risk: This refers to understanding the nature of the risks you have identified. Steps include: discussing where particular vulnerabilities might be, how some identified risks might be connected to other risks and whether it is correctly described and defined. An example might be employment. Poor pre-employment screening might lead to insider threats materialising, resulting in the loss of IP, and might result in termination (legal risk), and damage to corporate reputation (reputational risk).

Evaluate risk: Once risk has been analysed, it should be evaluated comprehensively. This refers to understanding the likelihood a risk will materialise, using factors such as magnitude of impact and time (i.e., if this unfolded in the near future, or in 5 years' time). This ensures that you can both rate risks effectively, and prioritise treatment for the most critical risk factors. Evaluation of risk also refers to decision-making around how to respond to this risk, including responses such as: (a) do nothing further, (b) use existing controls etc., as outlined in ISO 31000.

3.3 Responding to, and acting on, risk(s)

Treatment of risk: Once risk has been identified, analysed and evaluated, it should be treated (see simplified common template – Annex A). In treating risk, you should think about factors such as: 'removing the risk source', 'changing the consequences of the risk,' or even not proceeding, based on an informed business decision.

Documenting response(s) to risk: Once operational, your approach to risk management should remain active and iterative. A process for documenting known risks that have materialised, and treatment options and courses of action, should be maintained. This is often referred to as a 'risk register,' traditionally maintained by a company secretary and with visibility for senior s executives, and segmented to business areas, as needed. But it should include robust policies and processes more broadly. Entities should also think through a common reporting process for recording and assessing emerging risks that are identified, to maintain the cyclical and open approach to risk assessment.

Checklist:

For your smart places project, or program of activity, have you:

- Undertaken a structured, and documented, risk assessment process, consistent with the methodology of ISO 31000?
- Implemented policies to support sustained risk management, with clear leadership and ownership, and communicated this to employees and partners?

4 SMART INFRASTRUCTURE

The NSW Government's Smart Infrastructure Policy established the requirement that from 2020 onwards, all new and upgraded infrastructure will need to incorporate smart technology to achieve the government's vision of connected communities, to meet growing population needs, improve sharing of infrastructure data and obtain return on infrastructure investment.[4] Additionally, the global challenges of COVID-19 have accelerated the uptake of technology and changed the way we live and work. However, integrating technology and ICT into the urban environment requires services to be interoperable, accessible, energy efficient and scalable.[5] This is where standards can play a role in providing guidance and technical recommendations that decision-makers can use to set priorities, goals and objectives to accelerate their vision of connected communities.

4.1 Frameworks and maturity models

Developed by the international technical committee ISO/TC 268/SC1 *Smart community infrastructures,* there are currently 18 international technical publications of which 14 are international standards on smart community infrastructures.

As a starting point, the ISO 37153:2017 *Smart community infrastructures — Maturity model for assessment and improvement,* provides a methodology to determine the level of smart community infrastructure maturity within an area or community, to assist planners and designers in identifying potential areas of improvement. The standard can be used to assess all types of community infrastructure, including energy, water, waste, transportation and ICT.

The recent publication of the following international standards provides a framework for the integration and operation of smart community infrastructures, from lifecycle to strategy development of smart community infrastructures:

ISO 37155-1:2020
Framework for integration and operation of smart community infrastructures — Part 1: Recommendations for considering opportunities and challenges from interactions in smart community infrastructures from relevant aspects through the life cycle.

ISO 37155-2:2021
Framework for integration and operation of smart community infrastructures — Part 2: Holistic approach and the strategy for development, operation and maintenance of smart community infrastructures.

These standards provide the framework, including processes and methodologies to describe the interactions between community infrastructures, stakeholders and the external environment to ensure they are identified and managed. The standards can be applied in two potential scenarios: a greenfield site, where the infrastructure is being designed and developed, and a brownfield site, where there are existing urban infrastructures. It is considered a useful guide by planners and investors involved in new infrastructure developments by providing specifications to manage interactions and to establish appropriate measures in the planning and operation phase.[6]

[4] NSW Government (2019). *Smart Infrastructure Policy*. Retrieved from https://www.digital.nsw.gov.au/policy/smart-infrastructure-policy
[5] ITU (2021). *Smart Sustainable Cities*. Retrieved from https://www.itu.int/en/publications/Documents/tsb/2021-ITU-Smart-Sustainable-Cities/index.html#p=1
[6] ISO (2021). *ISO 37155-1:2020 Framework for integration and operation of smart community infrastructures — Part 1: Recommendations for considering opportunities and challenges from interactions in smart community infrastructures from relevant aspects through the life cycle.* Retrieved from https://www.iso.org/obp/ui/#iso:std:iso:37155:-1:ed-1:v1:en

4.2 Community security and resilience

When designing or planning urban areas, place owners may consider incorporating the ISO 22300 series developed by the international technical committee ISO/TC 292 *Security and Resilience*, for guidance on emergency management and developing community resilience to proactively plan for the needs of the community, in the event of an emergency.

The International Organization for Standardization (ISO) has many standards to support community resilience such as ISO 22328-1:2020 which provides guidance for implementing a community based disaster early warning system (EWS), ISO 22326:2018 to monitor facilities with identified hazards, ISO 22396:2020 for information exchange between organisations and ISO 22395:2018 for supporting vulnerable persons in an emergency. These standards help the community prepare for unexpected circumstances while fostering the development of safe and secure communities.

