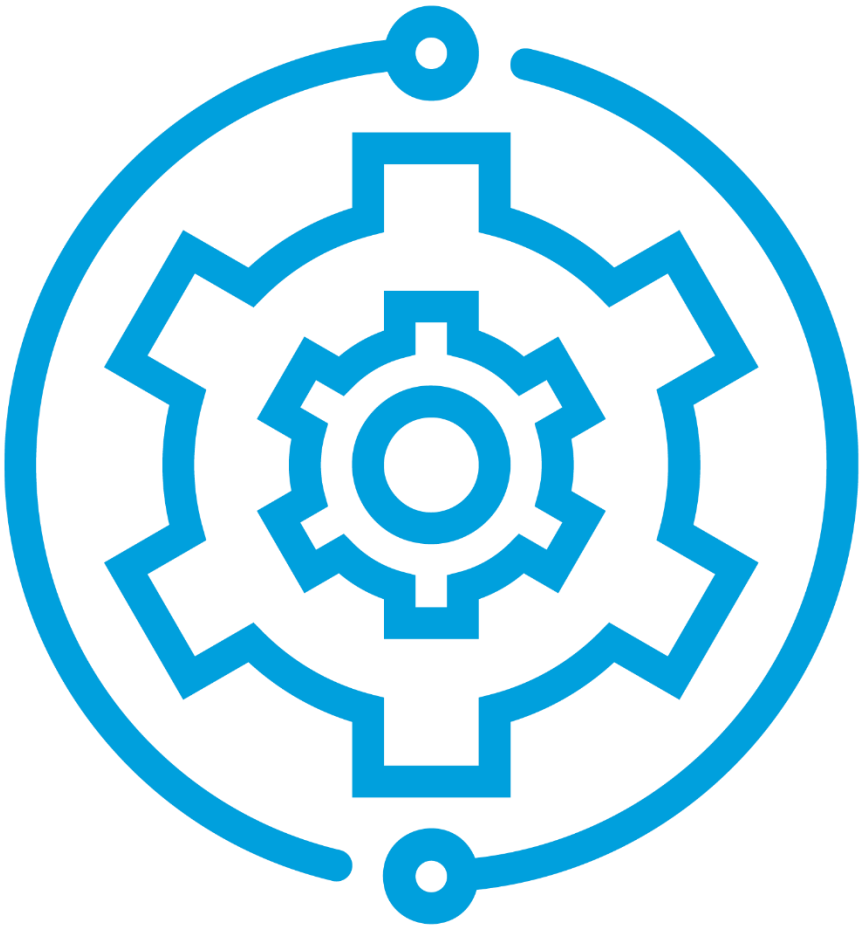
OPENAIR

Operational Network of
Air quality Impact Resources

Best Practice Guide

BP307 | Implement and operate

Cybersecurity for smart air quality monitoring networks



Introduction

Cybersecurity is an important concern that must be addressed to ensure the secure, reliable operation of low-cost air quality monitoring sensors, networks, and applications. It requires a holistic approach that involves people, processes, and technologies.

Cybersecurity technologies include secure identity management, authentication, authorisation, access, encryption, and monitoring. These are used to protect low-cost sensing systems from security threats (such as data flow interruptions, tampering, and denial of service attacks).

Cybersecurity practices for low-cost sensing networks address device security, network security, data security, incident response, and compliance.

Air quality data is generally not considered critical or sensitive when compared to other types of personal or operational data. For this reason, air quality monitoring networks usually consist of low-cost Internet of Things (IoT) sensors (often deployed in public spaces) that use a variety of wired and wireless data communications networks.

However, an air quality monitoring IoT system can still be exposed to certain types of risks that may impact the system's availability, integrity, and data security, including:

- **confidentiality risks** – unauthorised access to the system or data, eavesdropping on communications, or data breaches that can expose sensitive information
- **integrity risks** – tampering with sensor data, unauthorised changes to the system configuration, or software bugs that can compromise the integrity of the data or system
- **availability risks** – denial of service, malware infections, or hardware failures that disrupt the availability of the system.

