TECHNICAL CODE

COMMUNICATIONS INFRASTRUCTURE ASSET MANAGEMENT

Developed by

Malaysian Technical Standards Forum Bhd

Registered by

MCMC

Registered date: 5 May 2026

MCMC MTSFB TC G057:2026

Development of technical codes

The Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) ('the Act') provides for a Technical Standards Forum designated under Section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to Section 185 of the Act shall consist of, at least, the requirements for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by Section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under Section 185 of the Act.

A technical code prepared in accordance with Section 185 shall not be effective until it is registered by the Commission pursuant to Section 95 of the Act.

For further information on the technical code, please contact:

Malaysian Communications and Multimedia Commission (MCMC)
MCMC HQ Tower 1
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8688 8000
Fax : +60 3 8688 1000
Email : stpd@mcmc.gov.my
Website: www.mcmc.gov.my

OR

Malaysian Technical Standards Forum Bhd (MTSFB)
Level 3A, MCMC Tower 2
Jalan Impact
Cyber 6
63000 Cyberjaya
Selangor Darul Ehsan
MALAYSIA

Tel : +60 3 8680 9950
Fax : +60 3 8680 9940
Email : support@mtsfb.org.my
Website: www.mtsfb.org.my

Contents

Committee representation

This technical code was developed by the Communications Infrastructure Asset Management Sub Working Group under the Green ICT, Environment & Climate Change Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB), which consists of representatives from the following organisations:

CelcomDigi Berhad

Digital Connect Society

Digital Nasional Berhad

D'Harmoni Telco Infra Sdn Bhd

Edgepoint Tower Sdn Bhd

EDOTCO Malaysia Sdn Bhd

FNS (M) Sdn Bhd

International Islamic University Malaysia

Maxis Broadband Sdn Bhd

Measat Broadcast Network Systems Sdn Bhd

REDtone Engineering and Network Services Sdn Bhd

The IO Network MY Sdn Bhd

TM Technology Services Sdn Bhd

TIME dotCom Berhad

U Mobile Sdn Bhd

Universiti Teknikal Malaysia Melaka

YTL Communications Sdn Bhd

Foreword

This technical code for the Communications Infrastructure Asset Management ('this Technical Code') was developed pursuant to Section 185 of the Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) by the Communications Infrastructure Asset Management Sub Working Group under the Green ICT, Environment & Climate Change Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB).

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

MCMC MTSFB TC G057:2026

COMMUNICATIONS INFRASTRUCTURE ASSET MANAGEMENT

0. Introduction

Communications assets are the components that make up the digital backbone of a nation and the communications services which are critical to local authorities, central governments, and communities.

The current lack of a structured and standardised approach to asset management among Service Providers (SPs) increases the risk in infrastructure assets management, leading to potential service disruptions, operational inefficiencies, and a decline in consumer confidence and service quality. Besides, ensuring the accuracy and timely reporting of infrastructure data to regulatory bodies remains a challenge, highlighting the urgent need for improved governance, standardisation, and accountability across the industry.

To address these challenges, a more structured Communications Infrastructure Asset Management (CIAM) approach is essential. CIAM involves establishing a comprehensive and accurate inventory of infrastructure assets at the organisational level. This enables stakeholders across both public and private sectors to enhance governance, ensure regulatory compliance and reporting, and optimise the financial and service value of physical assets and ultimately contributing to more reliable services and greater public benefit.

CIAM ensures communications assets are planned, operated, and maintained effectively throughout their lifecycle to support national security, economic stability, and public well-being. Effective CIAM improves regulatory oversight and compliance, enhances data accuracy, and optimises service delivery costs. It promotes social equity by expanding access to reliable communications services and reducing the digital divide, while supporting environmental sustainability through long-term, well-planned infrastructure management. CIAM also strengthens the resilience of public services against disruptions such as natural disasters and health emergencies, ensuring dependable, continuous communications for citizens, businesses, and government.

The objectives of this Technical Code are to serve as a guide for the industry on matters relating to the management of communications infrastructure assets with respect to the asset management lifecycle, and to fulfil regulatory requirements and protect consumer interests including:

a) to improve governance of infrastructure asset, as well as the relevant internal processes and procedures in addressing the required outcomes;

b) to improve the assets' effectiveness and efficiency, and to optimise equipment reliability;

c) to ensure that the infrastructure asset is managed in a way that it meets the expected requirements for coverage and quality of service; and

d) to promote coordinated planning, development, and use of communications infrastructure assets, and to facilitate accurate and timely asset data reporting to regulatory bodies for effective monitoring and compliance.

The CIAM framework, as shown in Figure 1, serves as a guideline for establishing a comprehensive asset management process, ensuring the reliability, efficiency, and sustainability of communications infrastructure. This framework provides a structured approach to managing assets across their entire lifecycle, integrating systems, stakeholders, and processes to enable consistent governance, effective decision-making, and accurate reporting.

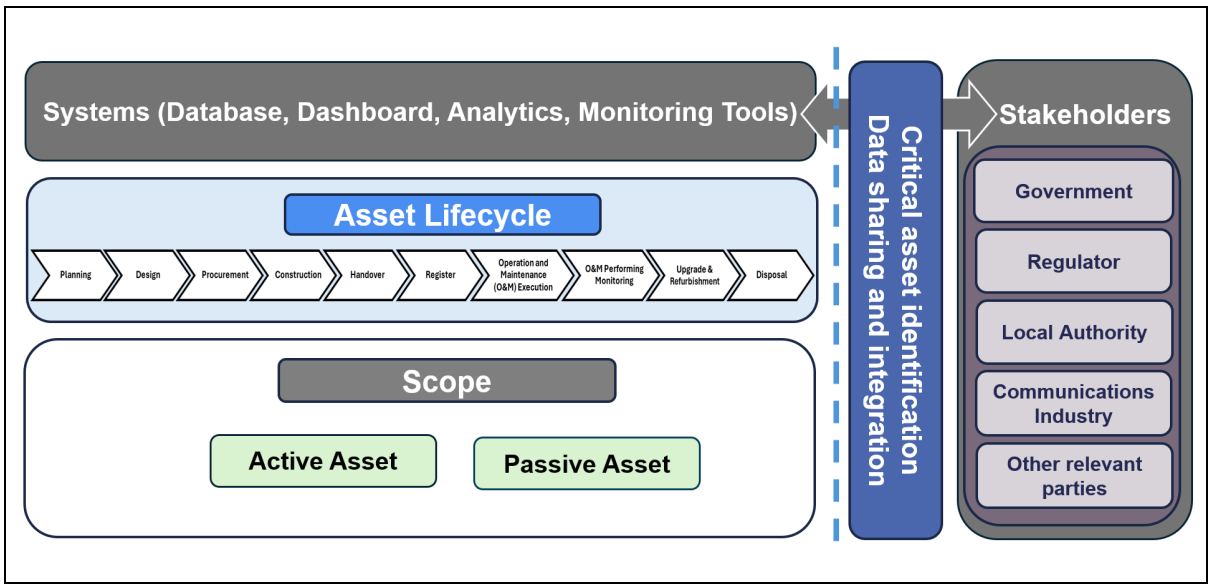

Figure 1. Communications infrastructure asset management framework

The key components of the CIAM framework are explained below.

a) Systems, which includes databases, dashboards, analytics tools, and monitoring tools essential for data collection, analysis, and visualisation.

b) Asset lifecycle outlines the various stages of an asset's life, including planning, design, procurement, construction, handover, registration, operations and maintenance, performance monitoring, upgrades and refurbishment, and disposal.

c) Scope of the assets define the boundaries of the CIAM framework, encompassing a broad spectrum of both active and passive infrastructure assets. The list of these asset categories is detailed in Annex A.

d) Stakeholders represent the various parties involved in CIAM, such as government, regulators, local authorities, communications industry, and other relevant organisations. It outlines the roles of the key stakeholders involved in CIAM, their responsibilities, and how they should interact with the CIAM process. It provides a reference for understanding the relationships and expectations within the CIAM framework.

e) Data-sharing and integration, component highlights the critical role of data-sharing and integration among stakeholders and systems to enable effective decision-making and asset management. It also supports critical assets identification, ensuring that assets vital to network operations, national security, and public services are prioritised for protection, management, and resource allocation.

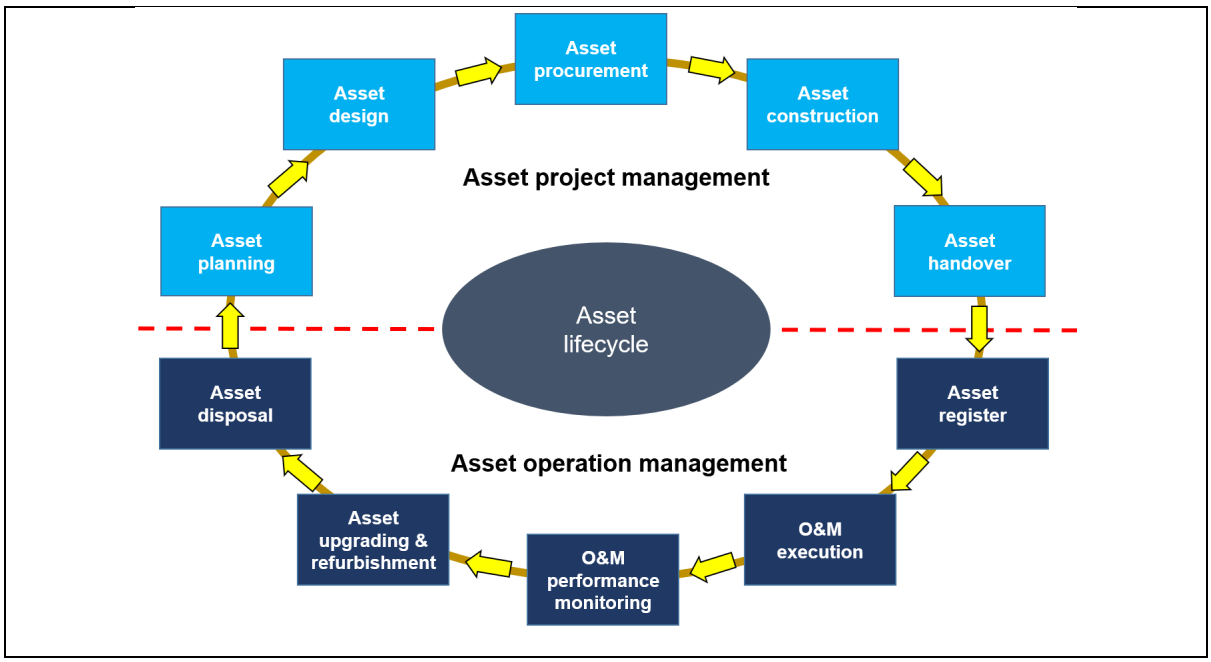

Figure 2. Communications infrastructure asset management lifecycle

1. Scope

This Technical Code specifies the requirements for managing the physical communications infrastructure asset, throughout the entire lifecycle. It covers the network that provides connectivity and access to the end-users, with 2 basic categories.

a) Active assets

This may include electronic and powered components, including, but not limited to, switches, servers, radio access nodes, transmission equipment and core network equipment.

b) Passive assets

This may include a non-electronic, non-powered component with diverse range of assets, such as towers, antenna, manhole, cabinets, fibres, and power generation equipment.

2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

Act 127, *Environmental Quality Act 1974*, Department of Environment (DOE)

Environmental Quality (Scheduled Wastes) Regulations 2005, Department of Environment (DOE)

Communications and Multimedia (Technical Standards) Regulations 2000

Standard Radio System Plan (SRSP)

MCMC MTSFB TC G009, *Information and Network Security - Requirements (Second Revision)*

MCMC MTSFB TC G014, *Business Continuity Management - Requirements*

MCMC MTSFB TC G041, *Radiocommunications Network Facilities - Compliance Audit for Radiocommunications Structure*

ISO 9001, *Quality Management Systems - Requirements*

ISO 14001, *Environmental management systems - Requirements with guidance for use*

ISO 27001, *Information security, cybersecurity and privacy protection - Information security management systems - Requirements*

ISO 55000, *Asset Management - Overview, principles and terminology*

Environmental Requirements: A Guide for Investors (11th ed.), Department of Environment Malaysia. (2010).

Guidelines for Packaging, Labelling and Storage of Scheduled Wastes in Malaysia, Department of Environment Malaysia

3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

See Annex B.

4. Terms and Definitions

For the purposes of this Technical Code, the following terms and definitions apply.

4.1 Active asset

An elements or components on the active layer of a communications network, including, but not limited to switches, servers, radio access nodes, transmission equipment and network equipment.

4.2 Asset

An item, thing, or entity that has potential or actual value to an organisation.

4.3 Asset construction

Referring to the deployment or roll-out process of active and passive infrastructure assets which are used to deliver and provide communications services.

4.4 Asset lifecycle

End-to-end process by which an asset is purchased, stored, used, and maintained over the course of its useful life. It involves stages such as planning, purchasing, deployment, operation, maintenance, and disposal or renewal of the asset.

4.5 Asset management system

A system that is used by the organisation to direct, coordinate and control asset management activities with a structured approach over different life cycle stages, start with the planning of the need for the asset, through to its disposal, including the managing of any potential post disposal liabilities.

4.6 Asset owner

The party who is financially responsible for the asset, owns the asset and can make decisions that can affect the state of the asset at any point.

4.7 Capital expenditures (Capex)

Company’s major purchases that are used over the long term.

4.8 Communications

The exchange of information, whether between persons and persons, things and things, or persons and things, in the form of sound, data, text, visual images, signals or any other form or any combination of those forms.

4.9 Operating expenses (Opex)

Daily costs incurred to maintain business operations.

4.10 Passive asset

Infrastructure that is not part of the active layer in communications network, including a non-electronic, non-powered component with diverse range of assets, such as towers, antenna, manhole, cabinets, fibres, and power generation equipment.

4.11 Redundant, Obsolete, Trivial (ROT)

Digital information that has little or no business value to the organisation but is still stored.

4.12 Stakeholders

An individual, group or organisation that's impacted by the outcome of a project.

4.13 Supplier

An appointed party by the asset owner in carrying out any specific tasks related to the asset management activities.

5. Asset planning

Asset planning in CIAM is to create a methodical and tactical plan that aligns an organisation's infrastructures and other assets with an agreed-upon standard of service.

Below are the recommended considerations for asset planning.

a) Needs assessment

Identify current and future communications needs, considering factors such as population growth, technological advancements, and market demand.

b) Goal setting

Establish clear objectives and goals for communications infrastructure development, aligning with broader national, regional, or organisational strategies.

c) Risk assessment

Evaluate potential risks and challenges associated with communications infrastructure projects, including regulatory, environmental, and financial risks.

d) Budgeting

Allocate resources and funding for communications infrastructure projects based on strategic priorities and financial constraints.

Figure 3 represents the base guideline for the asset planning process specifically for CIAM. The details are described in 5.1 to 5.6.

Figure 3. Asset planning process

5.1 Initiation or user request

The asset planning process starts with identifying the high-level needs or requirements to establish infrastructure assets, based on the information and considerations below as shown in Table 1.

Table 1. Considerations for project initiation and user request

Type of consideration	Details
Technology request cycle	Producing a plan from the initial development of a technology to its obsolescence, which involves technology's adoption, growth, maturity and decline over time and is often used to analyse the dynamics and evolution of technologies.
Asset lifecycle	A maximum workload/capacity and gradual deterioration over a specific time before it requires an upgrade or replacement.
Resource planning and optimisation	Plan on asset replacement over time which may be driven by technological changes, asset design limitation and industry market change.
Risk management	A risk-based approach helps make better decisions by evaluating current and potential risks, which consider factors on business risk, service disruption risk, and security risk.
Business strategy and alignment and financial expectation	Alignment of asset planning with business or financial strategies that can lead to improve service delivery and making services more affordable for end users or the community.
User experience and satisfaction	Include factors that affect the service coverage and capacity needs in the infrastructure planning, such as users, socio-economic conditions, and regulatory requirements.

5.2 User requirements

Detailed requirements are to be gathered and analysed as part of the infrastructure planning. Examples of user requirements are given below.

a) Stakeholders goal and perspectives

Define and reconcile the goals of all key internal and external stakeholders (e.g., regulators, customers, operations, finance) to ensure infrastructure investments maximise long-term business value and public benefit.

b) Technical scalability and futureproofing

Assess the capacity and architectural flexibility required to support projected demand growth (e.g., data traffic, connected devices) and to integrate emerging technologies over the asset's lifecycle.

c) Define use case and business requirements

Clearly define the specific services or applications the infrastructure must support (its use case) to establish precise technical parameters and justify the financial viability (the business case) of the asset. Different use cases may require different infrastructure and planning considerations.

d) Key Performance Indicators (KPIs)

Establish quantitative and measurable metrics (e.g., network uptime, latency, mean time to repair, coverage penetration) to ensure the new or modified asset performs successfully and meets all required quality of service standards.

5.3 Asset assessment

Asset assessment may involve several evaluations of the asset condition, performance, and value to determine their strategic importance and the need for maintenance activity. Table 2 shows the common types of asset assessment.