4.3 Related technical standards

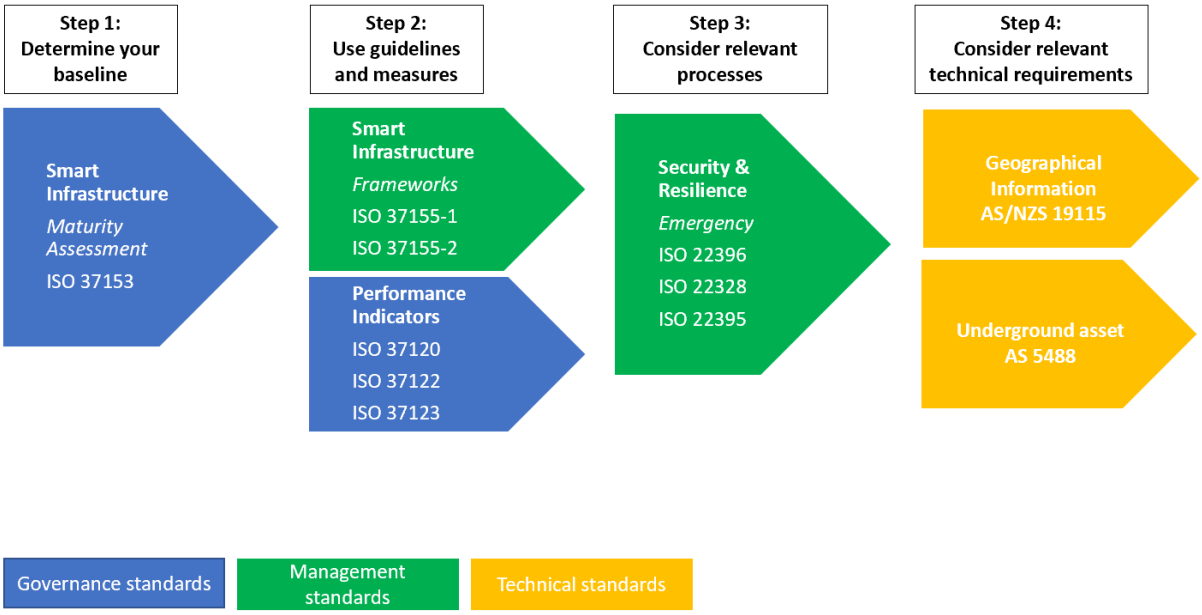
Within the smart infrastructure ecosystem, there may be specific technical standards providing guidance on asset information. For example, the technical standard AS 5488.1:2019 *Subsurface utility information* for the classification of underground assets, developed by the Australian Standards Committee IT-036 *Subsurface Utility Information,* to provide a consistent approach in recording the location and mapping of underground utilities assets. The first publication of the AS 5488 was made in 2013, and since the revised version in 2019, the technical committee is currently reviewing the AS 5488 to incorporate the Australian Government's standard for geospatial data as defined by the Geocentric Datum of Australia 2020 (GDA2020). The move towards GDA2020 is to improve the accuracy of Australia's geospatial data by aligning it more closely with the Global Navigation Satellite System (GPS) positions.[7] Similar to AS 5488, the AS/NZS ISO 19115:2015 *Geographic information - Metadata, Part 1: Fundamentals* is also under review to reflect the requirements of GDA2020. In the longer term, as the NSW Government continues to develop its Digital Twin platform, using AS 5488 as a guide to record, collect and identify underground utilities assets and/or AS/NZS ISO 19115 to structure geographical metadata will increase the accuracy of data records on assets held by the state.

4.4 Relationship with standards

When considering the relationship between standards and smart infrastructure, it is important to note that there are hundreds of standards that exist to support planners, engineers and the community to design a safe and sustainable community. It is not necessarily a one size fits all approach but rather an opportunity to tailor the list by selecting the main standards that can support place owners to achieve their goals and objectives. The key consideration is the type of standardisation, that is, process, governance and technical (see section 1.3). Based on these themes, a place owner can narrow down the list of standards according to their desired outcome. Each standard has a specific scope and objective, which can be used to assess the suitability of the standard. The below diagram provides a simplified view of the relevant standards that could be considered when planning and designing new infrastructures or repurposing existing infrastructures.

[7] ICSM (2020). *Geocentric Datum of Australia 2020*. Retrieved from https://www.icsm.gov.au/gda2020

Simplified Example of Applying Standards



4.5 Use Case 1: Smart meters (electricity) - application of standards

With the growth of smart grids and smart homes, smart meters have become an important part of the energy network. A smart meter, also known as an advanced meter, is a device that digitally measures a household or businesses energy consumption.[8] Smart meters are manufactured and installed according to international and Australian Standards. These standards provide technical specifications for vendors, suppliers and installers to ensure they meet the minimum safety and performance requirements. While they have limited application for the average consumer, these standards provide market confidence that the products are safe to use and correctly installed. As of June 2021, there are currently 25 relevant technical standards for smart meters (electricity), as summarised in Appendix A.[9]

