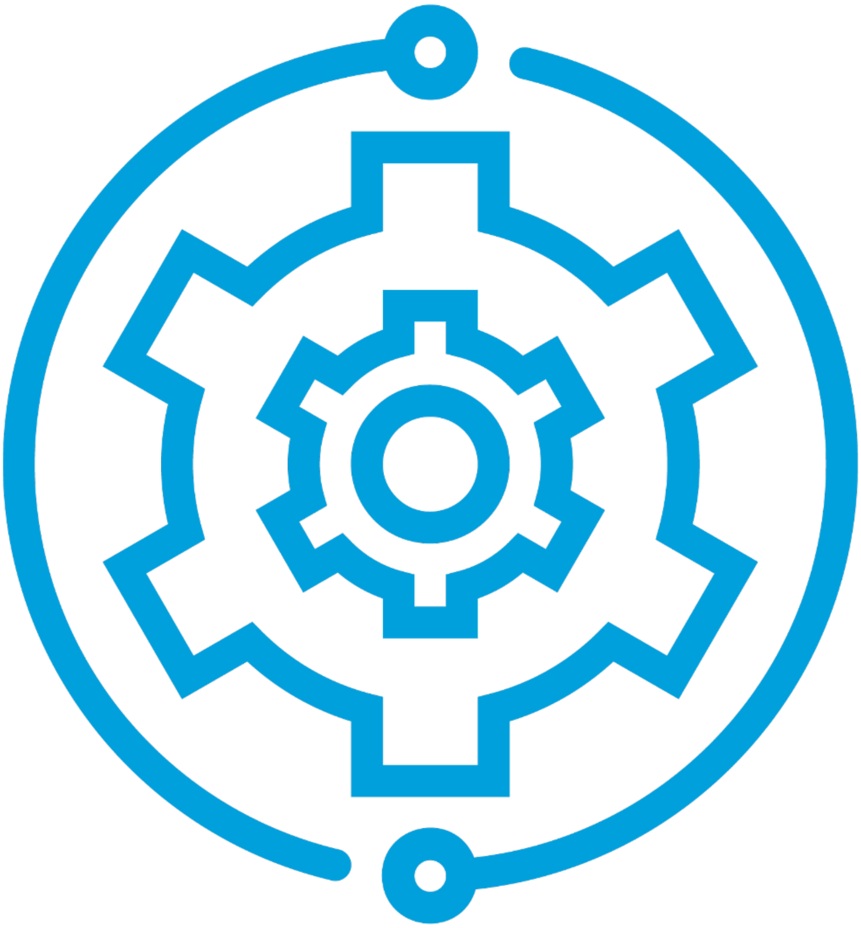
OPENAIR

Operational Network of
Air quality Impact Resources

Best Practice Guide

BP306 | Implement and operate

IoT system operations



Introduction

“IoT”, or the Internet of Things, is the relatively recent connection of physical objects to the internet in order to send information to or from those objects. Although air quality sensors were used before the advent of IoT, people previously needed to visit the devices periodically to manually obtain the data they had collected.

With IoT, sensing devices are connected to the internet so they can send air quality data to a centralised data storage location for access, visualisation and analysis.

An IoT system consists of the sensing devices, data communications networks and various data and other systems needed to manage the devices and ensue data is available to users.

The term ‘IoT system operations’ refers to the process of monitoring, assessing, and maintaining an IoT system, as well as tracking and resolving IoT service issues. Ideally, IoT system operations should be integrated into an organisation's standard procedures and day-to-day operations. IoT-enabled air quality monitoring systems operate continuously, and must be actively managed to ensure they meet business needs.

This document is not intended as a replacement of any existing IT (information technology) operating models and frameworks in your local government organisation. Rather, it highlights IoT-specific considerations for IT managers.

Who is this resource for?

This resource aims to assist people involved in the IoT system operations of a local government organisation. It is also a practical guide for anyone involved in designing, implementing, and using IoT systems for air quality monitoring projects using low cost sensing devices, including:

- IT architects
- IT operations managers
- IT procurement managers
- IoT system users.