It is important for local governments in charge of an air quality monitoring sensor network to take cybersecurity seriously, and to implement appropriate security measures to protect against these risks. The potential consequences of a security breach can be serious. For example, unauthorised access to the network could result in the theft or manipulation of data, the disruption of system operations, or unauthorised access to other connected systems (containing personal or operational information).

Who is this resource for?

This resource provides information about the cybersecurity implementation process, and a practical cybersecurity checklist. It is designed to assist project leads or members of local government smart city projects or programs. It is also a practical tool for anybody responsible for the cybersecurity of an IoT project, including:

- **IoT network administrators** who manage and maintain low-cost sensing and air quality monitoring networks
- **Researchers** who use low-cost sensing and air quality monitoring networks to collect and analyse environmental data

- **Policymakers** responsible for regulating the use of low-cost sensing and air quality monitoring networks, and promoting cybersecurity best practices.

How to use this resource

This document can be used as a starting point for local governments trying to understand the cybersecurity needs of their air quality monitoring systems. It is organised into two sections:

1. An overview of the cybersecurity implementation process
2. A cybersecurity checklist.

Cybersecurity implementation process

The cybersecurity implementation process described here is adapted from the Australian Government's Protective Security Policy Framework (PSPF).

The PSPF is a set of guidelines and best practices for Australian organisations to protect their staff, information, and assets from security risks and threats (both domestically and overseas). The PSPF is designed to help organisations meet their legal and regulatory obligations for protecting sensitive information and assets. It is a key resource guiding cybersecurity implementation in Australian Government agencies.

The PSPF can be applied by using a **security risk management approach**, and working through the **practical cybersecurity checklist** (for risk assessment), as outlined in Figure 1.

The PSPF framework consists of seven components organised into four categories: (1) governance, (2) people, (3) physical and technological security, and (4) information security management.