4.6 Use Case 2: Digital meters (water) and Smart water meters – general guidance

'Smart meters' also have applications in the water sector, but the standards for smart water meters have not been fully developed. This may be due to the early phase of adoption, with trials taking place across Australia and therefore a period of maturity will need to occur before smart water meter technical standards are established. Currently, Sydney Water is trialing digital water meters in the suburbs of Liverpool, due to be completed by the end of 2021.[10] Furthermore, the Department of Infrastructure, Transport, Regional Development and Communications and Mid-Western Regional Council NSW formed a partnership on a Smart Water Meter (SMW) project, which they

[8] Australian Energy Regulator (2021). *Smart Meters*. Retrieved from https://www.aer.gov.au/consumers/my-energy-service/smart-meters

[9] Standards Australia (2021). *Standards Catalogue: EL-011 Electricity Metering Equipment*. Retrieved from https://www.standards.org.au/standards-catalogue/sa-snz/electrotechnology/el-011

[10] Sydney Water (2021). *Digital Meters*. Retrieved from https://www.sydneywater.com.au/SW/accounts-billing/reading-your-meter/about-your-meter/digital-meters/index.htm

recently completed in June 2021, to identify opportunities to save water through early leak detection and water usage.[11] These initiatives are likely to require a review of existing plumbing standards to incorporate new technical requirements. Currently, Sydney Water has guides on water meter installation such as the Multi-level individual metering guide, which incorporates the plumbing standard series AS/NZS 3500 *Plumbing & Drainage*.[12] They are currently working with industry and suppliers to design a data sharing system to meet regulatory requirements and customer needs for the collection of data from digital water meters.

4.7 Use Case 3: Multi-function poles

The humble electric street light pole has evolved since its inception in the 1800's to provide street lighting. Today, there are around 320 million street lights around the world. The street lighting market has been boosted with changes in technology and regulatory policies encouraging energy efficiencies, the convergence of Internet of Things (IoT), a drop in LED prices and the emergence of 'smart poles' or multi-function poles. These multi-function poles allow cities and communities to repurpose a street light pole to a range of functionality, from basic LED replacement with remote control capability to improve energy efficiency, to the more sophisticated level of traffic monitoring, CCTV and Wi-Fi connection.[13]

As a strategic public infrastructure asset, a multi-function pole provides significant cost saving opportunities for asset owners. However, despite its potential, large scale deployments have been limited in many countries. This has been partly due to the limited demand and financial constraints faced by public administrators.[14]

In Australia, multi-function poles have been deployed in some local council areas including the City of Sydney, Geelong, and the City of Newcastle. In the City of Sydney, the multi-function poles were deployed in the Sydney Royal Botanic Gardens and the Domain to provide visitors with free internet connection through its Wi-Fi capability with the integration of Optus small cells. The integration of the small cells also provided the added benefit of minimising the visual impact on the street landscape.[15] The opportunity to integrate the small cells with multi-function poles will drive the growth of the multi-function pole as it will become an attractive option for telecommunications providers like Optus and Telstra looking to deploy their 5G network. With the 5G market expected to reach 1 billion subscribers globally by 2024, network providers like Optus and Telstra will need to build new 5G small cells to keep up with demand. The multi-function pole is seen as the most convenient solution to host 5G small cells as it meets the densification requirement while minimising the visual impacts for cities and communities.[16]

4.7.1 City of Sydney - from standards to technical specifications

When it comes to designing and installing a multi-function pole, the most relevant standard is the AS/NZ 1158 series which includes AS/NZS 1158.1.2:2010 *Lighting for roads and public spaces Vehicular traffic (Category V) lighting - Guide to design, installation, operation and maintenance*. This standard is referenced in the City of Sydney's Lights Public Domain Design Code, providing technical guidance for the installation, operation and maintenance of public lighting.

---

[11] Department of Infrastructure, Transport, Regional Development and Communication (2021). *Smart Water Meters*. Retrieved from https://www.infrastructure.gov.au/cities/smart-cities/collaboration-platform/smart-water-meters.aspx

[12] Sydney Water (2020). *Multi-level individual metering guide*. Retrieved from https://www.sydneywater.com.au/web/groups/publicwebcontent/documents/document/zgrf/mdc0/~edisp/dd_074401.pdf

[13] Arthur D Little (2019). *The evolution of the street lighting market*. Retrieved from https://www.adlittle.com/en/insights/report/evolution-street-lighting-market

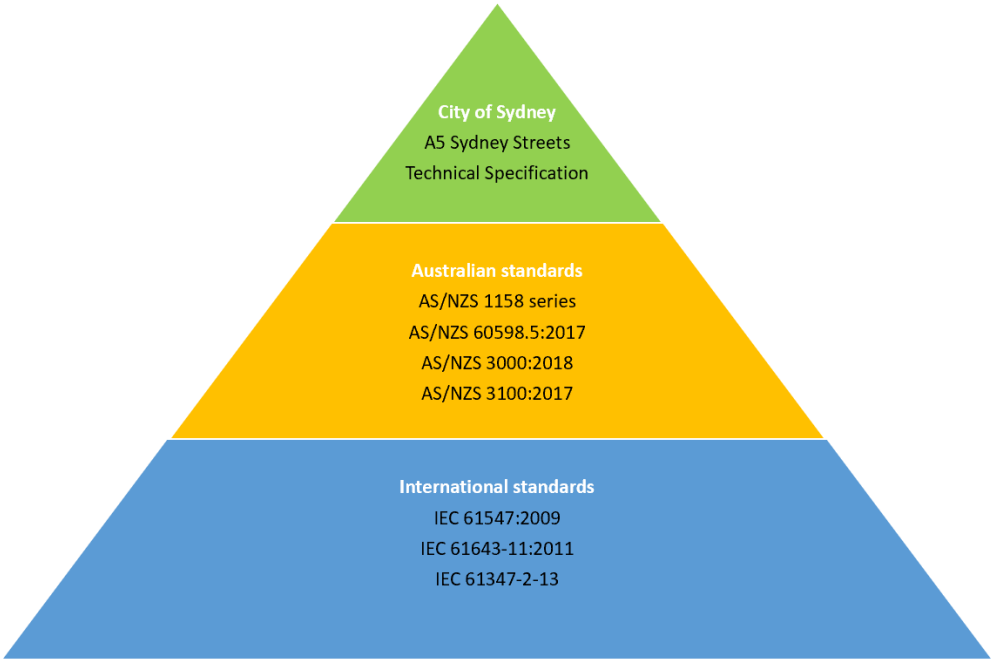
[14] Arthur D Little (2019). *The evolution of the street lighting market*. Retrieved from https://www.adlittle.com/en/insights/report/evolution-street-lighting-market