How to use this resource

This OPENAIR Best Practice Guide chapter provides a broad overview of IoT system operations. It highlights issues local governments should consider when defining their IoT operational requirements, tools, and processes.

The first section describes key foundational concepts that apply to most IT systems, and considerations specific to IoT systems. Subsequent sections provide more detail on device management, data communications, IoT platforms, data storage, security, and data sharing. The final section is focused on ways to minimise the cost of IoT operations.

System operations concepts

This section describes key foundational concepts that apply to most IT systems, and identifies considerations specific to IoT systems. The following list of concepts is not exhaustive, but is simply a general guide that can be adjusted and expanded, according to your organisation's needs:

- Service Level Agreements (SLAs)
- System availability
- Insourced vs outsourced services
- Periodic audits
- User access management
- User help desk and technical support
- Change management
- Bugs, troubleshooting, and updates.

Service Level Agreements

A Service Level Agreement (SLA) is a contract between an IT service provider and a customer that defines the level of service that the customer can expect from the provider. SLAs typically specify agreed levels of service for system availability, reliability of the service, response times for service requests, and the process for reporting and resolving service outages. SLAs can also include details about penalties for service failures, and service credits for customers (in the event that the provider does not meet the conditions of the service agreement).

In the context of IoT systems, SLAs can be used to define the level of availability and reliability of the system, as well as the process for reporting and resolving system outages. IoT device maintenance (such as periodic cleaning and recalibration of sensors) can also be included in an SLA.

System availability

IoT system availability refers to the ability of an IoT system to function correctly, and provide service to its users. It is usually measured as a percentage of 'uptime' (the amount of time that the system is operational) versus 'downtime' (the amount of time that the system is not operational). High system availability is important for ensuring that IoT systems are reliable, and can meet the needs of their users. Availability requirements (and management procedures) are generally established in SLAs.

Air quality monitoring systems – such as the kind a local government might implement – are mostly considered to be non-critical systems (since they do not, in general, have a direct impact on human health or safety). This means that these systems can afford to have more downtime than a critical system (such as a traffic control system).

Insourced vs outsourced IT services

There are different ways of obtaining the IT (and IoT) services needed to run your organisation (and, in turn, to support your air quality monitoring project). 'Insourcing' refers to using internal resources and employees to provide the relevant services, while 'outsourcing' refers to obtaining these services from an external provider.

Both approaches have pros and cons, as shown in Table 1. Overall, the choice between insourcing and outsourcing will depend on the specific needs of your organisation and your air quality monitoring project, and the resources available.

Table 1. Pros and cons of insourced vs outsourced IT services

	Insourcing	Outsourcing
Pros	• Greater control over the service and the ability to customise it to meet specific needs • Better understanding and knowledge of the service • Greater flexibility in terms of scaling the service up or down, as needed • Better protection of confidential information.	• Lower costs, as external providers may be able to provide the service more efficiently • Access to specialised expertise and resources that may not be available internally • Increased scalability and flexibility, as external providers may be able to adapt more easily to changing needs.
Cons	• Potentially higher costs, if internal resources are more expensive than external providers • Limited expertise and resources, which can lead to less efficient and effective service.	• Loss of control over the service, as it is being provided by an external provider • Dependence on the external provider, which can lead to disruptions if the provider is unable to meet the needs of the customer • Risk of data breaches and other security issues (if sensitive information is being shared with an external provider) • Risk of vendor lock-in, which can make it difficult to switch to a different provider later on.

Periodic audits

Periodic internal and external IT operations audits are an important way to assess the effectiveness and compliance of an organisation's systems, operations, and processes.

Internal audits are conducted by the organisation's own staff, and are primarily focused on evaluating the effectiveness of the organisation's internal controls and processes. They are used to identify any areas of weakness or non-compliance with internal policies, regulations, and standards.

External audits are conducted by independent, third-party auditors, and are primarily focused on evaluating the organisation's compliance with external regulations and standards. External audits can include financial audits, compliance audits, and operational audits.