Table 2. Types of assessment

Type of assessment	Descriptions
Risk and safety	Focuses on identifying and evaluating the risks to an organisation's assets. Need to assess the likelihood of the identified threats occurring and determine the impact on the business. Threats can be in the form of natural, man-made or environmental
Regulatory and compliance	Compliance with the regulations is essential for any organisation. Adhering to the regulatory aspect shall enable seamless integration of any asset to be used for its service. Eventually, the integration of new assets shall always consider industry-set standards, national rules and regulations, and acts. All communications equipment is required to be certified by the registered certifying agency, in accordance with the Communications and Multimedia (Technical Standards) Regulations 2000.
Useful life	Organisations shall always plan on the longevity of their assets. It shall run smoothly throughout their lifespan and always on minimal preservation requirements.

Table 2. Types of assessment *(continued)*

Type of assessment	Descriptions
Environmental impact	It is imperative to integrate sustainability and green technologies into the core of asset planning and evaluation for future generation use.
Technology evolution	As technology progresses, organisations must ensure that their assets remain relevant and practical by adopting advancements that align with latest industry standards. Any new technology integration should prioritise efficiency, scalability, and agility while ensuring compatibility with the existing systems.

5.4 Asset data collection

Asset data collection refers to a systematic process of gathering, organising, and analysing information to support effective infrastructure management. In CIAM, it involves compiling a comprehensive inventory of assets, evaluating their condition, performance, and resilience, and analysing usage patterns, demand forecasts, and demographic trends. It also includes identifying risks and vulnerabilities, such as environmental hazards, technological obsolescence, and regulatory changes, to develop mitigation strategies. Ultimately, this process supports informed decision-making and optimises the lifecycle, efficiency, and sustainability of communications infrastructure assets. Table 3 shows the common asset data collection methods.

Table 3. Asset data collection methods

Methods	Activities
Field surveys and inspection	Involve visiting a site to collect and assess data through observation and measurement.
Stakeholder engagement	A process of involving and communicating with people or groups who are interested in or are affected by a project or decision.
Remote sensing technologies	Satellites or aerial sensors are used to collect data about an area from a distance, allowing for large-scale monitoring and analysis.
Data analytics	Involve examining and interpreting data to uncover patterns and insights that inform decision-making and predictions.

5.5 Asset prioritisation

Asset prioritisation is a systematic approach to determining the importance and values of assets. It involves assessing the criticality of each asset and determining the potential impact on the business. Figure 4 illustrates the five (5) purposes of asset prioritisation, which can be done with several methods but are not limited to those as shown.

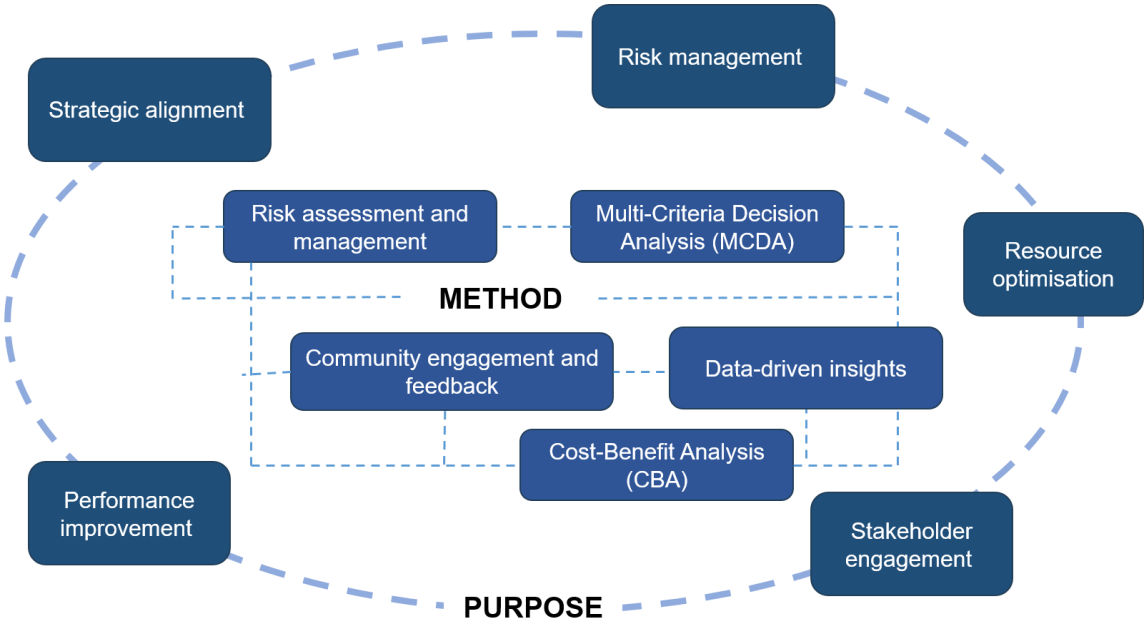

Figure 4. Purpose of asset prioritisation and its methods

Asset prioritisation serves the following five key purposes.

a) Strategic alignment

Sets the organisation's goals, initiatives, and resources and ensures they are in sync with its overall strategy and objectives.

b) Risk management

The ability to identify, assess, and prioritise potential risks to an organisation’s operations, followed by implementing strategies to mitigate or manage those risks effectively.

c) Resource optimisation

Good practice of optimising the use of available resources (such as time, personnel, finances, and technology) to achieve maximum efficiency and productivity while minimising waste.

d) Stakeholder engagement

Actively involving key individuals, groups, or organisations in the decision-making process to ensure that asset management strategies align with their needs, concerns, and expectations.

e) Performance improvement

The ongoing effort involves enhancing an organisation’s processes, productivity, and outcomes, by setting clear performance goals, and implementing strategies to boost efficiency, effectiveness, and quality.

Asset prioritisation can be achieved using various methods, including but not limited to:

a) Community engagement and feedback

Involves local communities, customer groups, or public stakeholders to gather a more comprehensive view of asset impact on social, environmental, or quality-of-life.

b) Cost-Benefit Analysis (CBA)

Weighs the costs of maintaining or replacing an asset against the potential benefits (e.g., improved efficiency, reduced downtime, or compliance).

c) Data-driven insight

Uses qualitative and quantitative factors such as performance metrics, asset condition data, historical trends, and stakeholder feedback to enhance the prioritization decisions.

d) Multi-Criteria Decision Analysis (MCDA)

Evaluates assets based on multiple criteria, such as cost, performance, risk, and strategic value by engaging stakeholders in the process.

e) Risk assessment and management

Assesses the risks associated with asset failure, which includes factors such as probability of failure and the potential consequences of failure.

f) Performance metrics

Uses performance data such as uptime, efficiency, or throughput to evaluate how well assets contribute to organisational goals.

5.6 Budget, resource allocation and decision-making

Three crucial pillars to effectively manage successful projects are budgeting, resource allocation, and decision-making with stakeholder approval, emphasising the importance of careful planning and execution.

The strategic priorities, lifecycle costs, risk management, stakeholder insight, and data-driven are among the key considerations for budget planning.

The commonly used methods for budget planning of infrastructure asset development are as follows:

a) Incremental budgeting

A budgeting method where the previous year's budget is used as a starting point, with adjustments made for the current year based on changes in revenue or expenditure. It typically involves making incremental changes rather than a complete overhaul.

b) Zero-Based Budgeting (ZBB)

A budgeting approach where every expense shall be justified for each new period, starting from a zero base. All expenditures are evaluated and approved based on their necessity and alignment with current priorities, rather than on past budgets.

c) Activity-based budgeting

A method where resources are allocated based on specific activities or projects. Costs are assigned to individual activities or projects, and budgeting is done by assessing the resources needed for each activity to achieve organisational goals.

d) Performance-based budgeting

A budgeting approach that links funding to the achievement of specific performance outcomes or goals. Resources are allocated based on expected results, aiming to improve efficiency and effectiveness by focusing on performance metrics.

e) Capital budgeting

The process of planning and evaluating investments in long-term assets, such as infrastructure or major equipment. It involves assessing large expenditures' financial viability and potential returns to ensure that capital investments are strategically sound.

The key factors that affect stakeholders' decision-making, recommendation and approval are as follows:

a) strategic and business alignment;

b) regulatory compliance;

c) financial viability;

d) risk management; and

e) stakeholder engagement.

The following activities shall support the decision-making process but not limited to:

a) project evaluation and selection;

b) formal review;

c) approval and endorsement; and

d) documentation and reporting.

6. Asset design

Asset design involves planning and creating the physical and virtual components necessary for efficient communications networks. The goal is to optimise performance, reliability, scalability, and security while meeting the specific needs and objectives of the organisation.

Below is an outline of the recommended considerations for asset design:

a) Stakeholder needs

Understand the requirements and expectations of stakeholders, including telecom operators, regulatory bodies, and end-users.

b) Service demands

Assess the anticipated demand for telecom services, including voice, data, video, and emerging technologies like 5G and Internet of Things (IoT).

c) Technical specifications

Define technical specifications for the telecom infrastructure, such as bandwidth, coverage area, reliability, and scalability.

d) Emerging technologies

Evaluate emerging technologies, such as 5G, edge computing, and Software-Defined Networking (SDN), to support future growth and innovation in telecom services.

The asset design process and its components are described as per Figure 5.

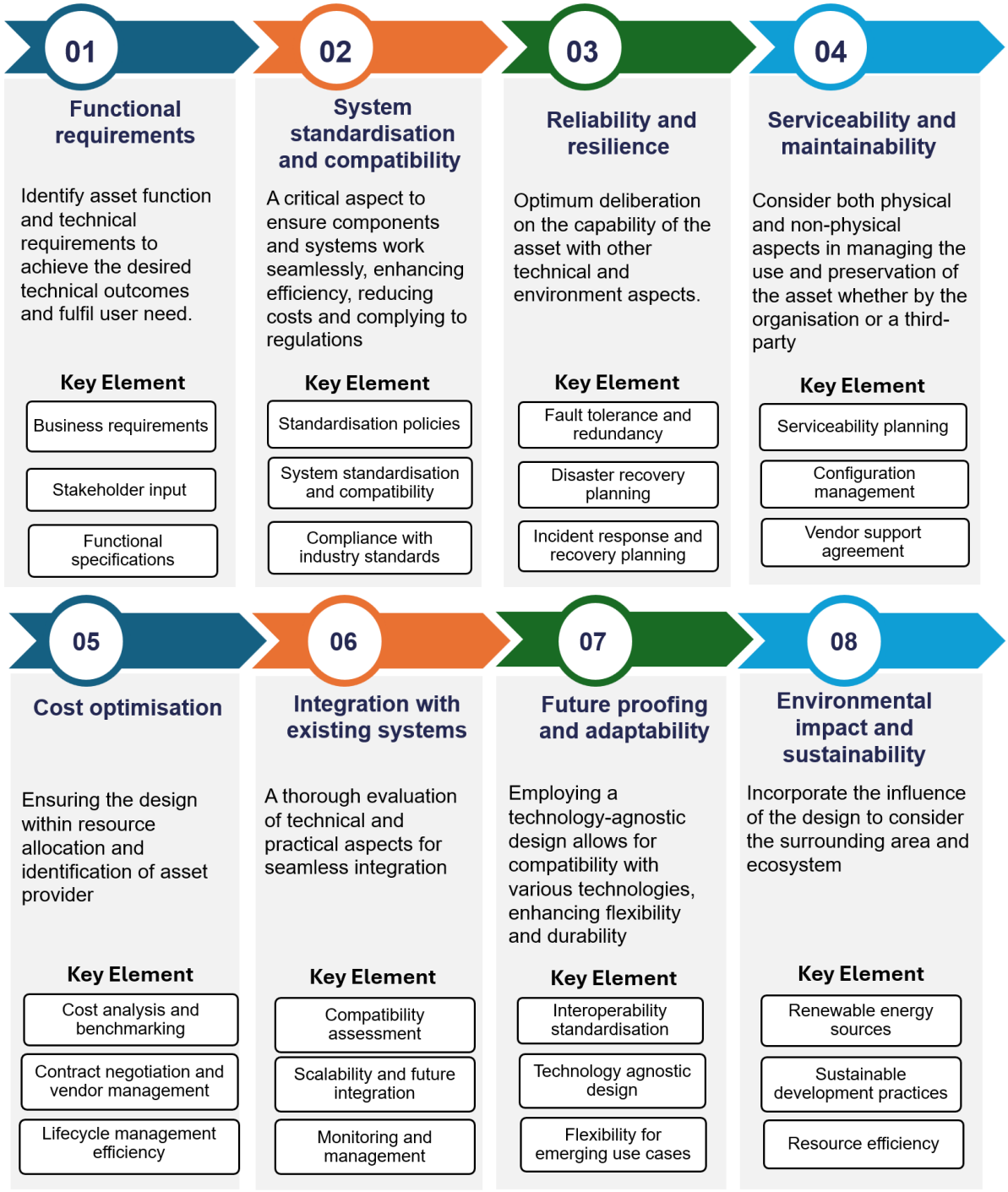

Figure 5. Asset design process and its components

7. Asset procurement

Asset procurement is sourcing and obtaining assets for an organisation's assets to support its operations and achieve business goals.

Below are the recommended considerations for asset procurement:

a) Request for Proposal, Quotation or Information (RFx)

Prepare and issue RFx to qualified suppliers, outlining project requirements, technical specifications, evaluation criteria, contract terms, and deadlines for submission of proposals.

b) Supplier selection

Select the most qualified and competitive suppliers based on the evaluation results, considering factors such as technical expertise, financial stability, past performance, and alignment with project goals and timelines.

c) Contract development

Draft and finalise contracts with selected suppliers, detailing the scope of work, deliverables, milestones, payment terms, dispute resolution mechanisms, and any other relevant terms and conditions.

d) Purchasing

Issue purchase orders or procurement contracts to selected suppliers, specifying the quantity, specifications, prices, and delivery instructions for procuring communications infrastructure assets.

e) Supplier management

Selecting suppliers, negotiating contracts, controlling costs, reducing supplier-related risks and ensuring service delivery.

Figure 6 represents the base guideline for the asset procurement process. The details are described in 7.1 to 7.3.

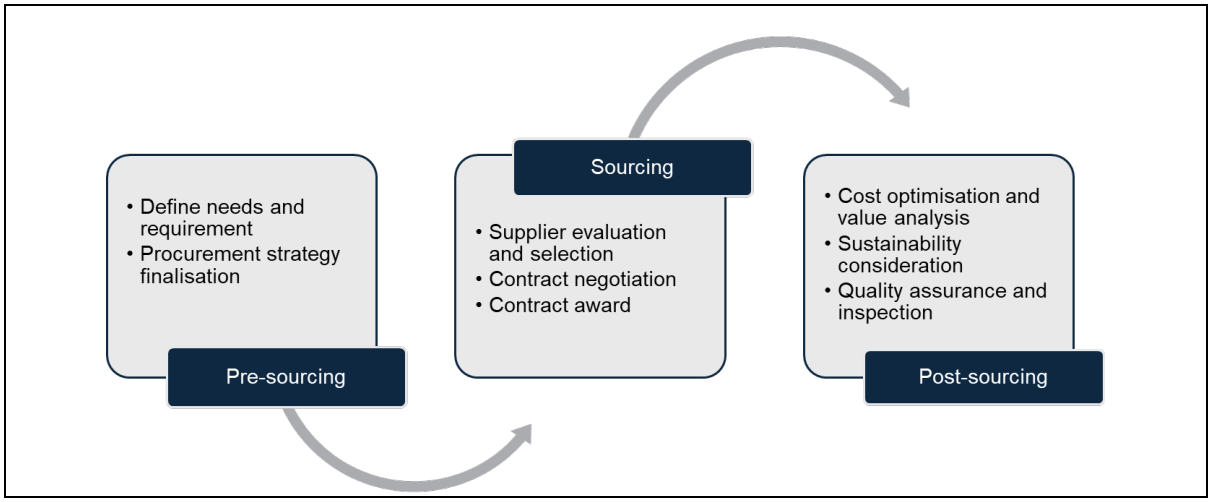

Figure 6. Asset procurement process

7.1 Pre-sourcing

Pre-sourcing involves identifying and understanding the needs and requirement for goods or services. It may include having a business case outlining the requirement cost and risk to secure budgeting, the supplier landscape and development of a procurement strategy for high value or complex items that aligns with the strategic goals of the organisation.

7.1.1 Define needs and requirement

In defining procurement needs and requirements to acquire goods and services that meet operational needs and support broader business objectives, an organisation should consider the following key factors:

a) Market research;

b) business growth projections and forecast;

c) functional and technical specifications approved documents;

d) performance metrics;

e) intellectual property rights;

f) performance guarantees;

g) product warranty; and

h) warranty period.

7.1.2 Procurement strategy finalisation

Finalising a procurement strategy is a critical stage in the procurement process, ensuring that the approach is well-aligned with the organisation's operational needs and strategic goals. Elements to be considered are:

a) procurement and project timeline;

b) sourcing method or strategy;

c) Request for Proposal (RFP), Request for Quotations (RFQ), Request for Information (RFI), competitive bidding;

d) local sourcing and global sourcing;

e) reverse auction (bidding);

f) supplier diversity;

g) supplier databases;

h) quality management systems;

i) government and industry certifications; and

j) capacity and scalability.