[15] ENE.Hub (2020). *Optus and partner deliver free internet – and also visitor monitoring.* Retrieved from https://ene-hub.com/smart-poles-come-to-sydneys-domain-and-botanic-garden/

[16] Arthur D Little (2019). *The evolution of the street lighting market*. Retrieved from https://www.adlittle.com/en/insights/report/evolution-street-lighting-market

Furthermore, the City of Sydney has published a Technical Specification to incorporate the requirements of a "smart pole", based on the foundations of international and Australian Standards as outlined in the Sydney Streets Technical Specification A5 Street Lighting Design.[17] The Technical Specification is designed to provide a consistent approach to the design, construction and operation of the council's physical infrastructure including public lighting and 'smart poles' or multi-function poles.

The below diagram provides an overview of the hierarchy of technical standards relevant to multi-function poles. For a complete list of technical standards, refer to the Sydney Streets Technical Specification A5 Street Lighting Design, pages 64 and 65.



4.7.2 Digital Infrastructure Technical Report - Western Parkland City

When planning future data and connectivity requirements, place owners may refer to the recently published Digital Infrastructure Technical Report for Western Parkland City, which provides technical guidance for the planning, design and construction of 'in ground' telecommunications and smart infrastructure within the Western Parkland City precinct.[18] While the report is specifically designed for the Western Parkland City precinct, it is a useful technical guide for considering the telecommunications and smart infrastructure requirements of a city or community. The report sets out the telecommunication network elements and minimum dimensions to support planners considering the 'digital plumbing' requirements of a city or community. This will ensure the longer-term data and connectivity needs are factored at the planning and design stage, to minimise the need for costly site excavations in the future. The technical requirements were developed from a set of Australian telecommunications standards, handbooks, and industry guidance. Also included in the report is a general recommendation on the installation of 'Smart pole Type 1'

[17] City of Sydney (2019). *Sydney Streets Technical Specifications*. Pages 61-100. Retrieved from https://www.cityofsydney.nsw.gov.au/design-codes-technical-specifications/sydney-streets

[18] NSW Department of Planning, Industry and Environment (2021). *Digital infrastructure technical report: Western Parkland City*. Retrieved from https://www.planning.nsw.gov.au/-/media/Files/DPE/Reports/DOC21-94178--Western-Parkland-CityDigi-Infrastructure-Technical-Report-2020120221.pdf

(full capability) for pole bases or mounts. However, the report notes that further industry consultation is required to develop technical specifications for the installation, maintenance and upgrades of 'smart poles'.

4.8 Data management and standards

Data quality and management were identified as critical to the adoption of smart place initiatives by the Standards Australia Smart Cities Standards Reference Group.[19] The Reference Group also noted that data generated by different devices and systems with undefined proprietary features would make data accessibility and interoperability extremely difficult. As a result, the Reference Group published a list of recommendations including the need to establish minimum data standards to support data compatibility and interoperability. Furthermore, it recommended Australia establish foundational data labelling, storage, and quality requirements as this was an important step in enabling future data use and analytics. While Australia has been inactive in the development of international standards for data management, steps have been taken by the Commonwealth in mid-2020 to rejoin the international committee JTC 1/SC 32 Data Management and interchange, chaired by the United States' standards body, ANSI. Some of the published standards that are relevant for owners of data repositories include the technical standard ISO/IEC 11179 series for metadata registries (MDR) or metadata repositories, which addresses the formulation of data definitions and naming conventions.

At the state level, the NSW Government developed the NSW Infrastructure Data Management Framework (IDMF) to provide guidance on the management of data generated and used during the lifecycle of infrastructure.[20] Within this framework, both international and Australian standards are referenced to provide detailed technical guidance on the format and structure of metadata including ISO/IEC 11179 *Metadata registries*, AS/NZS ISO 15836:2016 *Information and documentation* and AS/NZS ISO 19115:2015 *Geographic information - Metadata, Part 1: Fundamentals.*

Additionally, the NSW Government's Data & Information Custodian Policy encourages the use of standards to manage metadata, store and archive data. Such policies can be supported by referencing the relevant technical standards to provide further guidance on how this can be achieved. Other international technical standards which are relevant to the design and structure of data include:

- ISO/IEC 30182:2017 *Guidance for establishing a model for data interoperability.* Provides guidance on a smart city concept model (SCCM) and the basis of interoperability between component systems of a smart city, by aligning the ontologies in use across different sectors.