Periodic internal and external audits can have several benefits, including:

- identifying areas of non-compliance
- identifying opportunities for improvement, which can lead to increased efficiency, cost savings, and better overall performance
- demonstrating to stakeholders and regulators that the organisation is committed to compliance and good governance
- providing an independent and objective assessment of the organisation's operations and processes.

Many organisations choose to conduct annual or bi-annual audits, and alternate between internal and external audits.

User access management

User access management for an IoT system refers to the processes and controls that are put in place to ensure that only authorised users can access and use the system. This can include controls such as user authentication, or role-based access control.

User authentication is the process of verifying the identity of a user before allowing them to access the system. This can be done using usernames and passwords, or with biometric methods, such as fingerprints or facial recognition. The level of access can be based on a user's role and responsibilities within the organisation, or on the specific tasks they need to perform. For example, some users may only be able to view data, while others can control devices, or make changes to the system.

Role-based access control is a method of restricting system access to authorised users. It defines permissions and roles for different users, and limits the actions users can perform within the system. For example, a guest user might have read-only access, while a system administrator might have full access to all system functions.

Any kind of user access management system should have a process for revoking access when a user's role or responsibility changes, or when the user is no longer authorised to access the system.

User help desks and technical support

User help desks and technical support teams provide assistance to users of an IoT system by troubleshooting problems, answering questions, or providing information.

Help desks are typically the first point of contact for users who need assistance with an IoT system. User issues may include trouble logging in, problems with device connectivity, or questions about how to use the system.

A technical support team includes skilled technicians and engineers who can provide advanced assistance to users with complex issues, such as software bugs, hardware failures, and network problems. Technical support teams can also be responsible for maintaining the system, and implementing updates and upgrades.

Both user help desk and technical support are essential for maintaining the availability and reliability of an IoT system. These support processes should be designed to be as efficient and user-friendly as possible, with clear procedures for reporting and resolving issues, and a centralised system for tracking and reporting on the status of support requests.

Change management

Change management refers to the process of planning, implementing, and monitoring changes to an IoT system. The change management process typically includes the following steps:

1. **Identifying and assessing the change:** identifying the need for change, and assessing the potential impact on the organisation, its processes, and its people
2. **Planning the change:** developing a plan for implementing the change, including timelines, resources, and communication strategies
3. **Implementing the change:** putting the plan into action, and making the necessary changes to the organisation, its processes, and its people
4. **Monitoring and controlling the change:** monitoring the progress of the change, and making any necessary adjustments to ensure that the change is implemented as planned
5. **Closing out:** evaluating the change to determine if it was successful, and documenting lessons learned.

Change requests should be evaluated and prioritised based on their potential impact on the system, and their alignment with the overall goals and objectives of the platform. A change request management process tracks the progress of requests, and ensures they are implemented in a timely and efficient manner.

In some cases, changes are not planned. This could be due to equipment failure, accident or some other unexpected event. To the extent that these cases can be foreseen it is worthwhile preparing plans to deal with them well in advance. These plans can then be used when circumstances arise.

Change management is important for IoT systems, as it ensures that changes are made in a controlled and orderly way, minimising the risk of system disruption.

Bugs, troubleshooting, and updates

All IT systems can be subject to unexpected behaviour. Diagnostic and troubleshooting processes and tools are used to identify the cause of any unexpected behaviour (e.g. software ‘bugs’, security breaches, or system overloads). Table 2 describes some common approaches to these issues.

Table 2. Common approaches to IT system issues

Issue	Approach
Troubleshooting	- A troubleshooting process should be in place to quickly identify and resolve issues that arise on the platform. This process should include a clear set of steps to identify the cause of an issue, and a plan for resolving it.
Bugs	- A bug management process is used to track and resolve any issues with an IT platform’s software. It should include a clear set of steps for reproducing the bug, identifying the cause, and resolving the issue.
Updates	- A software update process should be in place to ensure that the platform is kept up to date with the latest features and security patches, including a plan for testing updates before they are deployed to ensure they do not introduce new issues.