7.2 Sourcing

This phase involves engaging with suppliers. It includes supplier evaluation and selection, contract negotiation and contract award and establishment. The goal is to find the best value in terms of price, quality, and delivery terms.

7.2.1 Supplier evaluation and selection

Supplier selection is a strategic process where businesses identify, assess, and contract with suppliers that align best with the unique requirements and objectives of the business. It should be performed based on the following criteria:

a) technology roadmaps;

b) needs assessment and requirements compliance;

c) business growth projections and forecast;

d) legal review (record);

e) commercial submission;

f) supplier capacity and capability;

g) supplier performance evaluation;

h) Proof of Concept (POC) trial equipment; and

i) risk analysis.

7.2.2 Contract negotiation

Effective contract negotiation and management are crucial for maintaining good supplier relationships and mitigating potential risks. Below is the list of elements to be considered during the negotiation:

a) supplier negotiation and contract management;

b) agreement terms and conditions and agreements duration;

c) termination and exit strategy;

d) renegotiation and renewal planning;

e) performance guarantees and penalties;

f) benchmark and pricing; and

g) incentives and penalties.

7.2.3 Contract award and establishment

Contracts can be made to a single, multiple or a panel of suppliers depending on the award strategy. Upon successful award to the supplier, a contract shall be established, which clearly stipulates the agreed terms and conditions between both parties. Typical steps for contract establishment are as follows:

a) Letter of Intent (LOI);

b) Letter of Offer (LOO); and

c) Contract agreement and signing.

7.3 Post-sourcing

Post-sourcing involves contract management, monitoring supplier performance, ensuring timely delivery, processing payments, and maintaining long-term supplier relationships.

7.3.1 Cost optimisation and value analysis

It is the process of monitoring the declared cost saving (during pre-sourcing) with the actual (post-sourcing) during the contract utilisation. It is a strategic, continuous process used to ensure an organisation achieves the maximum possible value from its total expenditure on assets, operations, and services. Its primary goal is to maximise value while reducing waste.

To effectively realise the financial benefits of the procurement process, below are recommendations for organisation to consider.

a) Establish a baseline

Clearly define and document the declared cost savings and expected value (e.g., efficiency gains, reduced Opex) established during the pre-sourcing phase.

b) Track actual performance

Continuously monitor and quantify the actual costs, financial performance, and value realisation throughout the contract's term.

c) Conduct variance analysis

Periodically perform variance analysis to identify any significant deviations between the forecasted savings and the actual savings.

d) Initiate corrective action.

Use the analysis results to initiate timely corrective actions (e.g., renegotiation, process improvements, or contract adjustments) to close value gaps and ensure the asset continues to deliver its projected financial and operational value.

This practice ensures the asset investment remains financially optimised and delivers the maximum value over its lifecycle.

7.3.2 Sustainability consideration

Sustainability considerations are integral to decision-making processes across various domains, encompassing environmental, social, and economic aspects. Key sustainability considerations are:

a) environmental impact assessment;

b) energy efficiency ratings;

c) green standards and certifications;

d) recyclability and disposal practices;

e) carbon footprint reduction;

f) supplier sustainability practices; and

g) longevity and upgradeability.

7.3.3 Quality assurance and inspection

Quality assurance and inspection play pivotal roles in ensuring the reliability, performance, and compliance of products and services sourced from suppliers. Below is the sample list of inspections that can be done throughout the sourcing and post-sourcing phases:

a) User Acceptance Testing (UAT), Factory Acceptance Testing (FAT) and Integration Acceptance Test (IAT);

b) testing and inspection protocols;

c) quality assurance plan;

d) supplier quality assessment; and

e) supplier performance management i.e. supplier performance evaluation involves deliverables, compliance and quality, and service assurance.

8. Asset construction

The asset construction should consider several processes as illustrated in Figure 7, to ensure the assets' deliverable is completed according to the planning and design requirements. It shall be constructed in accordance with the required technical specifications and quality control in consideration of safety and environmental compliance. The activities details are described in 7.1 to 7.5.

Below is an outline of the recommended considerations for asset construction process:

a) Installation

Deploy communications infrastructure assets according to engineering specifications, safety regulations, and environmental considerations, coordinating with suppliers and stakeholders to ensure timely and efficient deployment.

b) Safety and environmental compliance

The supplier shall adhere to safety and environmental compliance which outlines standard procedures, rules, and protocols for protecting the well-being of workers and environmental impact.

c) Technical specification and quality control

Inspect incoming equipment and materials upon delivery to verify compliance with technical specifications, quality standards, and contractual requirements, rejecting non-conforming items and arranging for replacements or refunds as necessary.

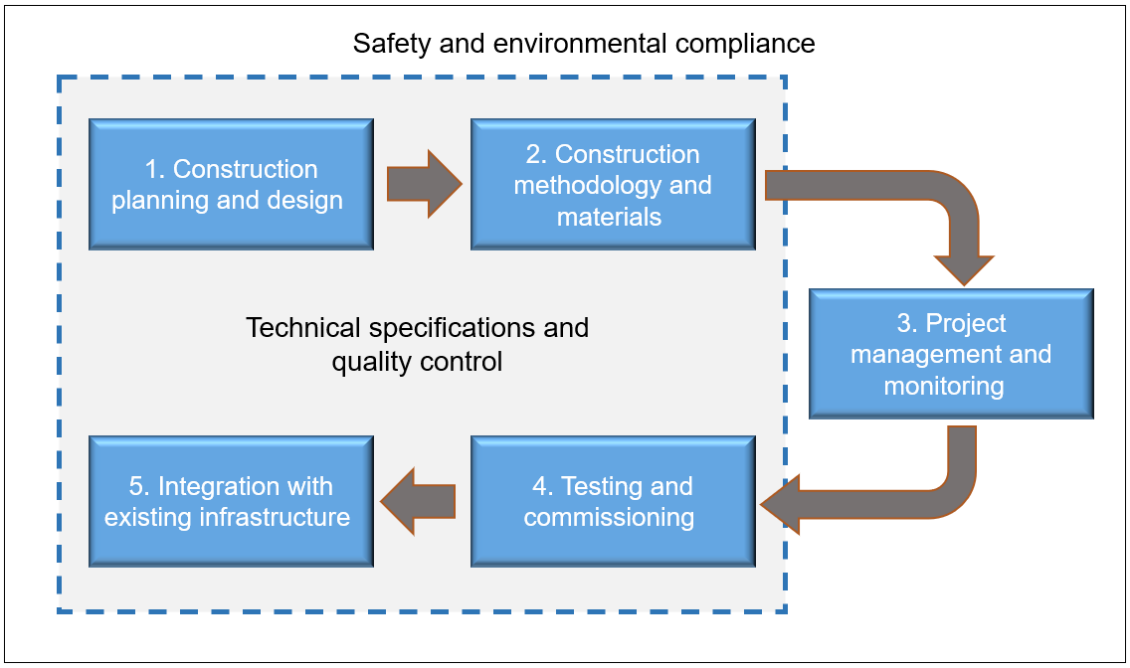

Figure 7. Asset construction process

8.1 Construction planning and design

Construction planning and design of active and passive infrastructure should include activities in preparing and executing construction projects such as below.

a) Conduct site engineering surveys to develop detailed site plans that consider asset placement, network topology, access routes, power, and future expansion requirements.

b) Mechanical and electrical design for heating, ventilation, and air conditioning for active infrastructure.

c) Prepare and submit Occupational Safety, Health, and Environment (OSHE) including environmental assessment factors, radio-frequency scanning, and potential hazards if necessary (new infrastructure).

d) Obtain necessary permits and approvals from relevant authorities, including local governments and environmental agencies.

e) The outcome of the site planning and design shall be documented.

8.2 Construction methodology and materials

The supplier should ensure effective and sustainable construction methods and materials for compliance and future reference which includes the below.

a) Selecting appropriate construction methodologies based on the type of asset, site conditions, and environmental considerations.

b) Utilising high-quality materials that comply with industry standards, ensure long-term durability, and comply with environmental regulations.

c) Implementing sustainability practices, such as energy-efficient construction techniques, use of recycled materials, and minimisation of waste.

d) The outcome of the construction methodology and materials shall be documented.

8.3 Project management and monitoring

Project management entails the application of knowledge, skills, tools, and techniques to project implementation to meet the requirements and ensure a smooth workflow progress. The following are some activities to optimise the project management workflow.

a) Develop comprehensive project plans that outline project scope, objectives, timelines, resource and budget allocation, and risk management strategies.

b) Utilise project management tools and techniques to track progress, manage resources, and promptly identify potential delays or issues.

c) Coordination with relevant stakeholders, including network operators, equipment suppliers and regulatory bodies, to ensure alignment and timely project completion.

d) Ensure effective cost management and optimisation including proper cost estimation, saving and control measures.

e) Monitor the implementation progress to ensure compliance with the project requirements, including relevant permits, local council/authority requirements, and safety.

f) The outcome of the project management and scheduling shall be documented.

8.4 Testing and commissioning

The asset supplier must ensure the effectiveness by performing necessary testing and commissioning. This is highly required to ensure all designated assets meet performance standards according to the design. Such processes or procedures include the following.

a) Conduct thorough testing and commissioning procedures to verify asset functionality, performance, and compliance with technical specifications.

b) Utilise appropriate testing equipment and methodologies to validate asset performance metrics, such as network connectivity, data transmission rates and signal strength.

c) Obtain necessary certifications and approvals from relevant authorities to ensure asset compliance and operational readiness (applicable to active).

d) Outcome of the testing and commissioning shall be documented.

8.5 Integration with existing infrastructure

Extensive interoperability testing and fact-based test cases are required especially for active assets to ensure the success of component integration which mitigates the impact or disruption to current network infrastructure to the lowest level as can be seen below.

a) Ensure seamless integration of new assets with existing communications infrastructure, including network elements, towers, and fibre optic cables.

b) Coordinate with network operators to plan and execute integration activities, minimising disruption to existing network operations.

c) Conduct thorough testing to verify interoperability and compatibility between new assets and legacy infrastructure.

9. Asset handover

Asset handover in CIAM is the formal transfer of ownership, responsibility, and accountability for a communications asset from one party (e.g., project team, contractor) to another (e.g., operations team, asset owner). This process involves detailed documentation, inspections, and knowledge transfer to ensure a smooth transition and effective ongoing management of the asset.

Below is the outline of the recommended considerations for asset handover.

a) Asset inspection

Conduct a physical inspection of the communications infrastructure assets to verify that they have been installed, configured, and tested according to the project specifications and quality standards.

b) Functional testing

Perform functional testing and validation of the assets, including connectivity tests, performance benchmarks, and user acceptance testing, to confirm that they meet operational requirements and service level agreements.

c) Formal acceptance

Obtain formal acceptance of the assets from the operation and maintenance team, acknowledging their readiness to assume responsibility for the ongoing management and maintenance of the assets.

d) Handover report

Prepare a comprehensive handover report documenting the key findings, outcomes, and recommendations from the handover process, including asset status, testing results, acceptance criteria, and any outstanding issues or action items.

The asset handover activities are shown in Figure 8 and the details are described in 9.1 to 9.8.

Figure 8. Asset handover activities

9.1 Asset documentation

Asset documentation is important as the document includes asset descriptions, asset location, serial number, purchase date, test results, operating manuals, and financial documentation such as contracts, amendments to the contracts, insurance policy, invoices and any other documents related to the asset. With complete asset documentation, asset owners can facilitate tracking and perform asset management.

The considerations of the documentation are as below.

a) Review and update asset documentation, including technical specifications, as-built documents, maintenance records and historical performance data.

b) Provide asset inventory that reflects the current state of assets, including location, condition, and configuration.

c) Prepare all relevant asset documentation in an organised and accessible format.

9.2 Asset tagging

Asset tagging is a fundamental practice in asset management, providing a unique identifier for each asset. This identifier enables efficient tracking, monitoring, and control throughout the asset's lifecycle. Below listing shows some of the common tagging methods:

a) Barcode tags

A barcode is a series of black and white lines that can be scanned by a barcode reader. Cost-effective, easy to read, and can store a limited amount of data.

b) Radio Frequency Identification (RFID) tags

RFID tags contain a small chip that emits a radio signal when activated by an RFID reader. Can be read from a distance, can store more data than barcodes, and are durable.

c) Quick Response (QR) codes

QR codes are two-dimensional barcodes that can store more information than traditional barcodes. Can be read from a distance, can store a large amount of data, and are visually appealing.

d) Laser engraving

Laser engraving involves using a laser beam to mark a permanent identifier onto an asset.

e) Etching

Etching involves using chemicals to create a permanent mark on an asset. Durable, tamper-proof, and can be customised with specific information.

f) Stamping

Stamping involves using a metal stamp to create a permanent mark on an asset. Cost-effective, easy to use, and can be customised with specific information.

9.3 Asset verification and condition assessment

It is important to ensure that the new asset owner receives the asset in the expected condition through a physical inventory checking of all assets to confirm their presence and match them with the handover documentation. The asset verification and assessment may include the following items.

a) Conduct thorough asset verification to ensure that all assets are accounted for, properly identified and in the expected condition.

b) Document any discrepancies or issues identified during asset verification and provide recommendations for corrective actions.

9.4 Training and knowledge transfer

The supplier shall arrange training and knowledge transfer to ensure the new asset owner is well-equipped with knowledge and skills on how to manage, operate, and maintain the asset, thereby ensuring operational continuity, efficiency, and safety. The following preparations are recommended to be performed.

a) Develop a comprehensive training plan to transfer the knowledge and skills related to asset operation, maintenance and troubleshooting to the owner's personnel.

b) Provide hands-on training sessions and demonstrations to ensure the owner's team is familiar with asset management procedures and practices.

c) Share relevant technical documentation, manuals, and troubleshooting resources to facilitate knowledge transfer and support ongoing asset management.

d) Record of the training and knowledge transfer is recommended to be documented for good practice.

Note: The training and knowledge transfer may not be applicable if the asset owner is well-equipped with the required skills to manage, operate, and maintain the asset.

9.5 Handover documentation and procedures

Asset handover activity by the supplier to the asset owner should be carried out to ensure a smooth transition of the information required for the asset to be used and operated according to the design and plan, such as the following items.

a) Prepare a detailed handover plan outlining the scope, responsibilities, timelines, and communications channels.

b) Establish clear handover procedures for each asset type, including asset verification, documentation transfer, training, and post-handover support.

c) Document the handover process, including acceptance by the asset owner, asset verification reports, training records and knowledge transfer materials.

d) Ensure that all relevant regulatory permits, certifications, and approvals are transferred to the owner (if applicable).

9.6 Post-handover activity and support

Preparing and transferring all relevant project information and documentation is required upon project completion. The activities after asset handover may include the following items.

a) Provide ongoing support to the asset owner during the initial post-handover period to address any concerns or issues that may arise.

b) Establish a communications channel for ongoing collaboration, knowledge exchange problem-solving and support related to asset management.

c) Conduct evaluations to determine the success and efficiency of the handover process, making improvements if necessary.

9.7 Regulatory compliance and permit transfer

Compliance with any relevant laws, standards and guidelines made by the government is a critical aspect and process for maintaining the legality, reputation, and operational integrity. The compliances may include the following items.

a) Ensure compliance with regulatory requirements related to asset operation, maintenance, and disposal.

b) Ensure regulatory compliance responsibilities are made known to the asset owner.

9.8 Data update and integrity check

It is crucial to ensure asset information’s accuracy, completeness, and reliability as it is transferred from the supplier to the asset owner. The data integrity check during handover helps the data owner understand the asset's current state and history, facilitating a smoother transition and reducing the risk of operational disruptions. The activities may include the following items.

a) Facilitation of the process of updating asset-related data in the owner's asset management system.

b) Ensuring data integrity and consistency throughout the update process to maintain accurate asset records.

c) Verification of the integrity of the data shall be done by the owner within the asset management system.

10. Asset register

The asset register is an organisation's comprehensive asset list. It provides essential details for effective asset management and decision-making. This record helps to track and monitor the assets while offering real-time insights. Below are the recommended considerations for asset register.

a) Inventory management

Comprehensive inventory of communications assets which should include network infrastructure, equipment, facilities, location, condition, and specifications.

b) Verification

Verify the accuracy and integrity of asset data by conducting periodic audits, physical inspections, and reconciliation checks to identify discrepancies or inconsistencies.

c) Data security

Implement data encryption, user authentication, and audit trail features to safeguard asset data against unauthorised access, data breaches, and cybersecurity threats.

d) Backup and recovery

Implement regular data backups and disaster recovery measures to protect asset data from loss or corruption due to hardware failures, software errors, or other unforeseen events.

e) Condition assessment

Assess the condition and performance of communications assets, using data analytics, inspections, and testing to identify maintenance needs, upgrades, or replacements.

f) Lifecycle analysis

Evaluate the lifecycle costs and benefits of communications assets, considering factors such as acquisition, operation, maintenance, and disposal costs over their lifespan.