- ISO/IEC 29161:2016 *Information technology — Data structure — Unique identification for the Internet of Things.*

- ISO/IEC 19763-1:2015 *Information technology — Metamodel framework for interoperability (MFI) — Part 1: Framework.*

Data management is also relevant to the procurement of Internet of Things (IoT) solutions, where ownership and access of data generated and collected by IoT solutions need to be clearly defined. Standards like ISO/IEC 27002:2013 *Code of practice for information security controls* and ISO/IEC 30161:2020 *Requirements of IoT data exchange platform for various IoT services* can be used to complement the NSW Government's IoT Policy Guidance.

[19] Standards Australia (2020). *Smart Cities Standards Roadmap*. Retrieved from https://www.standards.org.au/getmedia/bfe42f98-011e-4798-8fa5-5b70c8a2a6bd/SA_Smart_Cities_Roadmap.pdf.aspx

[20] NSW Government (2021). *NSW Infrastructure Data Management Framework*. Retrieved from https://data.nsw.gov.au/blog/nsw-infrastructure-data-management-framework

5 BEING CYBER SECURE AND PROTECTING PRIVACY: INFORMATION SECURITY AND PRIVACY MANAGEMENT

5.1 Privacy

At the broader level, the international standard for ISO/IEC 27701:2019 *Privacy information management* compliments the ISO/IEC 27000 series on information security management systems, which many organisations are currently audited on each year.[21] The ISO/IEC 27701:2019 is the first Privacy Information Management System (PIMS) standard which enables companies to be certified against, thereby giving companies a distinct advantage over their competitors. The standard requires organisations to consider both the security and privacy risks of managing personal information. It is mapped against the European Union's General Data Protection Regulation (GDPR), helping organisations to meet the regulatory requirements of managing personally identifiable information (PII). It has the potential to be recognised by the European Union as a 'certification mechanism' under GDPR, making it an attractive option for organisations managing cross border data flow.[22]

While each country has their own privacy laws, the standard allows a consistent approach while providing the flexibility for countries like Australia to modify the standard to suit local privacy laws. The standard sets a global approach to privacy to ensure customer's personal information is protected. Additionally, it helps to reconcile the different regulatory requirements and bridges the gap between existing privacy laws. Furthermore, an open source Data Protection Mapping Project has been established to allow the public to view the ISO/IEC 27701 against the relevant privacy legislations, including Australia's Privacy Principles and *Privacy Act 1998* (Cth).[23] The ISO/IEC 27701:2019 is in the process of being modified as an Australian standard, mapped against Australia's Principles and *Privacy Act 1998* (Cth), to provide guidance to organisations on Australia's privacy requirements.

While not yet an international standard, ISO/IEC TS 27570, *Privacy protection – Privacy guidelines for smart cities* is a Technical Specification (TS) providing guidelines and recommendations for privacy protection through the lens of smart cities. There are a range of privacy considerations from the aspect of governance, data management, risk management, engineering, and citizen engagement. The Technical Specification (TS) provides guidance on privacy protection within a smart city ecosystem, how standards can be used for the benefit of citizens and processes for smart city privacy protection. It is also the first step towards developing future privacy standards for smart cities such as privacy management plans, policy making, and consent management.[24]

5.2 Information security

There are a range of widely used information security standards in existence internationally. Recognised Standards Development Organisations, such as ISO and IEC, develop some of these, whilst national bodies, such as the National Institute for Standards and Technology (NIST) in the United States, often pioneer new approaches, which can be described as 'good practice.' It is important to note that content developed by NIST, as known vulnerabilities and threats evolve, often later helps shape ISO/IEC revisions to standards, through expert processes. So, these standards are not mutually exclusive and are often used for different purposes (i.e., to achieve an uplift in cyber hygiene in a sector or area, vs. achieving certification across a large entity, and at a range of levels).

[21] ISOFocus (2020). *How Microsoft makes your data its priority*. Retrieved from https://www.iso.org/news/ref2489.html
[22] Siganto, J. (2020). *ISO 27701 Privacy Management System: How useful is it?* Retrieved from https://privacy108.com.au/insights/iso-27701/
[23] GitHub (2020). *Data Protection Mapping Project.* Retrieved from https://dataprotectionmapping.z21.web.core.windows.net/#/dashboard
[24] ISO News (2021). *Protecting our privacy in smart cities*. Retrieved from https://www.iso.org/news/ref2631.html

Within information security, ISO/IEC 27001 *Information Security Management Systems - Requirements* is a widely known standard in the family of ISO/IEC 27000 series, providing an Information Security Management System (ISM) to assist organisations that manage the security of information assets such as financial information, employee details or intellectual property. The standard provides a model on how to set up and operate a management system, and for which organisations can demonstrate conformance through an audit and certification process.

As noted previously, standards like ISO/IEC 27001 can be used in the NSW Government's ICT procurement process to drive behaviour change and create greater levels of quality assurance with suppliers. The NSW Government's Cyber Security Strategy, released in 2021, calls for agencies to adopt best practice for cyber security. Government agencies and local councils may consider including ISO/IEC 27001 in the Expression of Interest (EOI) or other tender-related processes, by asking suppliers to verify that they adopt and/or comply with ISO/IEC 27001. This enables a company to demonstrate, in a transparent way, their capabilities and provides baseline confidence to the buyer about the underlying security of their smart-places related technology. Companies might then also demonstrate additional cyber security capabilities.