Device management

IoT devices should not be treated as ‘set and forget’ – they require ongoing, active management and maintenance.

IoT device management generally involves a wide range of activities and processes to ensure the availability, reliability, and security of IoT devices, and to manage the life cycle of devices. Effective device management requires a combination of technical skills, organisation, and co-ordination, as well as clear processes and procedures.

Although an organisations IT department will typically be responsible for device management they will need to work with other groups such as facilities management groups to gain access to devices on site.

Table 3 summarises typical IoT device management activities and processes.

Table 3. IoT device management activities and processes

Activity	Process
Regular audits and reporting	The process of regularly reviewing and assessing the status and performance of devices on the network, as well as producing reports on the health of devices, and any identified issues. Audits and reporting can identify and resolve problems early.
Alerts and thresholds to support device management	This process can be used to notify administrators of potential issues or problems with devices (such as low battery levels, connectivity issues, or high resource utilisation).
Power management	The process of managing the power supply of devices (such as replacing batteries, cleaning solar panels, or ensuring that devices are properly charged). Power management is important to ensure that devices have the power they need to function properly.
Ongoing troubleshooting	The process of troubleshooting issues with devices (such as sensor drops or connectivity problems). This may include diagnosing and fixing problems, as well as identifying and resolving any underlying issues that may have caused the problem.
Device administration	The process of managing the addition, removal, and relocation of devices, as well as maintaining accurate records of device location, status, and associated user or customer information.
Updates and maintenance	The process of updating the software and firmware on devices (such as applying security patches, or upgrading to new versions).
Return to base (to fix or refurbish devices)	The process of returning devices to a central location for repair or refurbishment. This may include replacing components, updating software, or performing other repairs as needed. The central location may be an office, depot or supplier location. Fixing and refurbishing would typically be done by a product supplier.
Management of asset lifetime, vandalism and damage, decommissioning and end-of-life	The process of managing the life cycle of devices, from initial provisioning to end-of-life management. This may include monitoring for signs of wear and tear, vandalism or damage, and taking appropriate action to repair or replace devices as needed.
Site access for field staff or contractors	This includes providing field staff or contractors with the necessary access and permissions to perform their work, as well as ensuring they have the appropriate training and qualifications to perform their tasks safely and effectively.

Data communications

In an IoT system, the term ‘data communications’ refers to the transmission of data between devices and the IoT platform used to manage them (or to other systems).

IoT-connected environmental sensors (such as those used in air quality monitoring projects) will typically transmit data every few minutes. They can sometimes be configured to transmit data more or less frequently, depending on organisational needs. This is fundamentally different to how previous generations of environmental data logging systems would operate, where personnel were required to visit each sensing device in turn to collect data.

Key operational activities and processes relating to data communication will vary according to the data infrastructure chosen for an IoT system, but may include:

- network operations
- IP address management
- performance monitoring
- policy and fair use enforcement
- content filtering
- software updates and patching
- fault reporting and resolution
- spare parts reserves
- preventative maintenance (such as battery replacement)
- intrusion prevention and security
- change management.

Please refer to the OPENAIR Best Practice Guide chapter *Data communications procurement* for more information.

IoT and data platforms

IoT platforms are used to manage IoT devices. In some cases, they also manage the data collected from IoT devices. Separate data platforms can also be used to store and manage sensor data, and to make that data available to other systems, including analytics platforms.

For a detailed description of IoT and data platforms, please refer to the OPENAIR Best Practice Guide chapter *Platforms and digital services criteria*.

This section notes some key considerations for ensuring the smooth operation of air quality IoT and data platforms, including:

- adding and configuring new IoT devices
- integrating platforms with other systems.