The asset register activities are shown in Figure 9 and the details are described in 10.1 to 10.9.

Figure 9. Asset register activities

10.1 Asset identification and classification

The asset needs to be identified and classified based on its category, function, and status. The following shows the best practice on asset identification and classification.

a) Define a unique asset identification system to assign a unique identifier to each asset, ensuring traceability and preventing asset duplication.

b) Develop a comprehensive asset classification scheme that categorises assets according to network type and service (e.g. radiocommunications infrastructure, wired broadband, wireless coverage, fixed wireless/broadcast).

c) Standardise asset nomenclature and terminology to ensure consistent identification and understanding across different stakeholders.

d) Define asset data attributes that capture essential information about each asset, such as asset class, description, location, and acquired date.

e) Standardise data formats and data types for each asset attribute to facilitate data exchange and integration with other systems.

f) Consider using industry-standard asset data models to ensure data consistency and interoperability.

Figure 10 shows samples of categorisation and sub-categorisation of assets.

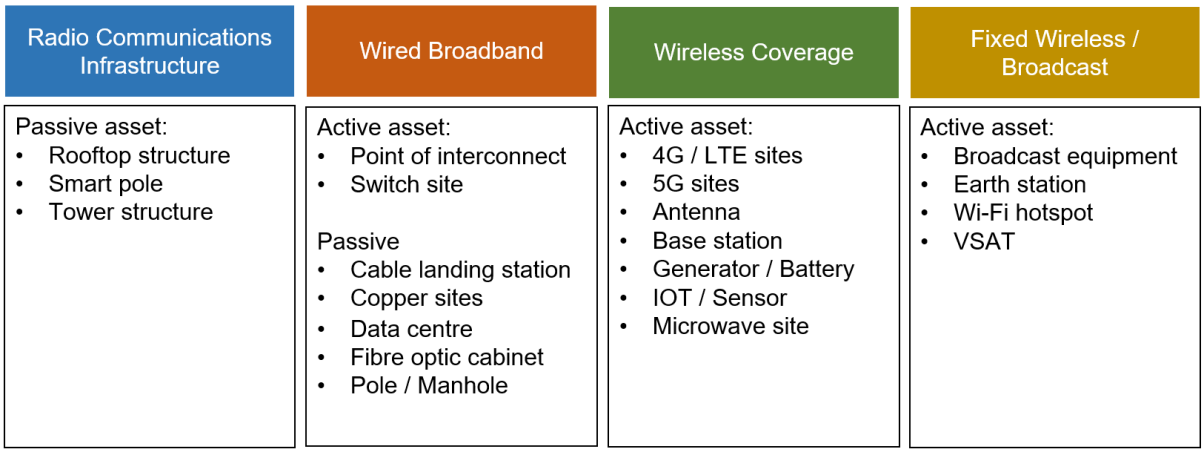

Figure 10. Samples of categorisation and sub-categorisation of asset

10.2 Asset data collection and input

The asset should be inventoried in the appropriate repository record or system based on identification and classification. The data should also be updated and cleaned periodically to ensure the accuracy and integrity of the information. The activities may include the following items.

a) Identify and integrate data sources for asset information, including procurement records, inventory records, installation reports and maintenance records.

b) Establish a centralised data repository to store and manage asset data, ensuring data integrity, accessibility, and security.

c) Implement data quality checks and cleansing procedures to ensure data accuracy, consistency, and completeness.

d) Ensure sufficient data storage to store asset inventory based on a standard data retention period.

10.3 Asset data access and security

The access to the asset data should be made in a controlled environment based on dedicated user matrix so that the security and confidentiality of the data can be monitored and traced for any leakage and unauthorised access according to ISO 27001. The following are the recommended activities to be performed.

a) Implement Role-Based Access Control (RBAC) to restrict access to asset data based on user roles and permissions.

b) Establish data security measures to protect sensitive asset information from unauthorised access, modification, or disclosure.

c) Implement data anonymisation and masking techniques to safeguard sensitive information in data when sharing with third party.

Note: ISO 27001 is a framework that sets out the requirements for an Information Security Management System (ISMS). An ISMS is a systematic approach to managing sensitive company information, including intellectual property, financial data, and personal data.

The asset data access and security best practices can be implemented as follows:

a) fulfilment of international recognised requirement;

b) systematic detection of vulnerabilities;

c) control of risks;

d) reduce the chances of security breaches within your IT environment;

e) confidentiality of the information;

f) minimisation of IT risks, possible damage, and consequential cost; and

g) a structured method to address compliance requirements.

10.4 Asset data visualisation and reporting

Asset owner is recommended to have data visualisation to ease the monitoring of the performance, and status of the asset and for the purpose of reporting to relevant stakeholders such as regulator and local authorities, which includes the following items.

a) Developing data visualisation tools and dashboards to provide insights into asset status, performance, and trends.

b) Generating comprehensive asset reports that summarise asset inventory, maintenance history, and performance metrics.

c) Integrating asset data with other business data sources to gain a holistic view of network operations and asset utilisation.

A sample of the dashboard on asset data is shown in Figure 11.

Figure 11. Sample of asset data visualisation

10.5 Asset data integration and updates

Data integration refers to the process of combining data from different sources or formats to provide end users with a unified view of information. With all different system, agency and subsidiary integrated into the single asset management system, data from disparate sources is consolidated into a single coherent asset management system as illustrated in Figure 12.

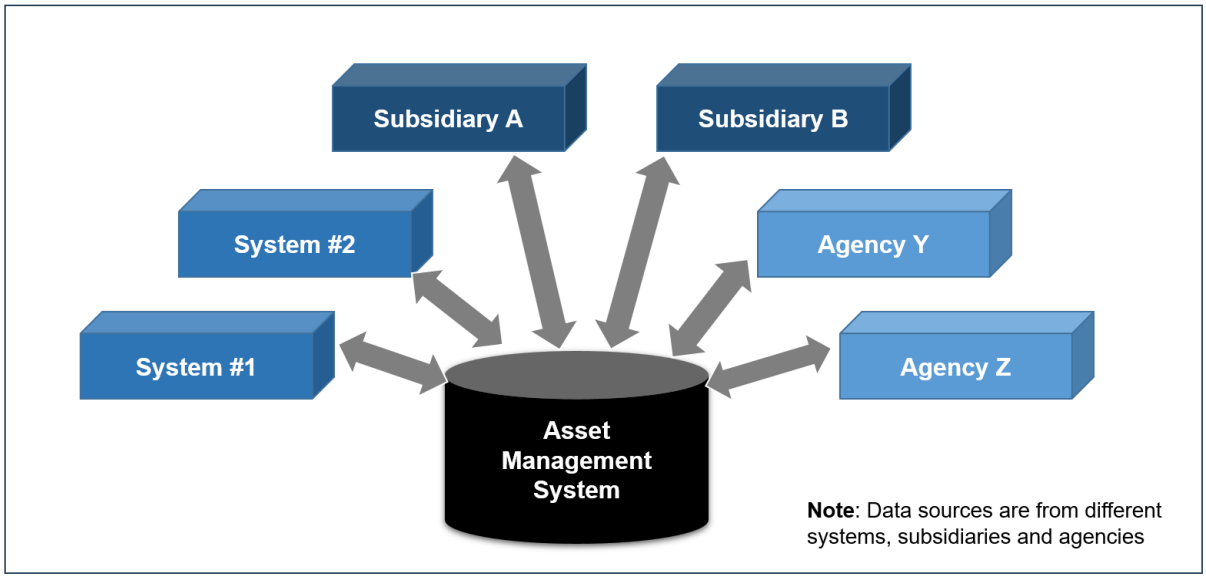

Figure 12. Data integration and exchange

Supplier and asset owner shall work together to ensure the asset data integration is done and the asset data are updated so that the information used for planning, operations, and maintenance is updated and reliable. Data integration must be consistent across all platforms to enhance overall business operations, efficiency and safety and such practices shall not be limited to below.

a) Establish data exchange protocols to integrate asset data with other communications management systems.

b) Perform data validation, cleansing and integration processes to ensure data integrity and consistency.

Asset data integration activity may also be subject to the asset's owner policy in ensuring data integrity and confidentiality across the organisation and protection from any data breach.

10.6 Asset data sharing and data exchange

It is important to ensure that the asset data owners retain control over their data and its usage while allowing data sharing or data exchange with the data recipient. Data usage control policy shall be established involving proper guidelines and standards to ensure secure, transparent, and trustworthy data transactions between multiple parties, by specifying data usage conditions, including licensing terms, data anonymisation requirements, and access restrictions, such as specifying who can access the data, under what conditions, and for what purposes. Data-sharing policy could include the following items.

a) The asset owner has an obligation to share data with the regulatory body or authority as required by relevant legislation.

b) The data owner to establish data classification and access controls, granting rights only to authorised personnel based on the data's sensitivity (e.g., restricted, confidential, public). These controls shall be underpinned by formal legal agreements with all relevant parties, explicitly outlining data protection measures, usage terms, liability, and agreement termination clauses.

c) Deploy necessary technology infrastructure and information security policy to support secure data-sharing.

d) Provide stakeholders with training on data-sharing policies and best practices.

e) Continuous monitoring of data-sharing activities to ensure compliance with relevant acts, regulations, policies, or/and obligations.

10.7 Asset data audit and validation

An asset data audit and validation are critical for ensuring asset information’s integrity, accuracy, and reliability. Validating asset data helps identify discrepancies, outdated information, and potential errors. Correcting these issues enhances operational efficiency by ensuring that maintenance schedules, resource allocation, and operational planning are based on accurate data. Best practices can be as the following items.

a) Conduct regular asset data audits to verify data accuracy, completeness, and consistency.

b) Implement data quality checks and validation rules to identify and resolve data anomalies or discrepancies.

c) Reconcile asset data with physical asset inventories to ensure data accuracy and prevent asset discrepancies.

d) Outcome of the asset data audit and validation shall be documented into any system implemented by the organisation (e.g. asset data management system).

In many cases, the asset owner had already decommissioned the physical asset on the ground, but it has not been removed or updated in the inventory system. This situation may lead to inaccurate asset records and affect several operational activities such as maintenance plan of the assets.

10.8 Asset data archiving and disposal

Regularly disposing of Redundant, Obsolete, or Trivial (ROT) data ensures that only valuable and necessary information is retained. This practice supports effective data governance and ensures that data management policies are upheld, which are not limited to the following items.

a) Establish data archiving policies and procedures to preserve asset data for historical and compliance purposes.

b) Implement data disposal procedures to securely dispose of outdated or sensitive asset data in accordance with regulatory requirements.

c) Maintain data retention policies to ensure compliance with legal and regulatory obligations related to data retention and disposal.

10.9 Asset ownership transfer

Current asset owner shall be responsible for the asset ownership transfer in the event of merging, splitting, buying over, or dissolving the company's asset. The new asset owner shall be responsible for all the activities involved in asset management framework.

11. Operation and Maintenance (O&M)

Operation and maintenance (O&M) involve the management of network assets to ensure optimal performance, reliability, and service delivery. There are 2 aspects under O&M, namely execution and performance monitoring as shown in Figure 13.

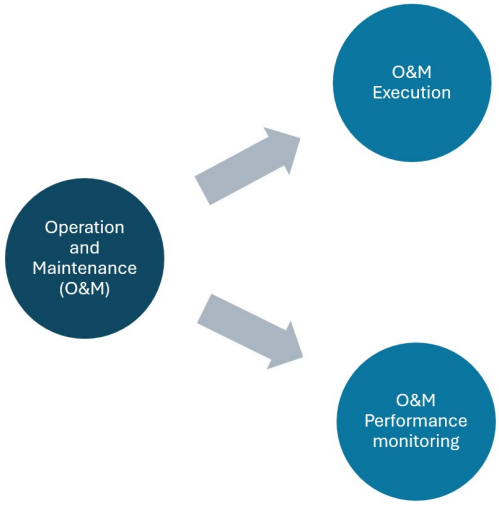

Figure 13. Operation and Maintenance (O&M) aspects

O&M execution is the practical application of maintenance plans to keep assets functioning optimally, while O&M performance monitoring measures how effective these actions are in achieving the desired outcomes.

The activities include monitoring, troubleshooting, repairing, upgrading, and replacing equipment, and managing network resources efficiently.

11.1 Operation and Maintenance (O&M) execution

Figure 14 illustrates the key activities of O&M execution, to ensure optimal performance. These activities include planning and scheduling maintenance tasks, executing different maintenance types, managing external suppliers, preparing for and responding to disasters, and ensuring compliance with regulations.

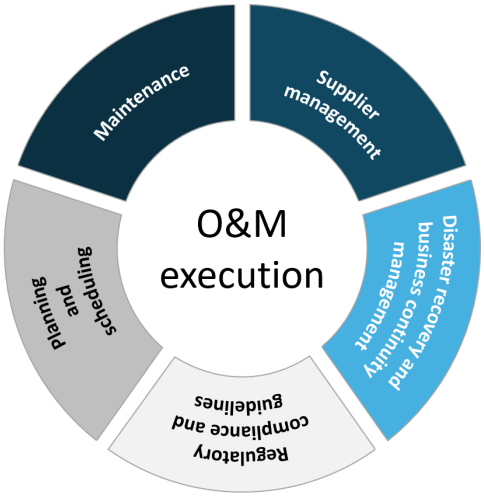

Figure 14. Operation and Maintenance (O&M) execution activities

11.1.1 Planning and scheduling

O&M planning involves the strategic organisation and scheduling of activities to ensure the efficient functioning and longevity of communications infrastructure, which comprise the following but are not limited to:

a) Contractual agreements

Asset owner shall establish long-term O&M contracts with a suitable, consistent, and experienced suppliers to ensure all active and passive asset always in good working order, which comprise the following but not limited to:

i) terms and conditions;

ii) asset inventory list;

iii) scope of service;

iv) service scheduling matrix;

v) rate/cost of service;

vi) safety procedure; and/or

vii) supplier performance consequence.

b) Asset inventory

The asset owner should maintain a detailed inventory to track asset condition, performance, and maintenance history. This information supports informed decisions on upgrades, repairs, or replacements to optimise resource allocation.

The inventory list should at least consist of the following items:

i) asset reference;

ii) asset description;

iii) current value;

iv) location (e.g. address and coordinate);

v) asset performance, history and condition; and/or

vi) asset maintenance manuals, records and schedules.

The asset owner should prepare the inventory list using the appropriate format. A sample of inventory format is provided in Annex C.

The asset owner should ensure that management of change in place by updating asset inventory in the regulatory asset management database.

11.1.2 Maintenance

Regular maintenance ensures that communications networks operate at optimal levels consistently resulting in more reliable and high-performing networks, reducing service disruptions, enhancing customer satisfaction, and extending the assets' lifespan.

Maintenance activities are categorised into 3 types as follows:

a) preventive;

b) corrective; and

c) predictive.

11.1.2.1 Preventive maintenance

Preventive maintenance involves regularly scheduled inspections and maintenance tasks to keep assets functioning properly and prevent unexpected breakdowns. The key activities in preventive maintenance consist of the following but not limited to the following items.

a) Periodic checks of physical and condition of communications infrastructure (e.g. Condition assessment).

b) Periodic updates of firmware and software to patch security vulnerabilities and improve performance. Updating network management and security software.

c) Testing and calibrating software and hardware of communications infrastructure.

d) Record and update the preventive maintenance activities.

The sample of preventive maintenance is provided in Annex D.

11.1.2.2 Corrective maintenance

Corrective maintenance is a type of maintenance that is performed after a failure or breakdown has occurred to restore a system or component to its original working condition. The key activities in corrective maintenance consist of the following but are not limited to:

a) Identification and analysis of the cause of faults using diagnostic tools and physical inspections to determine the necessary repairs, upgrades and/or replace.

b) Adjustment of system settings or software configurations to correct errors and optimise performance.

c) Quickly assess and address urgent issues to minimise service disruption and restore normal operations.

The sample of corrective maintenance is provided in Annex E.

11.1.2.3 Predictive maintenance

Predictive maintenance utilises data analytics (historical data and real-time performance metrics) to predict potential equipment failures based on patterns and trends to optimise equipment performance and prevent downtime.

The key activities for predictive maintenance consist of the following but are not limited to the following items.

a) Collect data from current and historical records; gathering data from sensors, monitoring devices, and equipment logs to track performance metrics such as temperature, vibration, and power usage.

b) Continuously monitor key indicators to detect anomalies or deviations from normal operating conditions.

c) Use data analytics tools (e.g. Machine Learning, Artificial Intelligence) and algorithms to analyse historical data and identify patterns or trends that may indicate impending failures or deterioration.

The sample of predictive maintenance and the sample of use cases for predictive maintenance are provided in Annex F.

11.1.3 Supplier management

Managing suppliers is crucial for the seamless operation of communications services. Key strategies such as supplier selection, contract negotiation, and supplier performance management must be implemented to effectively manage suppliers.

The following steps ensure the successful delivery of communications services and operations, helping organisations to effectively select and manage suppliers:

a) assess supplier capabilities;

b) review supplier reputation;

c) cost consideration;

d) evaluate support services; and

e) supplier performance monitoring.

