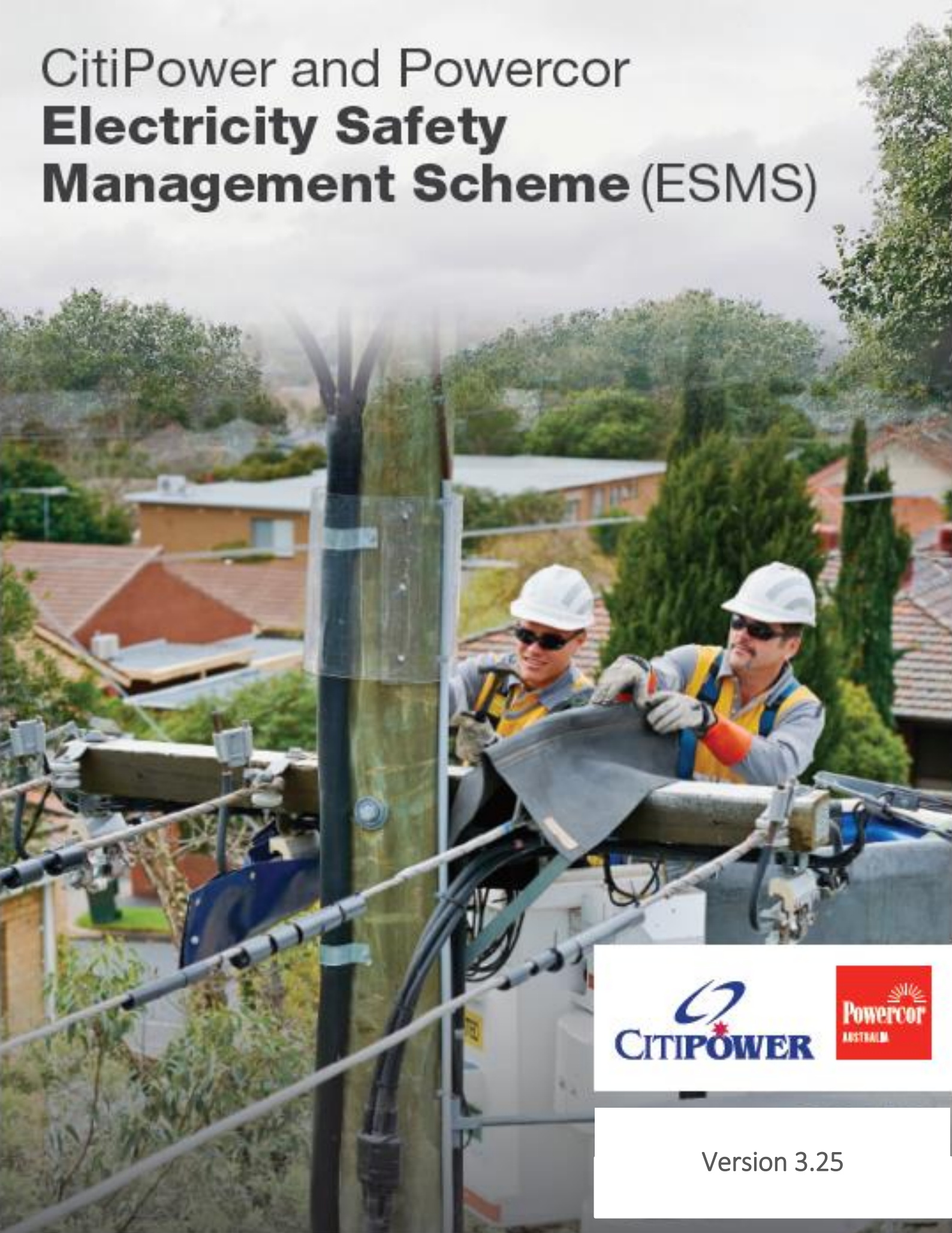
CitiPower and Powercor **Electricity Safety Management Scheme** (ESMS)



CITIPOWER

Powercor AUSTRALIA

Version 3.25

Our objective is to manage in a way that minimises the risk of

FIRE IGNITION

ELECTRIC SHOCK/INJURY

PROPERTY DAMAGE

INTERRUPTION OF SUPPLY

Table of Contents

MESSAGE FROM THE CEO

I am pleased to endorse the CitiPower and Powercor (CP-PAL) Electricity Safety Management System (ESMS) which demonstrates our commitment to providing customers with a safe, reliable and affordable supply of electricity.