Adding and configuring new IoT devices

The approach to adding new devices or data sources to IoT platforms should be systematic, well-documented, and involve close collaboration between all stakeholders. This ensures a smooth and efficient process, while maintaining security and scalability. The following steps are key:

- **Device compatibility check**: verify that the new devices or data sources are compatible with the existing IoT platform
- **Device onboarding**: develop a device onboarding process that includes the necessary steps for setting up and configuring new devices (such as provisioning device credentials, assigning device-specific configurations and parameters, and installing necessary software)
- **Data integration**: identify and implement the necessary steps for integrating data from the new devices or data sources with the existing platform
- **Security**: ensure the new devices or data sources are secure, and that they comply with any platform security requirements
- **Testing**: test the new devices or data sources to ensure they are working as expected, and that they do not create any unexpected system issues
- **Monitoring**: monitor the new devices or data sources to detect and troubleshoot any issues that may arise
- **Scalability**: consider the impact that the new devices or data sources will have on the overall scalability of the platform
- **Documentation**: document the process of adding new devices or data sources, including any configurations, dependencies, and instructions for troubleshooting
- **Communication**: communicate the existence of new devices or data sources to all relevant stakeholders, and describe any resulting changes to the system, or potential impact.

Platform integration with other systems

Integration of IoT and data platforms with other IT systems allows you to get more value from the data collected by an air quality monitoring system (for instance, using existing dashboards, websites, reporting, and analytical systems).

Some common methods used to integrate systems include:

- **Application Programming Interfaces (APIs)**: APIs allow different systems to communicate with each other and to share data in a structured and secure way (e.g. sensor device manufacturers can provide an API to their IoT platforms, so that organisations can easily access the data stored on them)
- **Data integration and transformation**: this method of ‘extracting, transforming, and loading’ data (known as ETL) from one system to another depends on a process of data integration (where data is extracted from the source, transformed to match the target system, and loaded to the target system)

- **Middleware**: provides a layer of abstraction between different systems, allowing them to communicate and share data in a more flexible and efficient way
- **Event-driven architecture (EDA)**: a design pattern that allows different systems to communicate with each other through a ‘publish-subscribe’ mechanism (where systems publish events, and other systems subscribe to those events, allowing for real-time communication)
- **Cloud integration**: cloud-based systems and platforms can be integrated through the use of cloud services and APIs
- **Service-oriented Architecture (SOA)**: a design pattern that allows different systems to communicate with each other through the use of services (which are well-defined interfaces that expose the functionality of a system)
- **Containerisation and microservices**: both of these approaches integrate different systems by breaking down monolithic systems into smaller, independently deployable, and manageable services
- **Data communication protocols**: different communication protocols (such as MQTT, AMQP, CoAP, or HTTP) can be used to enable data transfer between different systems and platforms (note: these protocols are different to those used to transmit data from sensing devices to IoT platforms).

The specific approach for integration will depend on the systems and platforms involved, and the requirements of your organisation. It is important to ensure that the integration is secure, reliable, and scalable, while maintaining the overall architecture.

TIPS: IoT and data platform integration (and operations) can be managed either by in-house staff, or outsourced to external providers. See Table 1 for the pros and cons of both approaches.

Data storage

Data storage relates to the ongoing management of data generated by smart air quality monitoring systems. Data storage can be implemented in IoT platforms, or handled in a separate data platform. Key considerations include:

- **requesting and implementing changes to the structure of the data storage solution**: the storage solution must be able to adapt to changing requirements, and handle new types of data and new data sources
- **requesting and managing updates to the project data schema**: the data storage solution must be able to handle updates to the data schema (such as adding new fields or telemetry).

Data backup and recovery are also important aspects of data storage management. Please refer to the OPENAIR Best Practice Guide chapter *Platforms and digital services criteria* for more information.

Security

Air quality monitoring devices are often located in publicly accessible areas, and may use public data communications networks. This makes them potentially vulnerable to certain security risks, including:

- **confidentiality risks** (such as unauthorised access to the system or data, eavesdropping on communications, or data breaches that can expose sensitive information)
- **integrity risks** (such as 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** (such as denial-of-service attacks, malware infections, or hardware failures that can disrupt the availability of the system)
- **physical security risks** (such as vandalism, weather-related damage, and accidental damage to devices, or power supply issues and network interruptions caused by natural disasters).

IoT air quality monitoring systems need to be actively managed to mitigate these security risks, and to detect and respond to security issues if they do occur.