11.1.4 Disaster recovery and business continuity management

Disaster recovery for communications network operations involves preparing for and mitigating the impact of various disasters and/or disruptions of service that could affect the availability, integrity, and confidentiality of network activities as well as the continuity and profitability of the organisation.

Assets affected by disasters may eventually impact the organisation’s business operations. Depending on the impacts caused, the organisation may incur losses. To mitigate these scenarios, organisations should prepare a business continuity plan by referring to the technical code MCMC MTSFB TC G014.

Figure G.1 in Annex G illustrates disaster recovery and Business Continuity Management (BCM) cycle sample.

11.1.4.1 Risk assessment and business impact analysis

Organisations should identify in advance potential risks and threats that could disrupt network operations, such as natural disasters (e.g., earthquakes, hurricanes), cyber-attacks, equipment failures, power outages, and human errors by conducting a thorough risk assessment to prioritise risks based on their likelihood and potential impact, both in the infrastructure and ultimately in the business.

Business Impact Analysis (BIA) assesses the potential consequences of network disruptions on business operations, including financial losses, productivity impacts, regulatory compliance issues, and damage to reputation.

Identify critical network assets, services, and dependencies that need to be prioritised for recovery.

11.1.4.2 Types of disasters

Disasters in disaster recovery and business continuity management encompass a wide range of natural and human-made threats, that can disrupt business operations. Table 4 shows the non-exhaustive list that could trigger a disaster recovery procedure.

Table 4. Types of disasters

Type of disaster	Description
Hardware failures	Hardware failures, such as router or switch malfunctions, server crashes, or cable faults, can disrupt network connectivity and services.
Software failures	Software failures, including operating system crashes, application bugs, or misconfigurations, can cause network services to become unavailable or unstable.
Network congestion	Network congestion occurs when there is excessive traffic on a network segment, leading to degraded performance, packet loss, and latency issues.
Power outages	Power outages or electrical disturbances can disrupt network operations causing network devices, servers, and infrastructure components to lose power.
Natural disasters	Natural disasters such as earthquakes, hurricanes, floods, wildfires, or severe weather events can damage network infrastructure, facilities, and communications lines, leading to service outages.

Effective disaster recovery and business continuity plans must be able to avoid these potential threats to ensure the assets remain in good condition in delivering the required quality of service.

11.1.4.3 Disaster recovery planning

Disaster recovery begins with adequate planning that should include the following steps, in accordance with MCMC MTSFB TC G014.

a) Defining recovery objectives and priorities based on risk assessment and business impact analysis by determining acceptable downtimes, data loss tolerances, and service level agreements or different network services and applications.

b) Implementing robust backups and data protection mechanisms to ensure the availability and integrity of critical network data and configurations.

c) Ensuring high resiliency by designing the network architecture with built-in redundancies and failover mechanisms to minimise the impact of hardware failures, link outages, and other disruptions.

d) Preparing a disaster recovery site, should be geographically separate from the primary site to mitigate regional risks and equipped with redundant infrastructure, backup systems, and connectivity to support rapid recovery of network operations.

e) Documenting detailed Incident Response and Recovery Procedures to guide network operations staff in responding to disasters and restoring services quickly and efficiently, including roles and responsibilities, escalation paths, and communications protocols for different phases of the recovery process.

f) Performing training and simulation exercises routinely to ensure that the network operations staff is intimately familiar with all the necessary procedures to bring back the asset from a state of recovery to fully operational.

11.1.4.4 Incident response

The organisations' response to a disaster will be determined by their ability to prepare for the eventuality and quickly detect, react and remediate the situation and bring the impacted assets back to being fully operational. In general, the response should observe the following steps:

a) Detecting the disaster as early as possible, failure of which may increase the likelihood of reaching the Minimum Business Continuity Objective (MBCO).

b) Executing a continuous technical assessment of the situation based on the organisation's recovery planning both during the recovery phase and once operations have been restored successfully to ensure a full recovery.

c) Executing an assessment of the business standing through the organisation's BIA, which may need to continue once operations have been restored successfully to ensure that the business is back to being profitable and observing any potential regulatory risks to be addressed.

d) Collecting all relevant data from the incident to generate the necessary reporting that should be used to further optimise the organisation's response and recovery procedures.

11.1.5 Regulatory compliance and guidelines

Regulatory compliance is the adherence to laws, regulations, standards, and guidelines set forth by local authorities. It ensures businesses operate ethically, protect stakeholders, and avoid legal and financial penalties. Compliance is crucial for maintaining trust, reputation, and market access.

O&M operators should comply to the regulations and guidelines summarise in the Table 5.

Table 5. List of regulations and guidelines

Instruments	Description
Environmental Quality Act 1974	a) Ensures O&M practices to comply when generating waste and handling potentially hazardous materials, b) Supports O&M practices in identifying potential environmental consequences to facilitate compliance with Environmental Impact Assessment (EIA) requirements mandated by regulatory authorities.
OSHA	Mandates a safe working environment for O&M personnel, requiring adherence to health and safety standards for activities such as working at heights (e.g., cell towers), electrical safety, and handling heavy equipment
MCMC MTSFB TC G009	a) Protects sensitive data, which is critical for O&M activities that involve handling customer information and network configurations. c) Enhances operational resilience and mitigates security threats that could disrupt O&M and communications infrastructure operations.

Table 5. List of regulations and guidelines *(continued)*

Instruments	Description
MCMC MTSFB TC G014	a) Assists O&M service providers in identifying areas that need improvement. b) Implement proactive maintenance practices to minimise the risk of non-compliance issues during audits by authority bodies. c) Provides a framework for what to expect during a compliance audit by an authority body, which also assists O&M service providers to prepare relevant documentation.
ISO 9001	Ensures consistent O&M quality, improves customer satisfaction, and promotes a culture of continuous improvement.
ISO 14001	a) Reduces environmental footprint, which O&M activities can generate waste (e.g., from equipment maintenance) and consume resources (e.g., energy for powering infrastructure). b) Optimises processes to minimise environmental impact.
Standard Radio System Plan (SRSP)	a) Sets the mandatory technical requirements for radio frequency usage, ensuring O&M activities (e.g., cell site deployment, equipment swap-outs) comply with regulatory specifications regarding frequency bands, power limits, antenna characteristics, and co-existence with other systems. b) Ensuring the network operates efficiently and minimises radio interference to other licensees and services.
ST guidelines	Governs the safe operation and maintenance of electrical systems, ensuring O&M activities adhere to safety standards for power supply and distribution within communications sites and infrastructure.

In some other cases or matters, O&M operators may refer to the specific contract, Service Level Agreement (SLA), or other definitive agreements (if applicable) for additional compliance requirements.

11.2 Operation and Maintenance (O&M) performance monitoring

Performance monitoring and reporting involves tracking network assets' efficiency, reliability, and overall health. It includes collecting data, analysing performance metrics, generating reports, and using insights to optimise asset utilisation, reduce costs, and improve service quality.

Below is the outline of the recommended asset performance monitoring and reporting process:

a) Assessment

Monitor key performance indicators (KPIs) for telecom infrastructure assets, including network uptime, service availability, response times, and customer satisfaction metrics.

b) Performance reporting

Generate regular performance reports and dashboards to communicate asset performance, maintenance activities, and service delivery metrics to stakeholders, enabling informed decision-making and accountability.

c) Gap identification

Benchmark telecom infrastructure performance against industry standards, best practices, and peer comparisons to identify areas for improvement and drive continuous performance enhancement.

The following 8 components of performance monitoring provide a systematic approach designed for transforming operational data into actionable business intelligence. By evolving from static KPIs to dynamic processes like real-time monitoring and trend analysis, organisations can more effectively diagnose failures through Root Cause Analysis (RCA). This shift enables proactive capacity planning, ensuring sustained optimisation and the delivery of superior customer value.

11.2.1 Key performance indicators (KPIs)

Key Performance Indicators (KPIs) for a communications infrastructure organisation should cover the following main areas:

a) Asset management

Ensuring assets are correctly categorised in accordance with regulatory guidelines.

b) Financial performance

Tracking revenue, subscriber growth, and profitability.

c) Customer experience

Measuring customer satisfaction and service quality.

Benchmarking is the process of comparing an organisation's KPIs to industry standards or best practices. It provides valuable insights into areas where improvements can be made to enhance efficiency, effectiveness, and overall performance.

By comparing KPIs within each area to industry benchmarks, organisations can identify strengths, weaknesses, and opportunities for improvement.

The key benchmarking areas below provide a comprehensive framework for assessing the performance of an organisation.

a) Financial metrics measure the financial health and performance.

b) Network metrics assess the quality and performance of the network infrastructure.

c) Customer experience metrics evaluate customer satisfaction and loyalty.

d) Operational efficiency metrics measure the effectiveness of internal processes and resource utilisation.

e) Innovation metrics gauge the organisation's ability to develop and implement new technologies and services.

11.2.2 Real-time monitoring and visualisation

Real-time monitoring and visualisation play a crucial role in ensuring smooth network operation, optimising resource allocation, and enhancing user experience.

The key aspect for real-time monitoring and visualisation to be considered as listed in Table 6 below but not limited to.

Table 6. Key aspect for real-time monitoring and visualisation

Aspect	Items
Key components	a) Data collection b) Data processing and analysis c) Visualisation tools d) Alerting and notification systems
Specific monitoring areas	a) Network performance b) Traffic patterns c) User behaviour d) Resource utilisation e) Service quality
Visualisation techniques	a) Dashboards b) Geolocation maps c) Network topology maps d) Heatmaps e) Real-time data streams
Industry trends	a) Machine learning (ML) and Artificial Intelligent (AI) b) Cloud-based monitoring c) Network Function Virtualisation (NFV) e) 5G network monitoring

11.2.3 Trend analysis and anomaly detection

Trend analysis and anomaly detection are complementary tools for understanding network and customer behaviour.

Trend analysis helps to understand the usual patterns, and anomaly detection helps to spot when things go off track. Table 7 indicates the difference between trend analysis and anomaly detection.

Table 7. The difference between trend analysis and anomaly detection.

Tool	Description
Trend analysis	Studies historical data on network performance, traffic patterns, and customer behaviour to understand usual patterns and predict future trends. (e.g. call volume, data usage, churn rates)
Anomaly detection	Identifies unusual events that deviate from established trends, potentially indicating issues. (e.g. sudden call drops, suspicious traffic patterns, customer support spikes)

By combining trend analysis and anomaly detection, organisations can better understand their networks and customers, enabling them to make more informed decisions and proactively address issues.

11.2.4 Reporting

Reporting is crucial to ensuring transparency, data-driven decision-making, and operational efficiency. It involves gathering, analysing, and presenting key performance indicators (KPIs) and other relevant information to various stakeholders. The data will report on the following:

a) network performance metrics (call success rates, data transfer speeds, latency);

b) traffic patterns (usage trends, peak hours, geographic distribution);

c) service quality (customer complaints, service availability); and

d) resource utilisation (bandwidth usage, equipment performance).

11.2.5 Root Cause Analysis (RCA)

Root Cause Analysis (RCA) plays a crucial role in ensuring smooth network operation, minimising downtime, and enhancing customer experience. Through the RCA, the underlying factors causing network issues, service disruptions, and customer complaints can be identified.

Effective communications RCA requires a combination of technical expertise, analytical skills, and a systematic approach as follows:

a) utilise structured frameworks to identify the root cause;

b) analyse network data, user logs, and customer reports;

c) involve technical experts from diverse areas (e.g. network operations, security, software development);

d) consider both technical and non-technical factors; and

e) conduct thorough investigations to identify the true root cause.

11.2.6 Continuous improvement and innovation

Continuous improvement involves ongoing effort to produce better network performance, products, services, and processes, deliver a better user experience and achieve greater efficiency. This process is repeated for the betterment of output after taking into consideration input such as customer feedback and market trends, as shown in Figure 15. Continuous improvement involves identifying problems, figuring out solutions, testing, and making them a standard if they work.

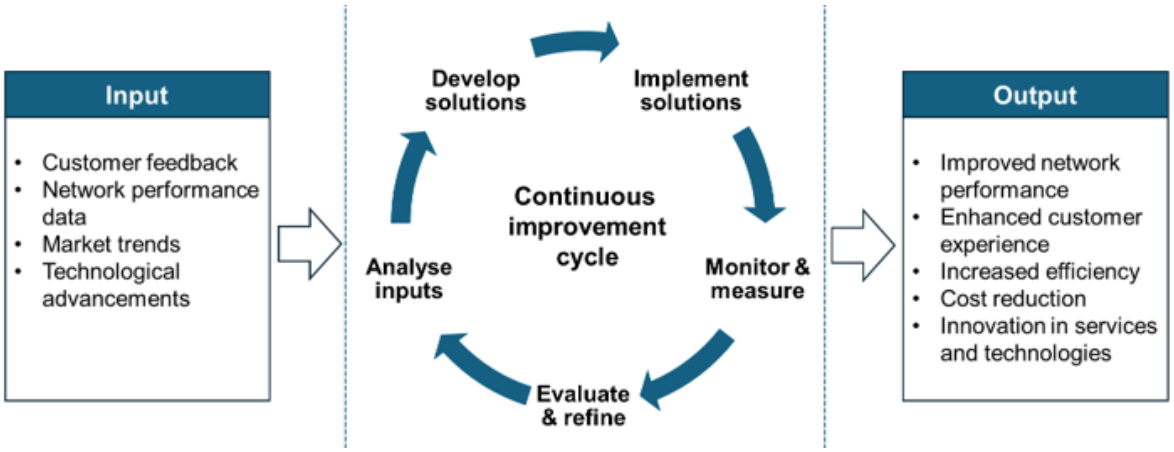

Figure 15. Continuous improvement activities

11.2.7 Optimisation

Optimisation encompasses many strategies and techniques to improve network performance, resource utilisation, and overall customer experience. Table 8 describes type of optimisation.

Table 8. Type of optimisation

Type of optimisation	Description
Network	a) Capacity management (dynamic resource allocation) b) Radio network optimisation (antenna configuration, cell size adjustment) c) SDN (automated configuration, traffic routing) d) Network function virtualisation (improved scalability, resource utilisation)
Resource	a) Power management (energy-efficient technologies) b) Spectrum management (utilising underused resources) c) Infrastructure optimisation (site consolidation, capacity upgrades)
Customer experience	a) Quality of service (prioritising bandwidth for critical applications) b) Content delivery network (caching content for faster loading) c) Personalisation (tailoring services based on user preferences) d) Proactive service management (identifying and addressing potential issues) additional considerations: e) Security optimisation (robust security measures) f) Data analytics (data-driven insights for decision-making) g) Collaboration (cross-functional teams for alignment)

11.2.8 Capacity planning

Capacity planning helps to navigate this challenge by ensuring sufficient resources are available to support seamless user experiences, avoid service disruptions, and optimise costs. The capacity planning best practice that can be used are structured approach, data analytics, collaboration with diverse stakeholders and continuous monitoring. Key activities of capacity planning consist of the following:

a) Demand forecasting

Analyse historical data, traffic trends, and emerging technologies to predict future needs.

b) Resource assessment

Evaluate current network capacity (bandwidth, processing power, storage) to identify bottlenecks.

c) Technology considerations

Factor in the impact of new technologies (5G, IoT, edge computing) on network demands.

a) Cost optimisation

Balance capacity needs with budget constraints through dynamic resource allocation and virtualisation.

b) Risk management

Proactively identify and address potential risks (traffic spikes, disasters, security breaches).

12. Asset upgrading and refurbishment

Upgrading and refurbishment activities involve improving existing asset conditions to extend lifespan, enhance performance, and align with evolving technological demands. Organisations can optimise asset utilisation, reduce operational costs, and maintain service quality by strategically investing in these activities.

Below are the recommendations on asset upgrading and refurbishment.

a) Future requirement planning

Forecast future demand for telecom services and infrastructure capacity requirements, conducting capacity planning exercises to anticipate growth, congestion, and scalability needs.

b) Technology upgrades

Implement technology upgrades and modernisation initiatives to enhance communications infrastructure assets' performance, reliability, and efficiency, such as upgrading to 5G networks or deploying fibre optic cables.

c) Efficiency improvements

Identify efficiency improvements and cost savings opportunities through optimisation measures, such as network consolidation, spectrum re-farming, and energy efficiency initiatives.

Figure 16 represents the activity of upgrading and refurbishing of the asset. The details are described in 12.1 to 12.5.