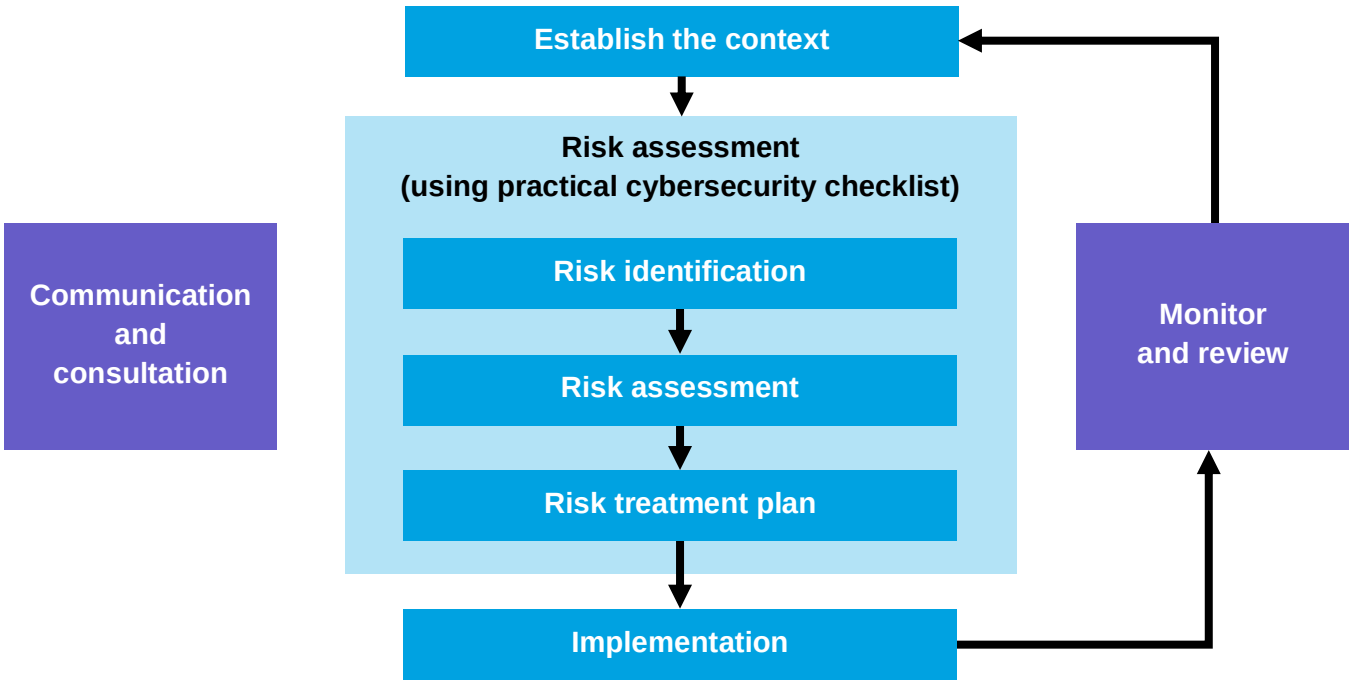


Figure 1: The PSPF risk assessment framework

Each stage of this cybersecurity risk assessment process is described in more detail in Table 1.

Table 1: Stages in PSPF risk assessment framework

Stage	Description
1. Communication and consultation	This stage involves engaging with stakeholders and relevant parties to identify and assess security risks. This may include identifying assets that need to be protected, potential threats to those assets, and the impacts of a security breach.
2. Establish the context	This stage is about understanding the organisation's mission, objectives, and the environment in which it operates. It also includes clarifying the organisation's legal, regulatory, and policy requirements and obligations. A concrete scenario is a local government project with the mission of improving air quality monitoring, and providing reliable data to stakeholders (including community organisations and researchers) to promote public health. Understanding this wider context can help the project team to identify specific risks, and to ensure that the risk management process is aligned with their organisation's objectives.
3. Risk identification	This stage involves identifying all potential security risks to assets, including internal and external threats, vulnerabilities, and consequences. The practical cybersecurity checklist can be used to conduct the risk identification process.

Stage	Description
4. Risk assessment	This stage involves evaluating the likelihood and impact of identified risks, and determining the overall risk level.
5. Risk treatment plan	This stage involves deciding how to manage the risks identified in the previous stages. This can include planning controls to mitigate or eliminate risks, transferring risks through insurance, or accepting the risks.
6. Implementation	This stage involves putting the risk treatment plan into action. This can include purchasing and installing security IoT devices for the system, developing policies and procedures, or providing training to employees.
7. Monitor and review	This stage involves monitoring the effectiveness of the risk treatment plan, and regularly reviewing the security risks and controls. It also involves continuously improving the security posture of the organisation by incorporating feedback and lessons learned.

This framework provides some high-level guidance to identify and manage security risks related to secure air quality monitoring. However, local governments should also consider modifying and tailoring their own internal security frameworks to apply to secure air quality monitoring.

Cybersecurity checklist

The cybersecurity checklist (in Table 2) identifies unique aspects of IoT systems that should be considered when assessing your network's security risks.

It is structured to reflect the 'layers' in the Internet of Things Alliance Australia (IoTAA) reference architecture. Please also see the OPENAIR Best Practice Guide chapter *IoT reference architecture for smart air quality monitoring.*

This checklist notes key security principles and supporting practices, mapped according to IoT reference architecture layers. It is not an exhaustive checklist, but a general guide. Local governments should identify their own specific security and compliance requirements, based on their context.