Further guidance on the topic of cybersecurity risk assessment (and a practical cybersecurity checklist) can be found in the OPENAIR Best Practice Guide chapter *Cybersecurity for smart air quality monitoring networks*.

Data sharing

The rationale for any proposed sharing of collected data should be very clear from the outset of your project. Before any data sharing happens, all relevant policies, roles, and responsibilities should be defined (see the OPENAIR Best Practice Guide chapter *Sharing air quality data* for more information).

Best practice management of data sharing involves taking the following actions:

- establish and execute data sharing processes in alignment with your organisation’s data sharing policy
- update your organisation’s data sharing policy and processes to comply with the latest regulations and best practice guidelines
- clarify the roles and responsibilities of data owners, custodians, and users
- keep records of data sharing requests, as well as any actual sharing of data (as per data sharing agreements)
- undertake periodic audits to ensure data sharing policies are being followed.

Ideally, organisations would undertake the above on a “whole or organisation” basis. Organisations just starting to share data may chose to focus on a particular project initially (such as their air quality monitoring project).

Minimising the cost of IoT system operations

IoT systems can incur significant costs. These can include the purchase of sensor hardware, software, and platform licences, as well as the cost of operational support and maintenance. All of these costs should be considered as part of the total cost of ownership of an IoT system (within the overall IT operations of an organisation).

There are several processes that can help local governments to minimise IoT system operational costs, including:

- **Integrated user and permission management**

  Implementing a centralised user and permission management system can streamline the process of managing users and devices, reducing the need for manual intervention and the risk of errors. It can also improve security by controlling access to the system and data.

- **Automated system operations**

  Automating repetitive or time-consuming tasks (such as device provisioning, software updates, and troubleshooting) can reduce the need for manual intervention, save time, and improve efficiency.

- **Performance monitoring and reporting**

  This kind of monitoring can identify potential issues early on, and prompt actions to resolve them before they become more serious or complex.

- **Service Level Agreement compliance reporting**

  Implementing a system for monitoring and reporting on compliance with SLAs ensures the system is meeting the agreed-upon performance and availability standards, identifies areas for improvement, and takes actions to improve the system’s performance.

- **Cloud-based infrastructure**

  Moving IoT systems to a cloud-based infrastructure reduces the need for on-premises servers and other hardware, as well as the associated costs of maintaining and upgrading that hardware. Cloud-based infrastructure can also provide scalability and flexibility. Organisations should do their own assessment to determine the best approach.

Additional resources

NSW Government | Internet of Things (IoT) Policy Guidance

The IoT Policy Guidance provides: (1) practical guidance to help organisations design, plan and implement IoT solutions (2) advice on standards and obligations where available and practical (3) tools and templates to help effectively manage an IoT-enabled project (4) guidance on where and how to source additional advice if required.

Simplilearn | What is ITIL- Concepts Process Benefits

This is a complete guide on what ITIL is and the key concepts, processes and benefits of it. In IT service management, ITIL has become the standard. It assists organisations in various industries offer their services in a way that’s economical and quality-driven.

Associated OPENAIR resources

Best Practice Guide chapters

Data communications procurement

This Best Practice Guide chapter explores the various communications technologies that can support smart low-cost air quality sensing, and provides advice on selecting technologies that are appropriate to a project and organisation.

Platforms and digital services criteria

This Best Practice Guide chapter provides guidance for the selection of appropriate platforms and digital services to support smart air quality monitoring.

Cybersecurity for smart air quality monitoring networks

This Best Practice Guide chapter provides guidance on key cybersecurity considerations for local governments establishing smart low-cost sensor networks and supporting platforms and services.

Sharing air quality data

This Best Practice Guide chapter provides guidance on the sharing of air quality data. It explores the process by which a local government might assess data to determine its shareability, and presents a series of practical options for implementing data sharing.

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 chapter is part of a suite of resources designed to support local government action on air quality through the use of smart low-cost sensor 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: 20231023 BP306 IoT system operations Version 1 Final