Tim Rourke

Chief Executive Officer

INTRODUCTION BY THE GENERAL MANAGER ELECTRICITY NETWORKS

As General Manager Electricity Networks, I am pleased to present the CP-PAL ESMS.

This important document demonstrates how we comply with the ESMS obligations as specified in the Electricity Safety Act and Electricity Safety (Management) Regulations. The CP-PAL Executive and other key internal stakeholders have endorsed the ESMS.

Health and safety of our employees, contractors, customers and the community is our highest priority. The Safety Case and ESMS describe how we design, construct, operate and maintain our assets to enable us to meet our obligations to minimise the hazards and risks as far as practicable associated with fire starts, electric shock/injury, property damage and interruptions of supply.

We look forward to continuing to provide safe and reliable electricity supply to our communities and thank Energy Safe Victoria (ESV) for their assistance in the preparation of this Safety Case and our ESMS submission.

Steven Neave

General Manager, Electricity Networks

ESMS APPROVAL

Description	Responsible Person's Title
Document Administrator	Network Safety Manager
Document Owner	Network Safety and Bushfire Mitigation Manager
Endorsed by	Executive Management Team

DOCUMENT VERSION HISTORY

The following table provides a summary of changes made to this document.

Issue No.	Date	Revision Summary
1.0	24/12/2015	Submitted to ESV
2.0	24/11/2017	Submitted to ESV – Post Safety Case Acceptance
3.0	03/10/2018	Submitted to ESV - Post ESMS Validation
3.1	16/10/2018	Revised to Address ESV Feedback
3.2	17/10/2018	Minor Amendments to: - Section 1.3 - Table 1-1 - Section 5.3
3.21	17/10/2018	Minor Amendments to: - Section 4.2.4
3.22	18/10/2018	Amendments to: - Section 4.2.4
3.23	31/10/2018	Appendix 17 ESMS Commitments Inserted
3.24	12/12/2018	Message from CEO Inserted
3.25	18/11/2019	Annual review and updates – 2019 Refer Appendix 18 for summary of key updates

ABBREVIATIONS

Term	Description
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
AFAP	As Far As Practicable In accordance with Section 98 of Electricity Safety Act 1998 '*General duty of major electricity company*'
ALARP	As Low As Reasonably Practicable In accordance with clause 3.1 of AS 5577 - *Electricity Network Safety Management System 2013 'ALARP*'
AMF	Asset Management Framework
AMP	Asset Management Plan
BFMP	Bushfire Mitigation Plan
BOM	Bureau of Meteorology
CBD	Central Business District
CBRM	Condition Based Risk Management
CEO	Chief Executive Officer
CFA	Country Fire Authority
CitiPower	CitiPower Pty Ltd
CKI	Cheung Kong Infrastructure Holdings
CP-PAL	CitiPower and Powercor
DSE	Department of Sustainability and Environment
EMCOP	Emerging Management Common Operating Picture
EMT	Executive Management Team
ENIDB	Electrical Network Incident Database
ENSMS	Electricity Network Safety Management System applied in CP-PAL
ERM	Enterprise Risk Management
ESC	Essential Services Commission
ESMS	Electricity Safety Management Scheme