Table 2: Practical cybersecurity checklist

Layer	Security principles	Checklist items to consider
IoT industry and solution	Specify the security and compliance requirements for given industry sectors	☐ Identify the specific industry segment or domain (e.g. environmental quality or health) that the IoT solution is targeted towards. ☐ Understand the cybersecurity implications and challenges specific to the industry segment, including regulatory requirements, data privacy concerns, and supply chain risks. ☐ Ensure compliance with relevant industry standards and regulations (such as the Australian Privacy Act 1988). ☐ Implement appropriate cybersecurity controls and practices based on the unique characteristics of the industry segment, and the specific IoT solution being developed.
Solution / service provider	Consider cybersecurity and privacy management for all stakeholders	☐ Identify all stakeholders (local governments, health authorities, local community groups, researchers, etc.) involved in the IoT solution, including the solution owner/operator (whether business, enterprise, or government) and service provider. Clearly define the roles and responsibilities of each stakeholder in the IoT solution. ☐ Develop and enforce policies and procedures to ensure compliance with applicable regulations and standards, such as data protection laws and cybersecurity frameworks. ☐ Conduct regular risk assessments to identify potential threats and vulnerabilities to the IoT solution, and implement appropriate mitigation measures. ☐ Establish a process for incident management and response, including reporting and resolution procedures for security incidents and breaches. ☐ Regularly review and update the IoT solution to ensure it continues to meet the needs and expectations of all stakeholders.
IoT users	Ensure IoT user security for both primary users (IoT solution owners) and secondary users (e.g. those who operate and manage the solution)	☐ Conduct regular training and awareness programs for primary and secondary users to understand cybersecurity risks and best practices. ☐ Enforce strong password policies and multi-factor authentication for user accounts. ☐ Establish access controls and permissions to limit user access to only what they need to perform their job responsibilities.

Layer	Security principles	Checklist items to consider
		☐ Encourage users to report any security incidents or potential vulnerabilities to the IT team. ☐ Have a plan in place for responding to security incidents, including incident reporting and response, investigation, and recovery.
IoT user interface	Ensure the security of user interfaces and IoT client devices (including desktops/laptops, tablets, smartphones, wearables, or purpose-made devices)	☐ Implement secure communication protocols (such as SSL/TLS) to encrypt the communication between the user interface and the IoT system. ☐ Regularly update and patch the user interface software to address known security vulnerabilities. ☐ Implement secure password policies to ensure that users choose strong passwords and change them regularly. ☐ Provide clear and concise security and privacy policies to users, and ensure they are informed of any changes to these policies.
Application enablement	Ensure the security of applications, web portals, and API enablers	☐ Implement strong authentication measures for users accessing the web portal or any applications built on the platform. ☐ Implement access controls to limit access to specific functions and services, based on user roles and permissions. ☐ Implement secure coding practices for any custom code developed for web or mobile applications, API enablers, or developer services. ☐ Regularly update and patch any third-party software or libraries used in the development of web or mobile applications. ☐ Implement measures to protect against common web application attacks, such as SQL injection and cross-site scripting (XSS).
Intelligence enablement	Ensure security for data at rest and in transit, and ensure compliance with governance policy	☐ Implement data encryption for all data at rest and in transit. ☐ Implement access controls for data platforms and analytics platforms. ☐ Implement data governance policies to ensure compliance with applicable regulations and standards. ☐ Regularly monitor data sharing activities, and ensure that only necessary and authorised data is being shared. ☐ Regularly monitor and update third-party data APIs for any security vulnerabilities or issues. ☐ Implement secure coding practices for any custom code developed for analytics or machine learning algorithms.