Another common approach cited is the Australian Signals Directorate (ASD) 'Essential Eight.' These are a set of practices that leverage common information security guidance internationally and are applicable across entities. It is important to note that the Essential Eight does not have a certification process that entities/organisations can attest to, and uptake is variable across Australia, including within the Australian Public Service. Anyone wishing to mandate the Essential Eight is advised to consult existing suppliers/partners to establish the degree of conformance. You might want to examine whether international standards, and related security controls companies adopt, might either meet or exceed these requirements, in addition to providing additional assurance in other areas.

Checklist:

For your smart places project, or program activity, have you:

- Undertaken a privacy impact assessment?
    - If so, have you implemented responses to any risks identified, including through using any recognised international standards that might be relevant to implement a comprehensive response?
- Determined whether information security standards are required to manage any identified security risks?
    - If so, have you differentiated between companywide policies, and requirements you consider important for specific sites and products by consulting the broader suite of standards (i.e., multi-functional poles, IoT devices etc.)?

6 APPENDIX A – SMART METER (ELECTRICITY) STANDARDS

Designation	Title
AS 1284.10.2-2006	Electricity metering, Part 10.2: Data exchange for meter reading, tariff and load control - Direct local data exchange via hand-held unit (HHU) - ANSI Standard interface
AS 1284.10.2-2006 Rec:2016	Electricity metering - Part 10.2: Data exchange for meter reading, tariff and load control - Direct local data exchange via hand-held unit (HHU) - ANSI Standard interface
AS 1284.11-1995	Electricity metering, Part 11: Single-phase multifunction watthour meters
AS 1284.11-1995 REC:2019	Electricity metering, Part 11: Single-phase multifunction watthour meters
AS 1284.1-2004 REC:2019	Electricity metering, Part 1: General purpose induction watt hour meters
AS 1284.12-1995	Electricity metering, Part 12: Polyphase multifunction (non-demand) watthour meters (Class 1)
AS 1284.12-1995 REC:2019	Electricity metering, Part 12: Polyphase multifunction (non-demand) watthour meters (Class 1)
AS 1284.4-2006	Electricity metering, Part 4: Socket mounting system
AS 1284.4-2006 Rec:2016	Electricity metering - Part 4: Socket mounting system
AS 62052.11:2018	Electricity metering equipment (ac) - General requirements, tests and test conditions, Part 11: Metering equipment (IEC 62052-11:2016 (ED.1.1) MOD)
AS 62052.21:2018	Electricity metering equipment (ac) - General requirements, tests and test conditions, Part 21: Tariff and load control equipment (IEC 62052-21:2016 (ED.1.1) MOD)
AS 62052.31:2017	Electricity metering equipment (AC) - General requirements, tests and test conditions, Part 31: Product safety requirements and tests (IEC 62052-31:2015 (ED.1.0) MOD)
AS 62052.31:2017 Amd 1:2021	Electricity metering equipment (AC) - General requirements, tests and test conditions, Part 31: Product safety requirements and tests (IEC 62052-31:2015 (ED.1.0) MOD)

AS 62053.21:2018	Electricity metering equipment (ac) - Particular requirements, Part 21: Static meters for active energy (classes 1 and 2) (IEC 62053-21:2016 (ED.1.1) MOD)
AS 62053.22:2018	Electricity metering equipment (ac) - Particular requirements, Part 22: Static meters for active energy (classes 0.2 S and 0.5 S) (IEC 62053-22:2016 (ED. 1.1) MOD)
AS 62053.23:2018	Electricity metering equipment (ac) - Particular requirements, Part 23: Static meters for reactive energy (classes 2 and 3) (IEC 62053-23:2016 (ED.1.1) MOD)
AS 62053.24:2018	Electricity metering equipment (ac) - Particular requirements, Part 24: Static meters for reactive energy at fundamental frequency (classes 0.5 S, 1 S and 1) (IEC 62053-24:2016 (ED.1.1) (MOD)
AS 62053.61:2018	Electricity metering equipment (a.c.) - Particular requirements, Part 61: Power consumption and voltage requirements (IEC 62053-61:1998, MOD)
AS 62054.11:2018	Electricity metering equipment (a.c.) - Tariff and load control, Part 11: Particular requirements for electronic ripple control receivers (IEC 62054-11:2004 (ED.1.1), MOD)
AS 62054.21:2018	Electricity metering (AC) - Tariff and load control, Part 21: Particular requirements for time switches (IEC 62054-21:2017 (ED.1.1), MOD)
AS 62056.21-2006	Electricity metering - Data exchange for meter reading, tariff and load control - Direct local data exchange
AS 62056.21-2006 Rec:2016	Electricity metering - Data exchange for meter reading, tariff and load control - Part 21: Direct local data exchange
AS IEC 62053.31:2018	Electricity metering equipment (a.c.) - Particular requirements, Part 31: Pulse output devices for electromechanical and electronic meters (two wires only)
AS/NZS 1284.13:2002	Electricity metering, Part 13: In-service compliance testing
AS/NZS 1284.13:2002 Rec:2016	Electricity metering - Part 13: In-service compliance testing