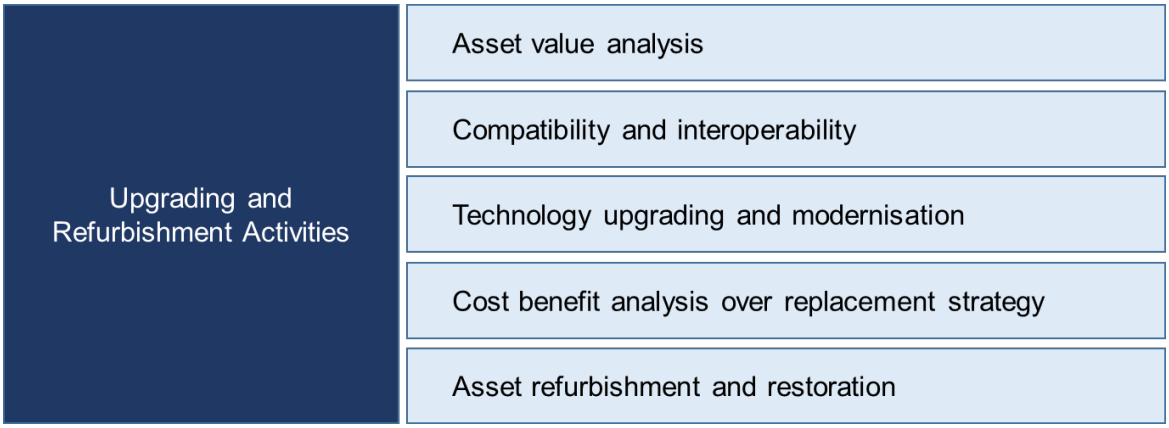

Figure 16. Upgrading and refurbishment activities

12.1 Asset value analysis

Asset value analysis is a comprehensive process of determining the current worth of an asset or a group of assets. It involves evaluating few considerations to assess the asset's fair market value or its contribution to the overall business as described in Table 9.

Table 9. Key considerations for asset value analysis

Key consideration	Description
Asset depreciation	The amount of the asset's value that has been used and depreciated over its useful life.
Asset useful life	The asset life extension evaluation aims to demonstrate that by extending the asset's life, the owner is not exposing the community surrounding the asset in the study to unacceptable risk in line with applicable international codes, standards, and best industrial practices.

In asset planning, useful life refers to the period during which an asset is expected to be effective and functional. It's the time span over which an asset can perform its intended function efficiently before it needs to be replaced or upgraded. This concept helps in planning the maintenance, replacement, and financial budgeting.

Organisations can make informed decisions, optimise resource allocation, and manage their assets by conducting through asset value analysis.

12.2 Technology upgrading and modernisation

Technology upgrading and modernisation involves replacing or improving outdated systems and processes with newer, more efficient ones. It's about staying current with technological advancements to enhance productivity, efficiency, and competitiveness.

It is the process of aligning a business or system with the latest technology standards.

The asset owner should consider upgrading technology and modernising as described in Table 10.

Table 10. Key considerations for technology upgrading and modernisation

Key considerations	Description
Technology screening	Evaluating available technologies to meet project requirements. It can be done for strategic positioning or solving operational issues.
Technology maturity	It refers to a technology's development stage. Mature technologies have been around long enough to have most bugs ironed out. Technology Readiness Levels (TRLs) are used to assess maturity.
Local support for the technology	Ensuring chosen technology has local support for maintenance throughout its lifecycle. Original Equipment Manufacturers (OEM) should train local supplier
Upskilling the workforce to adopt the technology - competency	Training the employees on the new technology before deployment. Activities like POC testbeds can provide hands-on experience.
Compatibility and interoperability	Ensuring that new systems and components can work seamlessly with existing infrastructure, preventing disruptions, and maximising the benefits of the upgrade. Details is in section 13.4.

12.3 Asset refurbishment and restoration

Asset refurbishment and restoration is the process of bringing an old or damaged asset back to a functional and often like-new condition. It involves repairing, cleaning, upgrading, and testing to extend the asset's lifespan and improve its performance.

The asset owner should consider asset refurbishment and restoration as described in Table 11.

Table 11. Key considerations for asset refurbishment and restoration

Key considerations	Proposed Action / Methodology
Assessment of the asset refurbishment	Identify items suitable for refurbishment by conducting an economic assessment including: a) Deterministic decision model with its basis b) Screening criteria for alternatives c) Business operating model alternatives d) Regulatory requirements (taxes, incentives) e) Cost-Benefit Analysis (CBA)
Warehousing	Identify storage for refurbished assets. Warehouses should have: a) Storage areas b) Loading docks c) Conveyors d) Material handling equipment - Air-conditioned rooms for sensitive assets (electronics part)
Asset inventory	a) tracking movement in and out of warehouses b) mitigate risks of theft, loss, obsolescence, or misplacement
Certification of fitness - Professional Engineer (PE) endorsement and verification	Obtain verification and approval from a PE to ensure: a) Refurbishment meets original plans b) Safe refurbishment c) Fitness for use - Submit supporting documents from relevant safety and regulatory bodies
Support warranty	Obtain a warranty from the supplier/OEM covering: a) Performance according to the intended function b) Freedom from material defects - coverage for a stipulated warranty period

12.4 Compatibility and interoperability

Compatibility and interoperability refer to the ability of different systems, devices, or software to work together seamlessly.

The asset owner should consider the compatibility and interoperability of assets as per Table 12.

Table 12. Key considerations for compatibility and interoperability

Key considerations	Description
Compatibility	A functional unit can meet interface requirements without modification. For active component replacement assets to be replaced must be compatible with existing parts, for example using industrial standards-based protocols for data exchange between different communications equipment (regardless of supplier).
Interoperability	Ability of two or more systems to exchange and use information. Example: verify compatibility between new software/firmware versions and existing versions.

12.5 Cost - Benefit Analysis (CBA) and replacement strategy

The Cost-Benefit Analysis (CBA) will be conducted with an over-replacement strategy to guarantee analytical rigor and optimise company value. This evaluation will comprehensively consider the following parameters:

a) expenditure;

b) ease of maintenance;

c) security;

d) technological needs;

e) potential hazards;

f) compliance obligations;

g) operational framework; and

h) geographic considerations.

13. Asset Disposal

Effective asset disposal is critical to organisational asset management, ensuring that outdated, used, or surplus assets are handled responsibly. Compliance with regulations and adopting environmentally sound waste management practices are essential for handling and disposing of affected materials. At the same time, organisations can mitigate their ecological footprint, enhance sustainability efforts, and protect ecosystems.

This section focuses on pre-disposal, disposal, Standard Operating Procedures (SOP) for Schedule Waste (SW) management and safety, training, and monitoring to highlight the best practices and strategies for sustainable waste handling.

Below is the outline of the recommended asset disposal process:

a) Condition assessment

Evaluate the condition and usability of assets slated for disposal, considering physical condition, functionality, and technological obsolescence factors.

b) Legal and regulatory requirements

Ensure compliance with relevant regulations governing the disposal of electronic and communications equipment, including environmental, health, and safety regulations.

c) Data security

Implement data sanitisation procedures to securely erase or destroy sensitive data stored on decommissioned assets, following industry best practices and data protection regulations.

d) Environmental impact assessment

Assess the environmental impact of disposal activities, such as energy consumption, greenhouse gas emissions, and waste generation, and implement measures to minimise environmental harm and promote sustainability.

13.1 Pre-disposal

Before disposal, every asset shall have complete documentation and approval by an authorised person or committee to meet the organisation's internal control and statutory reporting requirement. This process may differ among organisations, but it usually involves identifying and evaluating the asset for disposal and retiring the asset. The main activities are but are not limited to the following items.

a) Identify, evaluate, and dispose of assets meeting asset retirement criteria.

b) Ensure proper approval and documentation for asset retirement, including endorsed asset retirement forms, asset retirement notifications, and visual records.

c) Comply with data retention policy to save useful data, and securely erase data from the storage device to be disposed of, ensuring that the data cannot be recovered.

d) Apply accounting treatment according to financial reporting standards and accurately reflected in the respective company's financial record.

e) Minimise company losses and maximise recoverable value from asset disposal.

Development and operation of communications infrastructure may result in the generation of solid waste, typically divided into two categories: hazardous (scheduled waste) and general waste (non-hazardous), as shown Figure 17.

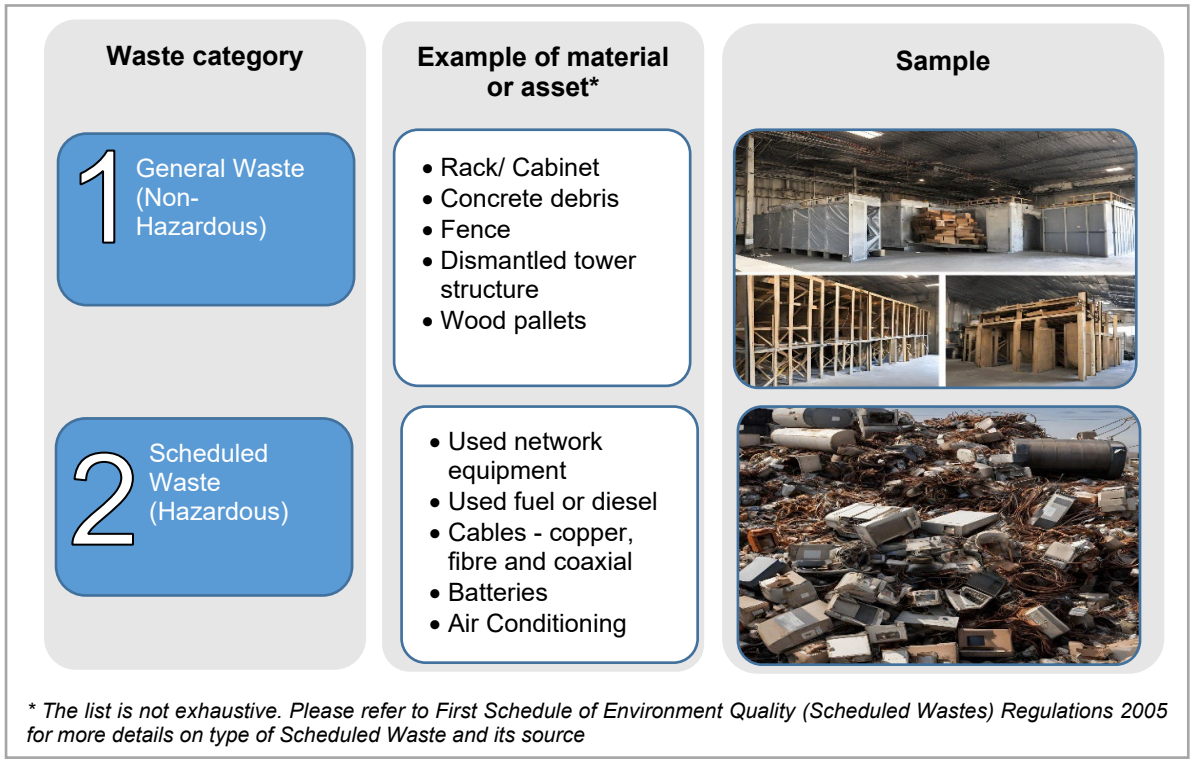

Figure 17. Waste category

13.1.1 Asset identification and evaluation

The identification and evaluation of assets that no longer contribute to future economic benefits to organisation. This may cover asset classification based on the categories below:

a) fully destroyed, physically damaged or incomplete equipment or material;

b) physical obsolescence or technology obsolescence; and

c) management or government directive.

This asset classification may determine to ensure an appropriate treatment of the asset to be disposed as the details in 13.2.

13.1.2 Asset retirement process

Asset retirement process shall be performed to ensure that the assets are systematically retired and disposed of while adhering to organisational policies and/or legal requirements. This process may vary from one organisation to another and provides an overall process of asset retirement from the point of asset retirement proposal until physical disposal action.

This is to ensure that the asset retirement is being captured and accounted for correctly in the financial statement and that physical asset disposal is being done in a timely manner. The organisation shall update the approved asset to be disposed of in the relevant asset registry (internal and/or external platform). The external platform can be from regulatory and/or authority bodies.

13.2 Disposal

A good and responsible company should minimise its environmental impact while maximising recoverable value from asset disposal. This includes:

a) Sustainable practices

Emphasize waste Reduction, Recycling, and Reuse (3R) to minimise environmental impact and preserve the ecosystem.

b) Sustainable disposal practices

Implement methods that prevent pollution, conserve resources, and protect ecosystems.

c) Circular economy

Incorporate the practice of reducing, reusing, recycling, and recovering to enhance sustainability and economic outcomes.

d) Waste handling evaluation

Assess proper waste handling and treatment options in compliance with environmental laws and regulations.

e) Method-Specific Disposal

Determine the disposal method, which can be in form of the following, as per Figure 18.

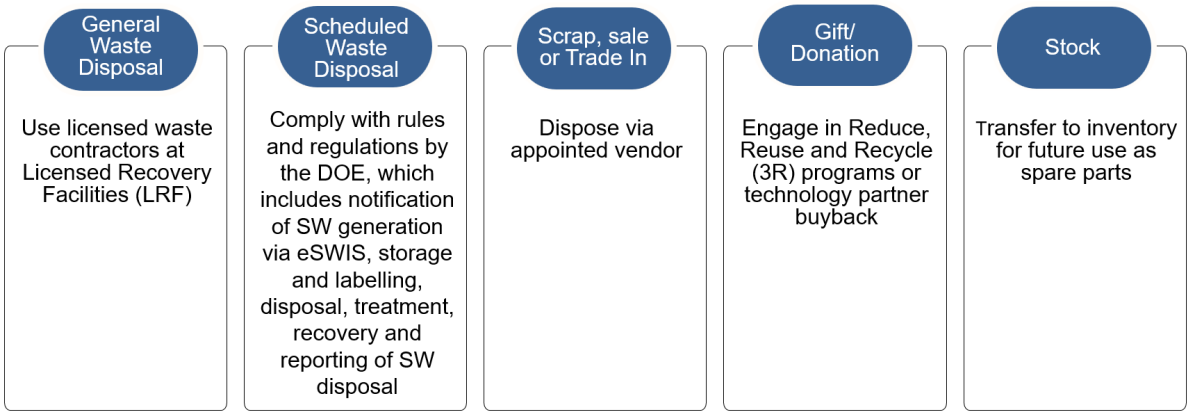

Figure 18. Common method of disposal

Figure 19 shows the general practice of asset disposal.

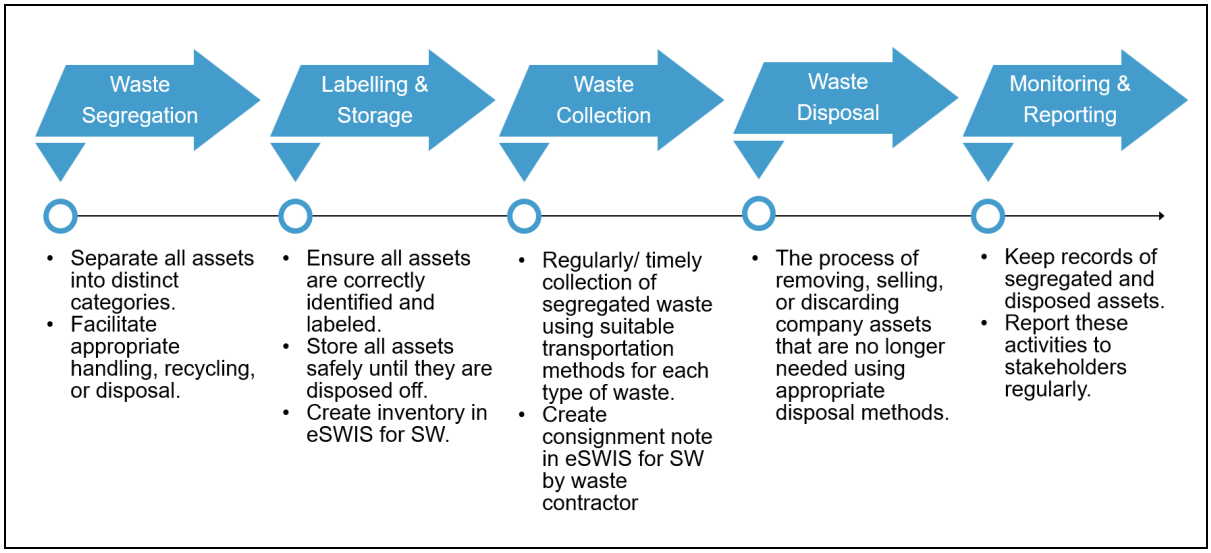

Figure 19. General practice of asset disposal

The general practice of asset disposal helps organisations to handle, manage and dispose of solid waste according to the relevant laws, regulations, and guidelines. It protects the organisation from potential legal liabilities and enhances operational efficiency and financial performance.

13.3 Standard Operating Procedures (SOP) for Schedule Waste (SW) Management

The details on SW management Standard Operating procedures (SOP), related guidelines and required compliance shall be referred to in the Environmental Quality Act 1974, Environmental Quality (Scheduled Wastes) Regulations 2005 and Guidelines for Packaging, Labelling and Storage of Scheduled Wastes in Malaysia.

To ensure the safe and environmentally sound management of scheduled waste and minimise environmental impact and health risks associated with scheduled waste management, it is imperative to adhere to the relevant procedures.

13.3.1 Categories of Scheduled Waste (SW)

Scheduled waste is classified into different categories based on its composition and potential hazards. Properly identifying and classifying of scheduled waste is crucial for its safe management and disposal.

The common SW categories in communications infrastructure are listed in Annex H. Refer to First Schedule of Environment Quality (Scheduled Wastes) Regulations 2005 for more details on type of SW and its source.