Layer	Security principles	Checklist items to consider
Connection management	Ensure secure management of networks, protocols, devices, gateways, ID, and user authentication	☐ Implement secure network and protocol management practices. Regularly monitor and update network and protocol settings to ensure they are secure and up-to-date. ☐ Implement secure device and gateway management practices. Regularly monitor and log device and gateway activity to detect and respond to security incidents. ☐ Use strong authentication mechanisms (such as multi-factor authentication and digital certificates) to authenticate both users and IoT devices.
Connectivity	Ensure communication security	☐ Use secure communication protocols (such as HTTPS, SSL/TLS, and SSH) to ensure confidentiality, integrity, and authenticity of data in transit. Make sure the adopted air quality monitoring network standards (e.g. LoRaWAN, NB-IoT, 3G, Sigfox, or Wi-Fi) support these secure communication protocols, and are correctly configured. ☐ Implement end-to-end encryption for sensitive data (e.g. location) transmitted over the network. ☐ Securely store and manage keys and certificates used for encryption and authentication. ☐ Segment the network to limit exposure and attack surface. ☐ Use strong authentication methods (such as multi-factor authentication and digital certificates) to ensure that only authorised devices can access the network. ☐ Monitor network traffic and device behaviour to detect and respond to security incidents. ☐ Log all remote access (with logs including the date, time, and source of access, at a minimum).
IoT gateway	Ensure network security of the gateway, and implement data security as an edge computing platform	☐ Understand that IoT gateways act as the aggregation point for a group of air quality sensors to co-ordinate their connectivity. ☐ Use secure protocols and standards for communication between the gateway device and other devices or networks. ☐ Ensure that the gateway device is properly segmented from other networks to limit exposure and attack surface. ☐ Implement firewalls and intrusion detection/prevention systems to protect the gateway device and the network from attacks. ☐ Change default passwords on devices. ☐ Keep gateway firmware/software up-to-date.

Layer	Security principles	Checklist items to consider
		☐ Understand that IoT gateways can also act as edge computing devices that perform data storage and analytics. ☐ Use strong encryption to protect sensitive data in transit and at rest. ☐ Implement data backup and recovery mechanisms to ensure data can be recovered in the event of a breach or other incident. ☐ Regularly assess and test the security of the gateway device and its data to identify vulnerabilities and ensure ongoing security.
IoT end point	Ensure physical device security	☐ Implement measures to prevent or detect physical tampering with devices (including air quality sensors and gateway devices), such as a minimum height for device deployment in public spaces (e.g. if being fitted to a wall/building/pole), and regular physical inspections of all devices in the network. ☐ Use tamper-evident seals and locks to prevent unauthorised access to devices. ☐ Properly label and track devices to ensure they are not lost or misplaced. ☐ Disable remote management on the device if not needed. ☐ Change default passwords on devices. ☐ Keep device firmware/software up-to-date. ☐ Define the device's functional lifespan at the time of installation, and securely dispose of devices when they reach end-of-life.

Additional resources

- ***Australian Government Department of Home Affairs | Proactive Security Policy Framework (n.d.)***
- ***IoT Alliance Australia | Internet of things security guideline (2017)***
- ***Data.NSW | Data Policy (2022)***
- ***NSW Government | Internet of Things (IoT) Policy Guidance (2021)***
- ***Digital.NSW | Smart Infrastructure Policy (2020)***

Associated OPENAIR resources

Factsheets

Cybersecurity for smart air quality monitoring networks

This factsheet provides an overview of key cybersecurity considerations for local governments establishing smart low-cost sensor networks and supporting platforms and services.

Best Practice Guide chapters

IoT reference architecture for smart air quality monitoring

This Best Practice Guide chapter introduces the OPENAIR reference architecture for smart air quality monitoring. The reference architecture is a framework that identifies the various components and data flows that make up a complete technical solution for smart air quality monitoring. It is a generic reference that can help local governments to design and implement their own technical solutions.

Further information

For more information about this project, please contact:

Peter Runcie

Project Lead, NSW Smart Sensing Network (NSSN)
Email: peter@natirar.com.au

This Best Practice Guide section is part of a suite of resources designed to support local government action on air quality through the use of smart low-cost sensing technologies. It is the first Australian project of its kind. Visit www.openair.org.au for more information.

OPENAIR is made possible by the NSW Government's Smart Places Acceleration Program.

Document No: 20231107 BP307 Cybersecurity for smart air quality monitoring networks
Version 1