Cybersecurity for air quality monitoring networks

Cybersecurity is an important concern that must be addressed to ensure the secure, reliable operation of low-cost air quality monitoring devices, 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.

This factsheet provides high-level information on Internet of Things (IoT) system risks, the cybersecurity implementation process, and a practical cybersecurity checklist for local governments to use for guiding the secure implementation and operations of low-cost air quality data monitoring. This information is adapted from the Internet of Things Alliance Australia (IoTAA) Security Guidelines and IoT Policy Guidance published by the NSW Government.

The implementation process and checklist described are a starting point from which local governments can add their own specific requirements and constraints.

IoT system risks

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 denial of service, malware infections, or hardware failures that disrupt the availability of the system.

AVAILABILITY RISKS

Denial of service, malware infections, or hardware failures that disrupt the availability of the system.

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

4 Information security management.

THE FRAMEWORK

This framework provides high-level guidance to help identify and manage security risks related to secure air quality monitoring. Local governments should also consider modifying and tailoring their own internal security frameworks and apply them to air quality monitoring and other IoT deployments.

Establish the context

Risk assessment (using practical cybersecurity checklist)

Risk identification

Risk assessment

Risk treatment plan
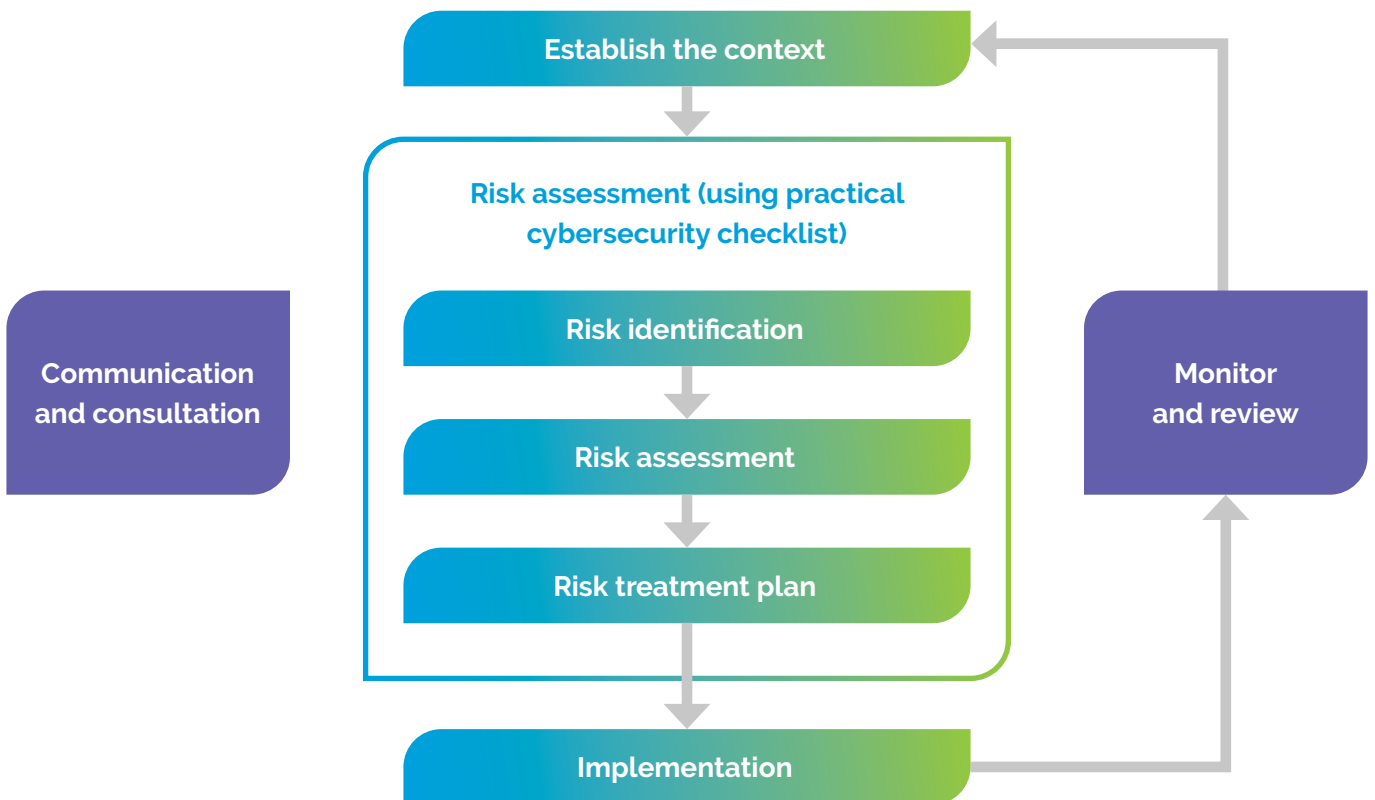
Communication and consultation

Monitor and review

Implementation

Figure 1. The practical cybersecurity checklist for risk assessment

Cybersecurity checklist

The cybersecurity checklist (in **Table 1**) identifies aspects specific to IoT systems that should be considered when assessing your network's security risks.

It is structured to reflect the 'layers' in the IoTAA reference architecture. See the OPENAIR Best Practice Guide chapter *IoT reference architecture for smart air quality monitoring* for a detailed overview.

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 1: Practical cybersecurity checklist.

	Layer	Security Principles
✓	**IoT industry and solution**	Specify the security and compliance requirements for given industry sectors
✓	**Solution/service provider**	Consider cybersecurity and privacy management for 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)
✓	**IoT user interface**	Ensure the security of user interfaces and IoT client devices (including desktops/laptops, tablets, smart phones, wearables, or purpose-made devices)
✓	**Application enablement**	Ensure the security of applications, web portals, and API enablers
✓	**Intelligence enablement**	Ensure security for data at rest and in transit, and ensure compliance with governance policy
✓	**Connection management**	Ensure secure management of networks, protocols, devices, gateways, ID, and user authentication
✓	**Connectivity**	Ensure communication security
✓	**IoT gateway**	Ensure network security of the gateway, and implement data security as an edge computing platform
✓	**IoT end point**	Ensure physical device security

Local governments should identify their own specific security and compliance requirements, based on their context.

Associated OPENAIR resources

The OPENAIR Best Practice Guide chapter *Cybersecurity for smart air quality monitoring networks* provides detailed guidance on this topic. For more information on IoT reference architecture see the Best Practice Guide chapter *IoT reference architecture for smart air quality monitoring*.

Further reading

The following resources provide additional guidance on cybersecurity of IoT systems in the context of NSW Government policy and best practice:

- NSW Government data policies
- NSW IoT Policy Guidance
- IoTAA Security Guideline V1.2 November 2017
- NSW Smart Infrastructure Policy
- Australian Government Proactive Security Policy Framework

FIND OUT MORE AND ACCESS OPENAIR RESOURCES

This factsheet is part of a suite of resources designed to support local government action on air quality through the use of low-cost smart sensing technologies. It is the first Australian project of its kind. Check the project website for resources and updates on post project collaborations: **www.openair.org.au**