Develop asset policies relevant to SW categories, subject to authority approval.

13.3.2 Appointment of competent person for SW

A competent person is important for a proper handling and management of SW to minimise and/or avoid of waste spillage incident. The competent person shall conduct the following activities:

a) coordinate e-waste management;

b) manage SW;

c) conduct studies;

d) oversee dismantling works;

e) prepare and submit environmental related reports or documentation; and

f) reports through the electronic Scheduled Waste Information System (eSWIS) portal.

13.3.3 Storage and handling

The storage and handling of scheduled waste require stringent measures to prevent environmental contamination and human health risks. Proper practices include:

a) Storage and warehouse criteria

   i) On-site storage

   Designated area away from manufacturing or processing and employee activity.

   ii) Off-site Storage

   This is to comply with Department of Environment (DOE) siting and zoning guidelines and located within an industrial area as stated in Environmental Requirements: A Guide for Investors by DOE (Appendix G, Guidelines for the Siting and Zoning of Industries).

b) Standard Storage

   i) Store SW for up to 180 days or not more than 20 metric tons.

   ii) Shall maintain records of collection, sale, transfer, and storage.

   iii) For storage over 180 days or over 20 metric tons, to promptly seek authority approval.

13.3.4 Disposal methods

Disposal methods for SW involve carefully controlled processes to minimise environmental impact. The methods must be compliant with regulations and effectively eliminate or contain hazardous substances.

These methods often include:

a) Dispose of identified waste in accordance with the rules and regulations.

b) Prioritise disposal of high-risk leakage and/or fire hazard materials.

c) Weigh appropriately the SW and record accordingly.

13.3.5 Handling and disposal

Handling and disposal of SW require meticulous attention to detail to protect human health and the environment. Proper handling encompasses secure storage, transportation, and preparation for disposal. This process involves a combination of technical expertise, adherence to safety protocols, and responsible environmental stewardship as shown below.

a) Proper handling and packing (if necessary) to designated locations by competent or authorised person.

b) SW should be transported and disposed of appropriately by waste generators and suppliers.

c) SW should be disposed at authorised Material Recovery Facility (MRF) and/or Landfill Recovery Facility (LRF).

13.3.6 Documentation

Documentation in SW management is crucial for compliance, accountability, and effective waste management. Detailed records of waste generation, storage, transportation, treatment, and disposal must be maintained. These records facilitate waste tracking, risk identification, and regulatory compliance as below practice.

a) Maintain records of SW disposal for at least three years from date of waste generation. Annex J provides guidance on the sample template with its key information to be collated, recorded, and stored.

b) Submit reports to law enforcement, local authorities, and regulators as required.

c) Monitor and evaluate hazardous waste management practices and compliance.

13.4 Safety, training, and monitoring

A robust safety culture, comprehensive training, and vigilant monitoring are essential for effective Scheduled Waste (SW) management. Employees must be equipped with the knowledge and skills to handle hazardous materials safely, preventing accidents and injuries. Regular training, including emergency response procedures, is crucial. Continuous monitoring of workplace conditions, employee compliance, and environmental impact ensures the safety of personnel, the public, and the environment.

13.4.1 Safety and health

a) Ensure the safety and health of its works and the protection of the environment from the adverse effects of SW and compliance with laws and regulations.

b) Implement a safety and health management system for SW management.

13.4.2 Training and responsibilities

Per legislative requirements, provide periodic training to relevant personnel on SW handling, labelling, transportation, storage, and spill response.

13.4.3 Monitoring and reporting

a) Monitor and evaluate waste management practices, action plans and compliance.

b) Disclose the waste data and action plans programs publicly via environmental report/ Integrated Annual Report/ Sustainability report / statement.

c) The results from the monitoring process shall be analysed, evaluated, and improved.

d) If required, the report could be submitted to external parties, such as law enforcement agencies, local authorities, and regulators.

13.4.4 Record keeping

Record keeping is required for 3 years from the date of SW generated, as cited in Regulation 11 of Environmental Quality (Scheduled Wastes) Regulations 2005 by DOE and/ or as specified by any other authorities and regulatory bodies.

Annex A
(normative)

List of active and passive asset

Table A.1 below shows the asset category, list of type of assets and its description as well as their example.

Table A.1. List of active and passive asset

Asset category	Type of ~~asset~~ services	Description	Example
Active asset	Mobile network	Includes components that facilitate communications, ensure connectivity, and support the transmission of data, allow mobile devices to connect to the internet or other communications services while on the go	Baseband unit (BBU), Remote Radio Unit (RRU)
	Internet of Things (IoT)	Refers to a network of physical devices, appliances, and other physical objects that are embedded with sensors, and network connectivity for data collection and sharing	IoT gateways, relays, sensors controllers
	Broadcast network asset	Allows messages or data to be sent to all the nodes within a network	Reconfigurable Optical Add-Drop Multiplexer (ROADM), router, switches
	Fixed transport infrastructure	Manages network and provide internet access to connected devices through fixed lines,	fibre link, metro-E
	Wireless transport infrastructure	Manages wireless network and provide internet access to connected devices	microwave, satellite
	Non-mobile network	Includes components that facilitate communications of data	Wi-Fi Access Point (AP), switch, controller
Passive asset	Structure asset	Includes towers and other associated assets to support the assets construction	Ground base tower (GBT), smart pole, street furniture, data centre
	Energy asset	Includes components for the generation, transmission, and distribution of electricity	battery, power systems, breaker, fuel cell
	Fibre asset	Enables fibre-based fixed network that includes fibre-optic cable assets and related accessories	Manhole, trunk, fibre-optic cables, optical distribution frame (ODF)/ Fiber distribution frame (FDF), main distribution frame (MDF) room, cable landing station
	Copper infrastructure	Enables copper-based fixed network	copper cables, patch, cable tray
Note: The list above is not exhaustive			

Annex B
(normative)

Abbreviations

3R	Reduce, Reuse and Recycle
5G	5th Generation Mobile Network
AI	Artificial Intelligence
AP	Access Points
BBU	Baseband Unit
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CBA	Cost-Benefit Analysis
DOE	Department of Environment
EIA	Environmental Impact Assessment
eSWIS	electronic Scheduled Waste Information System
FAT	Factory Acceptance Testing
FDF	Fiber Distribution Frame
GBT	Ground-based Tower
IAT	Integration Acceptance Test
IoT	Internet of Things
LRF	Landfill Recovery Facility
MBCO	Minimum Business Continuity Objective
MCDA	Multi-Criteria Decision Analysis
MDF	Main Distribution Frame
ML	Machine Learning
MRF	Material Recovery Facility
MTPD	Maximum Tolerable Period of Disruption
NFV	Network Function Virtualisation
O&M	Operations and Maintenance
ODF	Optical Distribution Frame
OEM	Original Equipment Manufacturers
OSHE	Occupational Safety, Health, and Environment

PE	Professional Engineer
POC	Proof of Concept
RCA	Root Cause Analysis
RFx	Request for Proposal / Information /Quotation
ROADM	Reconfigurable Optical Add-Drop Multiplexer
ROT	Redundant, Obsolete, Trivial
RPO	Recovery Point Objective
RRU	Remote Radio Unit
RTO	Recovery Time Objective
SDN	Software-Defined Networking
SLA	Service Level Agreement
SOP	Standard Operating Procedures
SW	Scheduled Waste
TRLs	Technology Readiness Levels
UAT	User Acceptance Testing

Annex C
(informative)

Sample of inventory list

Table C.1 below shows the sample of inventory list prepared by the asset owner.

Table C.1. Sample of inventory list

Asset reference	Asset description	Capitalisation date	Acquisition value (RM)	Book value (RM)	Address 1	Address 2	Address 3	Address 4
12345678	Antenna	dd-mm-yyyy	100,000.00	75,000.00	LOT46, MUKIM 16	JLN KG BARU	AYER HITAM	JOHOR

Annex D
(informative)

Sample of preventive maintenance

Table D.1 below shows the sample of preventive maintenance.

Table D.1. Sample of preventive maintenance

No.	Asset	Type of schedule maintenance	Frequency	Responsible parties
1.	Structure-tower	• Replacement of bolt & nuts • Application of anti-corrosion painting • Repainting	Once every X years	Tower provider
2.	Base Transceiver Station (BTS)	• Inspect and clean BTS cabinets and enclosures. • Check and clean air filters and fans. • Inspect and clean power supply units and connectors. • Ensure proper grounding and bonding.	Quarterly	Field Maintenance Technicians
3.	Optical Distribution Frame (ODF)	• Conduct optical time-domain reflectometer (OTDR) tests to check fiber integrity. • Measure and record signal loss (attenuation) levels. • Verify the operation of optical switches and splitters	Annually	Fiber Network Engineers

Annex E
(Informative)

Sample of corrective maintenance

Table E.1 below shows the sample of corrective maintenance.

Table E.1. Sample of corrective maintenance

No.	Condition of Asset / Service	Assessment Status	Recommended action
1.	Network Failure / Downtime has triggered. *e.g. ; Power failure*	CRITICAL	**24 hours** – Deployment of temporary asset / temporary recovery system - Emergency deployment to resolve the issue
2.	Potential of network failure / Downtime is **VERY HIGH** a) Asset defects / impairment is dangerous to human-being and may jeopardize the communications equipment / services is left unattended in **2 weeks' time** *e.g. ; Exposed fibre* b) Access to the location of the asset is inaccessible. *e.g. : Major landslide, broken climbing ladder*	SEVERE	**Maximum 2 weeks**
3.	Potential of network failure / Downtime is **HIGH**. a) Asset defects / impairment is dangerous to human-being and may jeopardize the communications equipment / services is left unattended in **8 weeks' time** *e.g. ; significant deformation of the tower members / indicant sign of failure*	MODERATE	**Maximum 3 months**
4.	Defects / impairment discovered but **NO SIGNIFICANT** impact to the human-being or communications equipment if left unattended for more than **3 months**	MILD	**Maximum 1 year**

Annex F
(informative)

Sample of predictive maintenance

Table F.1 below shows the sample of predictive maintenance.

Table F.1. Sample of predictive maintenance

Customer operations				Network operations			
Order entry	**Provisioning**	**Billing**	**Care**	**NOC**	**Problem resolution**	**Field service**	**Steering and management**
Error checking of entered orders	Real-time status updates	Billing and inventory reconciliation and revenue assurance	"Intelligent agent" for customer service	Predictive maintenance of network quality	Prescriptive solutions to common issues offered as self-help	Guided workflows linked to issues predicted	Analytics of key performance indicators for performance management
Customer-preference evolution	On-demand provisioning		Predictive issue identification based on usage analytics	Optimised linkage of NOC tech to field force and vice versa based on issue	Guided workflows	Optimised logistics through geo-analytics	
			Learning programs for response automation (fully AI agents)			Real-time status updates	

NOTE: NOC is Network-operations centre

Source (McKinsey & Company): https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/maximizing-value-from-advanced-analytics-in-telco-service-operations

Table F.2 below shows the sample of use cases for predictive maintenance.

Table F.2. Sample of use cases for predictive maintenance

Type of Operation	Dimension	Use cases
Customer Operations	Order entry	• Error-checking • Customer preference evolution
Customer Operations	Provisioning	• Real-time status updates • On-demand provisioning
Customer Operations	Care	• Predictive issue identification based on user analytics
Network Operations	NOC	• Predictive maintenance of network quality
Network Operations	Problem resolution	• Guided workflows
Network Operations	Field service	• Logistics • Real-time status updates

Annex G
(informative)

Sample of disaster recovery and Business Continuity Management (BCM) cycle

Figure G.1 illustrates a sample model of the timeline describing a disaster event, its impact evaluation and recovery.

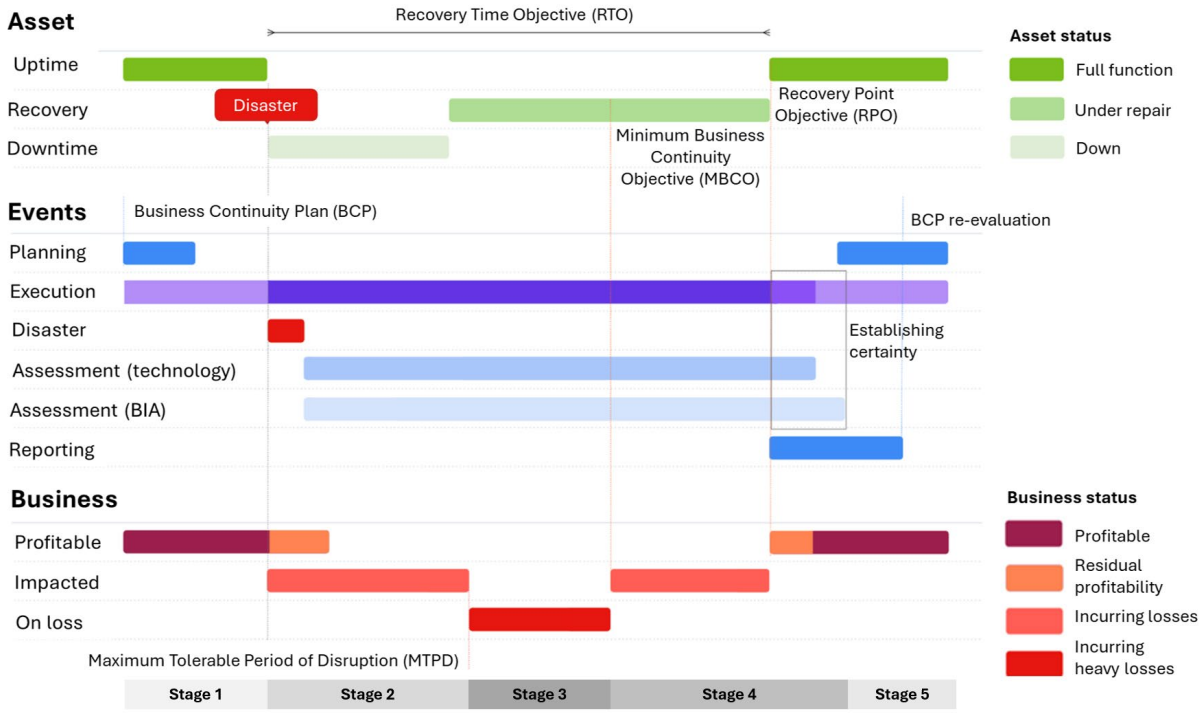

Figure G.1. Sample of disaster recovery and business continuity management cycle

The above diagram depicts the different phases an organisation will undergo, as well as the actions it should undertake, in the event of a disaster affecting infrastructure equipment.

This analysis covers asset management, operational events, and actions as well as business considerations, each of them depicted in their own distinct timeline. The diagram formulates 5 stages, with its distinct events and actions for each timeline.

Stage 1: Normal operations.

In this phase, the infrastructure assets are operating at optimal levels, enabling proper business operations and profitability, including SLA and regulatory compliance.

In this phase, companies should invest efforts in proper planning by developing their Business Continuity Plan (BCP) and implement the necessary capacity building actions to ensure all personnel are aware and ready for a possible disaster response. The objective must be to prepare the organisation to minimise losses by establishing a concrete and achievable Recovery Time Objective (RTO).

Stage 2: Disaster event

In the event of a disaster, the organisation will suffer a downtime in services and needs to react promptly, activating its BCP.

Assessments on the technical state of the assets as well as the business impact must begin immediately to evaluate the actual impact on the organisation.

Depending on the severity of the disaster, the business impact may still not reach a loss status. Organisations should strive to avoid reaching their established Maximum Tolerable Period of Disruption (MTPD) to remain in this stage.

Stage 3: Business loss

Once the downtime exceeds its MTPD, the organisation is formally incurring in losses. These losses may affect business revenue, compliance xxx and reputational impact, very often with compounding effects.

Palliative measures defined in the BCP are to be initiated right away, with special consideration of regulatory compliance to avoid further damage derived from future repercussions.

Depending on the state of repairs during the asset recovery, the organisation may switch between Stage 2 and 3 for several times before reaching its Minimum Business Continuity Objective (MBCO), therefore entering Stage 4.

Stage 4: Business recovery

Once the assets have been repaired sufficiently, the organisation will have recovered a functional status measured by achieving its MBCO. During this phase, the organisation must remain vigilant and establish full certainty that operations have been restored in full. This evaluation is to be done based on its BCP and for a duration not shorter than therein indicated.

Business profitability, if not recovered in full, should only be marginally impacted.

Reporting on the whole incident should also start, profiting from the proximity of the event and first-hand experience of the personnel involved. Ideally, reporting will include material intended for potential legal and public disclosures.

Stage 5: Normal operations restored

Once the Recovery Point Objective (RPO) is achieved, the organisation is officially back to normal operations and profitability.

The organisation must then proceed to revisit its BCP based on the incident’s report and fine tune it accordingly. Capacity building actions are to be undertaken as appropriate after any revision.

Annex H
(informative)

Environment Quality (Scheduled Wastes) Regulations 2005

The First Schedule (Regulation 2) of the Environment Quality (Scheduled Wastes) Regulations 2005 outlines the various types of scheduled wastes that are regulated under Malaysian law. This includes classification of wastes, waste codes and types of wastes.