7 APPENDIX B – RISK MANAGEMENT PLAN - ILLUSTRATIVE GUIDE

The following is an exemplar of what a risk management plan, maintained by your Board, or Executive, might look like. Refer to the more detailed guidance material within this document, and ISO 31000, as you refine and populate this. You might also want to draw on the detailed qualitative and quantitative techniques for risk management outlined in AS ISO 31010:2020 (Risk management – Risk Assessment Techniques).

a) An example: Risk Register

NAME OF ORGANISATION:

RESPONSIBLE PERSON/OFFICER & TITLE:

DATE OF APPROVAL [i.e. by Board, or Executive]:

DATE OF REVISION: [Should be formally within 12 months, & a standing item on each agenda]

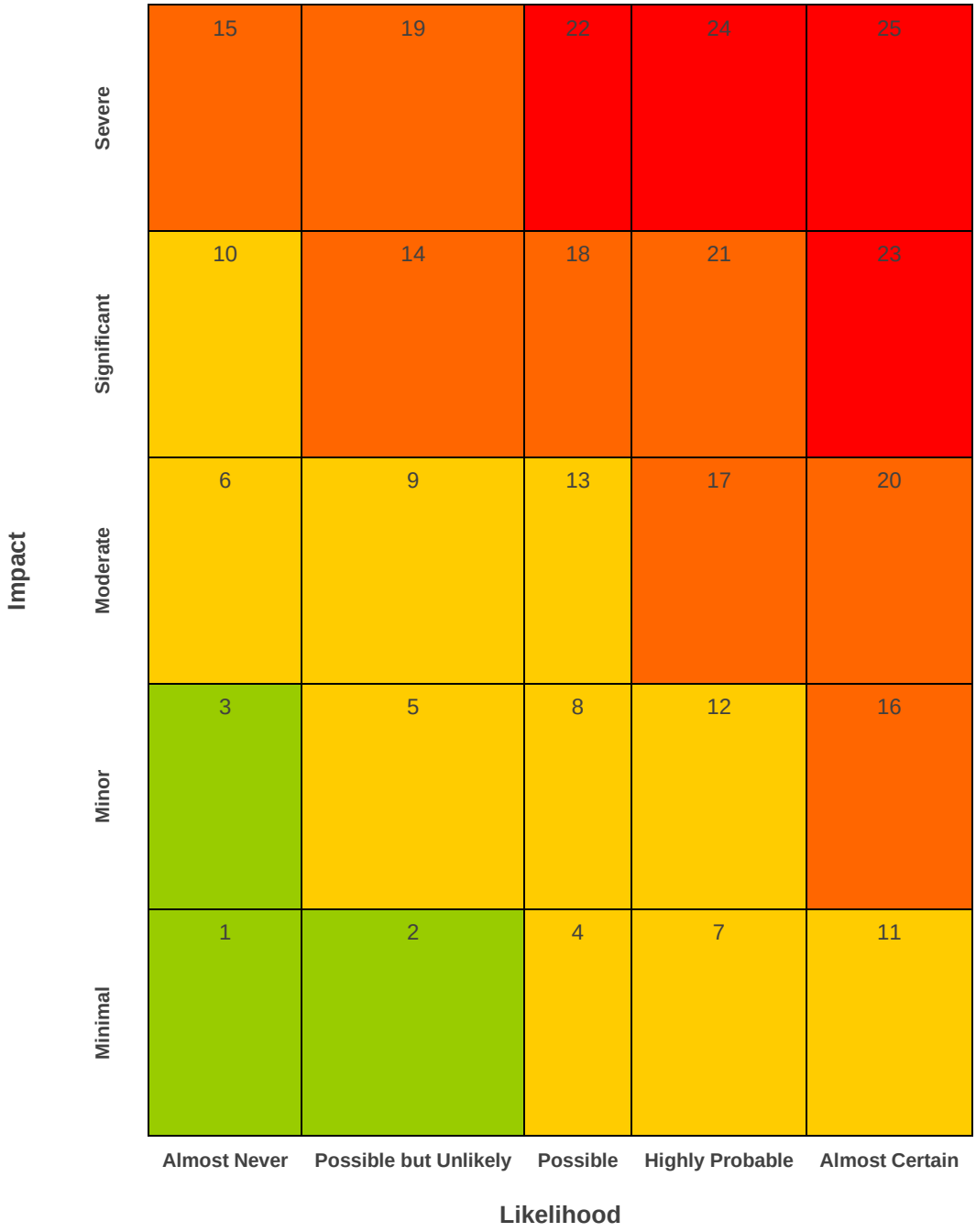
Risk domain	Likelihood	Impact	Mitigation strategies
LEGAL 1. Poor supply chain management, resulting in exposure to penalties associated with modern slavery legislation	Possible	Significant	a. Maintain a comprehensive contract register, with visibility for Board Members and the Executive b. Through standard contractual clauses, require all providers to attest to responsible supply chain practices and to provide their statement of compliance with modern slavery legislation
FINANCIAL 2. I.e. Grant or program reporting requirements and milestones (if externally funded program).			
REPUTATIONAL 3. I.e. Adequacy of community consultation, trust			

OPERATIONAL 4. I.e. adequate resourcing to deliver on program requirements			
SAFETY & SECURITY 5. I.e. employment screening, information security, protective security, non-discrimination, and anti-harassment policies			

b) An example risk assessment matrix

*You should use this, during the process to develop the above risk management plan. Through the below matrix, you should formally rate each of the risks identified in your initial scoping of risk (your initial list), to enable agreement on both the **likelihood** and **magnitude** of any identified risks amongst those involved in your risk management process.*

*Source **(requires copyright approval):** https://www.digital.govt.nz/dmsdocument/3-risk-assessment-process-information-security/html#appendix-b-–-example-risk-scales-and-matrix*



8 FURTHER READING

DIN (2014). *Standardization in the Smart City*.