Table H.1. SW1 metal and metal-bearing wastes

No	Description	Source/Example
SW1 Metal and Metal-Bearing Wastes		
1	SW 101 - Waste that contains arsenic or its compound.	Wood preservatives, fertilizer, pesticides, pharmaceuticals, semiconductors, car battery manufacturing industry, phosphoric acid recovery plant.
2	SW 102 - Waste of lead-acid batteries in whole or crushed form.	Lead-acid battery manufacturing industry, lead-acid batteries, recovery plant, automobile workshop, maintenance service.
3	SW 103 - Waste of batteries containing cadmium and nickel or mercury or lithium.	Button or rechargeable battery manufacturing industry, maintenance service
4	SW 104 - Dust, slag, dross or ash containing arsenic, mercury, lead, cadmium, chromium, nickel, copper, vanadium, beryllium, antimony, tellurium, thallium or selenium excluding slag from iron and steel factory.	Metal smelting industry, Scheduled waste incinerator.
5	SW 105 - Galvanic sludges	Zinc processing, electroplating or galvanizing industry.
6	SW 106 - Residues from recovery of acid pickling liquor	Iron and steel, and electroplating industry
7	SW 107 - Slags from copper processing for further processing or refining containing arsenic, lead or cadmium	Copper smelting, processing, and refining industry
8	SW 108 **-** Leaching residues from zinc processing in dust and sludges form	Zinc processing and Zinc electroplating Industry
9	SW 109 **-** Waste containing mercury or its compound	Medical equipment manufacturing (such as barometers and thermometers), fluorescent bulbs, LCD TV and computer monitor manufacturing industry.
10	SW 110 - Waste from electrical and electronic assemblies containing components such as accumulators, mercury-switches, glass from cathode-ray tubes and other activated glass polychlorinated biphenyl-capacitors, or contaminated with cadmium, mercury, lead, nickel, chromium, copper, lithium, silver, manganese or polychlorinated biphenyl	Electrical and electronic manufacturing and metal recovery industry.

Table H.2. SW2 wastes containing principally inorganic constituents

No	Description	Source/Example
SW2 Wastes Containing Principally Inorganic Constituents		
1	SW 201 **-** Asbestos wastes in sludges, dust or fibre forms	Clutch plate, brake pad, gasket, roof, ceiling, panel manufacturing industry.
2	SW 202 **-** Waste catalysts.	Refinery and automobile industry, recovery of waste catalyst plant.
3	SW 203 **-** Immobilized scheduled wastes including chemically fixed, encapsulated, solidified, or stabilised sludges	Treatment and disposal of scheduled waste plant or facility.
4	SW 204 **-** Sludges containing one or several metals including chromium, copper, nickel, zinc, lead, cadmium, aluminium, tin, vanadium, and beryllium	Wastewater treatment plant from electroplating, galvanizing, metal work and metal recovery industry.
5	SW 205 **-** Waste gypsum arising from chemical industry or power plant	Chemical industry or power plant (desulphurisation process)
6	SW 206 **-** Spent inorganic acids	Iron and steel, electroplating, metal work and automobile industry.
7	SW 207 - Sludges containing fluoride	Electronic, toothpaste, solar panel manufacturing industry.

Table H.3. SW3 Wastes containing principally organic constituents

No	Description	Source/Example
SW3 Wastes containing principally organic constituents		
1	SW 301 - Spent organic acids with pH less or equal to 2 which are corrosive or hazardous	Iron and steel, automobile and metal work industry (rust removal)
2	SW 302 - Flux waste containing mixture of organic acids, solvents or compounds of ammonium chloride	Automobile, metal work and steel furniture industry (from soldering, welding and brazing processes
3	SW 303 - Adhesive or glue waste containing organic solvents excluding solid polymeric materials	Resin, furniture and automobile manufacturing industry
4	SW 304 - Press cake from pretreatment of glycerol soap lye	Soap manufacturing industry
5	SW 305 - Spent lubricating oil	Industrial machine and automobile workshop
6	SW 306 - Spent hydraulic oil	Industrial machine and automobile workshop
7	SW 307 - Spent mineral oil-water emulsion	Petrochemical industry
8	SW 308 - Oil tanker sludges	Tanker desludging
9	SW 309 - Oil-water mixture such as ballast water	Shipping industry (oil cargo)
10	SW 310 - Sludge from mineral oil storage tank	Mineral oil storage tank (underground tank or surface tank)
11	SW 311 - Waste oil or oily sludge	Most industry and workshop
12	SW 312 - Oily residue from automotive workshop, service station oil or grease interceptor	Automotive workshop, service station and certain industry

Table H.3. SW3 Wastes containing principally organic constituents *(continued)*

No	Description	Source/Example
13	SW 313 - Oil contaminated earth from re-refining of used lubricating oil	Re-fining of used lubricating oil industry
14	SW 314 - Oil or sludge from oil refinery plant maintenance operation	Oil refinery industry
15	SW 315 - Tar or tarry residues from oil refinery or petrochemical plant	Oil refinery or petrochemical plant
16	SW 316 - Acid sludge	Acid manufacturing and acid recovery industry
17	SW 317 - Spent organometallic compounds including tetraethyl lead, tetramethyl lead and organotin compounds	Petrochemical based industry and catalyst manufacturing industry
18	SW 318 - Waste, substances and articles containing or contaminated with polychlorinated biphenyls (PCB) or polychlorinated triphenyl (PCT)	Electronic manufacturing products such as a capacitor, transformers, cooling liquid, e.g coolant or transformer oil, pesticide hydraulic fluid, lubricant
19	SW 319 - Waste of phenols or phenol compounds including chlorophenol in the form of liquids or sludges	Phenol, resin, pharmaceutical, herbicide, cosmetics, hair dyes and skin lightening manufacturing industry
20	SW 320 - Waste containing formaldehyde	Formaldehyde preservation, automobile, textiles, plywood, carpeting, paint, explosive, disinfectant, biocide, wood cabinet manufacturing industry
21	SW 321 - Rubber or latex wastes or sludge containing organic solvents or heavy metals	Rubber or latex-based industry (such as rubber glove)
22	SW 322 - Waste of non-halogenated organic solvents	Organic solvent, paint, ink, lacquer, resin, glue manufacturing industry, printing industry
23	SW 323 - Waste of halogenated organic solvents	Cleaning chemical manufacturing industry
24	SW 324 - Waste of halogenated or unhalogenated non-aqueous distillation residues arising from the organic solvents recovery process	Organic solvents recovery industry
25	SW 325 - Uncured resin waste containing organic solvents or heavy metals including epoxy resin and phenolic resin	Resin, automobile and furniture manufacturing industry
26	SW 326 - Waste of organic phosphorus compound	Pesticide or fertilizer manufacturing or repacking industry
27	SW 327 - Waste of thermal fluids (heat transfer) such as ethylene glycol	Gas processing plant, coolant, metal work and water manufacturing industry, automobile workshop

Table H.4. SW4 Wastes containing either organic or inorganic constituents

No	Description	Source/Example
SW4 Wastes containing either organic or inorganic constituents		
1	SW 401 - Spent alkalis containing heavy metals	Electroplating, iron and steel, metal work industry
2	SW 402 - Spent alkalis with pH more or equal to 11.5 which are corrosive or hazardous	Soap, biodiesel manufacturing industry, food preparation
3	SW 403 - Discarded drugs containing psychotropic substances or containing substances that are toxic, harmful, carcinogenic, mutagenic or teratogenic	Clinics, hospitals and pharmaceutical industry
4	SW 404 - Pathogenic wastes, clinical wastes or quarantined materials	Clinics and hospitals
5	SW 405 - Waste arising from the preparation and production of pharmaceutical product	Pharmaceutical industry
6	SW 406 - Clinker, slag and ashes from scheduled wastes incinerator	Scheduled waste incinerator facility
7	SW 407 - Waste containing dioxins or furans	Ash of the industrial, incinerator, PVC based, cleaning chemicals, toys and clothing manufacturing
8	SW 408 - Contaminated soil, debris or matter resulting from cleaning-up of a spill of chemical, mineral oil or scheduled wastes	Most industry
9	SW 409 - Disposed containers, bags or equipment contaminated with chemicals, pesticides, mineral oil or scheduled wastes	Most industry
10	SW 410 - Rags, plastics, papers or filters contaminated with scheduled wastes	Most industry
11	SW 411 - Spent activated carbon excluding carbon from the treatment of potable water and processes of the food industry and vitamin production	Waste water treatment plant and scrubber
12	SW 412 - Sludges containing cyanide	Electroplating, precious metal recovery, iron and steel industry
13	SW 413 - Spent salt containing cyanide	Iron and steel industry (carburation process)
14	SW 414 - Spent aqueous alkaline solution containing cyanide	Iron and steel and metal recovery industry (oxidation of CN)
15	SW 415 - Spent quenching oils containing cyanides	Iron and steel industry
16	SW 416 - Sludges of inks, paints, pigments, lacquer, dye or varnish	Inks, paints, pigments, lacquer, dye or vanish manufacturing industry
17	SW 417 - Waste of inks, paints, pigments, lacquer, dye or varnish	Inks, paints, pigments, lacquer, dye or vanish manufacturing industry
18	SW 418 - Discarded or off-specification inks, paints, pigments, lacquer, dye or varnish products containing organic solvent	Inks, paints, pigments, lacquer, dye or vanish manufacturing industry
19	SW 419 - Spent di-isocyanates and residues of isocyanate compounds excluding solid polymeric material from foam manufacturing process	Paint, lacquer and foam manufacturing industry

Table H.4. SW4 Wastes containing either organic or inorganic constituents *(continued)*

No	Description	Source/Example
20	SW 420 - Leachate from scheduled waste landfill	Scheduled waste landfill
21	SW 421 - A mixture of scheduled wastes	Certain industry
22	SW 422 - A mixture of scheduled and non-scheduled wastes	Certain industry
23	SW 423 - Spent processing solution, discarded photographic chemicals or discarded photographic wastes	Photographic shop and industry
24	SW 424 - Spent oxidizing agent	Textile, wafer, recycled paper and cleaning chemical industry
25	SW 425 - Wastes from the production, formulation, trade or use of pesticides, herbicides or biocides	Pesticides, herbicides or biocide manufacturing or repacking industry
26	SW 426 - Off-specification products from the production, formulation, trade or use of pesticides, herbicides or biocides	Pesticides, herbicides or biocide manufacturing or packing industry
27	SW 427 - Mineral sludges including calcium hydroxide sludges, phosphating sludges, calcium sulphite sludges and carbonates sludges	Automobile and petrochemical refinery industry
28	SW 428 - Wastes from wood preserving operation using inorganic salts containing copper, chromium or arsenic of fluoride compounds or using compound containing chlorinated phenol or creosote	Wood based industry
29	SW 429 - Chemicals that are discarded or off-specification	Certain industry, laboratory
30	SW 430 - Obsolete laboratory chemicals	Laboratory
31	SW 431 - Waste from manufacturing or processing or use of explosives	Manufacturing or processing or use of explosives industry
32	SW 432 - Waste containing, consisting of or contaminated with, peroxides	Peroxides manufacturing industry, textile, recycle paper and wafer manufacturing industry

Annex J
(Informative)

Sample template for reporting on waste data

Table J.1 shows the sample template as a guidance for an organisation to capture, monitor and track their waste data.

Table J.1. Sample template for reporting on waste data

No	Date and month	Type of waste & descriptions	Scheduled waste code (if applicable)	Weight (metric tonne)	Waste transporter and/ or contractor name	Supporting document (eSWIS record/ SW consignment note etc	Non-compliance / Incident (if any)

Bibliography

[1] ISO 55001, Asset management – Management synthesis – Requirements

[2] ISO 55002, Asset management – Management systems – Guidelines for the application of ISO 55001

[3] Daftar Bahan Binaan Yang Diperakukan CIDB. Kuala Lumpur: Lembaga Pembangunan Industri Pembinaan Malaysia (CIDB Malaysia, 2021).

[4] Dasar Pengurusan Aset Kerajaan versi 2.0 (DPAK)

[5] Garis Panduan Pembinaan Menara dan Struktur Sistem Pemancar Telekomunikasi di Kawasan Pihak Berkuasa Tempatan, KPKT 2002 (“Garis Panduan KPKT 2002”)

[6] Garis Panduan Perancangan Infrastruktur Komunikasi (GPP-I) Tahun 2022

Acknowledgements

Communications Infrastructure Asset Management Sub Working Group

Sub Working Group Leaders

Mr Mohd Azlan Zainudin (Chairman)	EDOTCO Malaysia Sdn Bhd
Mr Hadee Mustapa (Vice Chairman)	Edgepoint Tower Sdn Bhd
Ms Zuridah Hassan (Secretary)	Maxis Broadband Sdn Bhd

Drafting Committee Members

Mr Mohd Azlan Zainudin (Draft Lead)	EDOTCO Malaysia Sdn Bhd
Ms Humairah Ahmad Nasir (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Muhaimin Mat Salleh (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Mohamad Norzamir Mat Taib (Secretariat)	Malaysian Technical Standards Forum Bhd
Ms Fatin Nu Afnan	CelcomDigi Berhad
Ms Rosmawar Mohamad Rafiai	CelcomDigi Berhad
Dr Lee Wah Pheng	Digital Connect Society
Dr Lim Yee Mei	Digital Connect Society
Mr Sharul A Rashid	Digital Connect Society
Mr Sani Azrul Mohamad Salleh	Digital Nasional Berhad
Mr Mohd Azizi Abdul Aziz	EDOTCO Malaysia Sdn Bhd
Dr Asmarani Ahmad Puzi	International Islamic University Malaysia
Ts Dr Dini Oktarina Dwi Handayani	International Islamic University Malaysia
Mr Ahmad Fizri Mohd Azmi	TM Technology Services Sdn Bhd
Ms Arnida Amdan	TM Technology Services Sdn Bhd
Ms Erliz Rizuan	TM Technology Services Sdn Bhd
Ir Mohd Asmadi Mohd Umar@ Kasman	TM Technology Services Sdn Bhd
Mr Mohd Nizam Osman	TM Technology Services Sdn Bhd
Ms Monarnih Joni	TM Technology Services Sdn Bhd
Ms Norazilah Ismail	TM Technology Services Sdn Bhd
Ms Nur Dayana Muhamad	TM Technology Services Sdn Bhd
Assoc Prof Dr Tee Boon Tuan	Universiti Teknikal Malaysia Melaka
Mr Fadhlullah Muhammad Mohamed Yunos	YTL Communications Sdn Bhd
Mr Kelvin Ling Siew Hua	YTL Communications Sdn Bhd

Contributors

Mr Nik Mohd Hafeez Nik Aziz	Measat Broadcast Network Systems Sdn Bhd
Mr Mohamad Isa Mohd Razhali	Measat Broadcast Network Systems Sdn Bhd
Mr Low Kien Yap	CelcomDigi Berhad
Ms Siti Rizaidah Mokhtar	CelcomDigi Berhad
Ms Nurul Hidayah Atiqah Abu Samah	D'Harmoni Telco Infra Sdn Bhd
Ts Muhammad Nabil Irfan Khairul Anuar	D'Harmoni Telco Infra Sdn Bhd
Mr Juhasli Aizi Juperi	EDOTCO Malaysia Sdn Bhd
Ms Noor Saidatul Aina	EDOTCO Malaysia Sdn Bhd
Mr Muhammad Suhaimi Ithnin	EDOTCO Malaysia Sdn Bhd
Mr Ariff Olan Kholid	FNS (M) Sdn Bhd
Ms Norkhadhra Nawawi	FNS (M) Sdn Bhd
Mr Radhilufti Madehi	FNS (M) Sdn Bhd
Mr Eami Yusry Mohd Yusof	Maxis Broadband Sdn Bhd
Mr Phang Huey Meng	Maxis Broadband Sdn Bhd
Mr Razmin Syah Abdul Razak	REDtone Engineering and Network Services Sdn Bhd
Mr Jean F Queralt	The IO Network MY Sdn Bhd
Ms Maryam Lee	The IO Network MY Sdn Bhd
Ms Amelia Hanim Azahari	TM Technology Services Sdn Bhd
Mr Amirussyahri Ahmad	TM Technology Services Sdn Bhd
Mr Hakimi Md Din	TM Technology Services Sdn Bhd
Ms Helia Adriyani Nasrul	TM Technology Services Sdn Bhd
Mr Mohd Khairi Ahmad Sabari	TM Technology Services Sdn Bhd
Mr Mohd Zulkanain Mohd Shah	TM Technology Services Sdn Bhd
Ms SitiJuliana Mohd Shah	TM Technology Services Sdn Bhd
Ts Sufian Sulaiman	TM Technology Services Sdn Bhd
Mr Imran Zulkifli	TIME dotCom Berhad
Mr Nurfikri Halimi	U Mobile Sdn Bhd
Mr Tan Chin Aik	YTL Communications Sdn Bhd
Dr Dzaharuddin Mansor	*Amazon Web Services*
Ms Nurulhuda Nawam	*Petronas*