European Union (2016). *Analysing the potential for wide scale roll out of integrated Smart Cities and Communities solutions*.

ITU-T (2017).*Implementing ITU-T International Standards to Shape Smart Sustainable Cities: The case of Singapore*.

Joss, S., Cowley, R., de Jong, WM., Muller, B., Soon Park, B., Rees, W., Roseland, M., Rydin, Y. (2015). *Tomorrow's City Today: Prospects for Standardising Sustainable Urban Development*. University of Westminster.

NSW Department of Health (2009). *Healthy Urban Development Checklist: A guide for health services when commenting on development policies, plans and proposals*.

9 REFERENCES

Arthur D Little (2019). *The evolution of the street lighting market*. Retrieved from https://www.adlittle.com/en/insights/report/evolution-street-lighting-market

Australian Energy Regulator (2021). *Smart Meters*. Retrieved from https://www.aer.gov.au/consumers/my-energy-service/smart-meters

City of Sydney (2019). *Sydney Streets Technical Specifications*. Pages 61-100. Retrieved from https://www.cityofsydney.nsw.gov.au/design-codes-technical-specifications/sydney-streets

Department of Infrastructure, Transport, Regional Development and Communication (2021). *Smart Water Meters*. Retrieved from https://www.infrastructure.gov.au/cities/smart-cities/collaboration-platform/smart-water-meters.aspx

ENE.Hub (2020). *Optus and partner deliver free internet – and also visitor monitoring.* Retrieved from https://ene-hub.com/smart-poles-come-to-sydneys-domain-and-botanic-garden/

GitHub (2020). *Data Protection Mapping Project.* Retrieved from https://dataprotectionmapping.z21.web.core.windows.net/#/dashboard

ICSM (2020). *Geocentric Datum of Australia 2020*. Retrieved from https://www.icsm.gov.au/gda2020

ISO (2016). *ISO 37101 Sustainable Development in Communities*. Retrieved from https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/iso_37101_sustainable_development_in_communities.pdf

ISO (2021). *ISO 37155-1:2020 Framework for integration and operation of smart community infrastructures — Part 1: Recommendations for considering opportunities and challenges from interactions in smart community infrastructures from relevant aspects through the life cycle.* Retrieved from https://www.iso.org/obp/ui/#iso:std:iso:37155:-1:ed-1:v1:en

ISO (2021). *ISO/IEC TS 27570:2021 Privacy protection — Privacy guidelines for smart cities.* Retrieved from *https://www.iso.org/standard/71678.html*

ISO (2021). *Management System Standards*. Retrieved from https://www.iso.org/management-system-standards.html

ISO (2021). *Standards in our world*. Retrieved from https://www.iso.org/sites/ConsumersStandards/1_standards.html

ISOFocus (2020). *How Microsoft makes your data its priority*. Retrieved from https://www.iso.org/news/ref2489.html

ISO News (2021). *Protecting our privacy in smart cities*. Retrieved from https://www.iso.org/news/ref2631.html

ITU (2021). *Smart Sustainable Cities*. Retrieved from https://www.itu.int/en/publications/Documents/tsb/2021-ITU-Smart-Sustainable-Cities/index.html#p=1

NSW Government (2021). *NSW Infrastructure Data Management Framework*. Retrieved from https://data.nsw.gov.au/blog/nsw-infrastructure-data-management-framework

NSW Government (2019). *Smart Infrastructure Policy*. Retrieved from https://www.digital.nsw.gov.au/policy/smart-infrastructure-policy

NSW Department of Planning, Industry and Environment (2021). *Digital infrastructure technical report: Western Parkland City.* Retrieved from https://www.planning.nsw.gov.au/-/media/Files/DPE/Reports/DOC21-94178--Western-Parkland-CityDigi-Infrastructure-Technical-Report-2020120221.pdf

Siganto, J. (2020). *ISO 27701 Privacy Management System: How useful is it?* Retrieved from https://privacy108.com.au/insights/iso-27701/

Standards Australia (2021). *Standards Catalogue: EL-011 Electricity Metering Equipment*. Retrieved from https://www.standards.org.au/standards-catalogue/sa-snz/electrotechnology/el-011

Standards Australia (2020). *Smart Cities Standards Roadmap*. Retrieved from https://www.standards.org.au/getmedia/bfe42f98-011e-4798-8fa5-5b70c8a2a6bd/SA_Smart_Cities_Roadmap.pdf.aspx

Sydney Water (2021). *Digital Meters*. Retrieved from https://www.sydneywater.com.au/SW/accounts-billing/reading-your-meter/about-your-meter/digital-meters/index.htm

Sydney Water (2020). Multi-level individual metering guide*. Retrieved from* https://www.sydneywater.com.au/web/groups/publicwebcontent/documents/document/zgrf/mdc0/~edisp/dd_074401.pdf