Term	Description
ESV	Energy Safe Victoria
FMC	Field Mobile Computing
FSA	Formal Safety Assessment
GIS	Geographical Information System
H&S	Health and Safety
HBRA	Hazardous Bush Fire Risk Area
HS&E	Health, Safety and Environment
HV	High Voltage
IT	Information Technology
JSA	Job Safety Analysis
Key Network Activities	Design, Construct, Operate, Maintain, Operate and Decommission of Network Assets
kV	Kilovolts (1,000 Volts)
kW	Kilowatts (1,000 Watts)
LBRA	Low Bushfire Risk Area
LV	Low Voltage
MEC	Major Electricity Company
NER	National Electricity Rules
OMS	Outage Management System
PBST	Powerline Bushfire Safety Taskforce
P1	Priority 1 Maintenance
P2	Priority 2 Maintenance
P3	Priority 3 Maintenance
POEL	Private Overhead Electric Line
Powercor	Powercor Australia Ltd
RCM	Reliability Centred Maintenance
REFCL	Restricted Earth Fault Current Limiter
RTO	Registered Training Organisation

Term	Description
SAIDI	System Average Interruption Duration Index
SAP	SAP R/3 Mainframe Business Software System
SCADA	Supervisory Control and Data Acquisition
SECV	State Electricity Commission of Victoria
TFB	Total Fire Ban
TOA	Transmission Operations Australia Pty Ltd
TOA2	Transmission Operations (Australia) 2 Pty Ltd
VBRC	Victorian Bushfire Royal Commission
VDAR	Vibration Dampers and Armour Rods
VESI	Victorian Electricity Supply Industry
VICSES	Victoria State Emergency Service
VPN	Victoria Power Networks

Throughout this document the following symbol has been used:

Symbol	Description
	Used to highlight the Critical Controls which are mentioned within the ESMS for managing risks.

TECHNICAL GLOSSARY

Term	Definition
Applicable asset	Means a supply network owned or operated by CitiPower and Powercor
AFAP	In accordance with Section 98 of Electricity Safety Act 1998 'General duty of major electricity company'
ALARP	In accordance with clause 3.1 of AS 5577 - Electricity Network Safety Management System 2013 'ALARP'
Key Network Activities	Design, Construct, Operate, Maintain, Operate and Decommission of Network Assets as defined in AS 5577
Published Technical Standard Or Published Standard	As defined in AS 5577: Documents giving technical information, guidance or advice published by a national or international standards-making organization, such as— (a) Standards Australia; (b) Standards New Zealand; (c) the British Standards Institute; (d) the International Organization for Standardization; (e) the International Electrotechnical Commission; or (f) jurisdictional regulators or governments.

Section 1. BASIS OF ESMS (INTRODUCTION)

This section addresses the clause 4.1 of AS 5577:

4.1 – Basis of section

This Section sets out the requirements of an ENSMS to meet the fundamental principles in Clause 1.2 of this Standard.

The ENSMS shall contain the Network Operator's safety arrangements for the following:

a. *ENSMS policy*
b. *Planning*
c. *Implementation*
d. *Measurement and evaluation*
e. *Management review and change management*

The ENSMS shall include or refer to a description of the network(s), including or referencing suitable maps showing all network assets and the location of associated facilities such as substations and switching stations.

NOTES:

1 Existing documents may continue to be used as part of the ENSMS subject to review for adequacy.

2 For networks that are owned or operated by organisations that have an appropriate management system (such as for Asset Management, Environmental Health and Safety, Health Safety and the Environment, Work Health and Safety or a Safety Management System), the ENSMS may be developed to integrate with that management system to address specific assets that are particular to a network complying with this Standard.

3 See Appendix C for guidance on the description of the network.

How the Network Operator chooses to structure an ENSMS is flexible but the Network Operator shall address the requirements of this Standard.

The elements of an ENSMS, described in Clauses 4.2 to 4.6 below, are interdependent and are of equal importance. An ENSMS shall address these requirements.

1.1 ESMS Purpose and Objective

The purpose of the CP-PAL ESMS is to demonstrate that risks arising from the electricity networks are minimised As Far As Practicable (AFAP) throughout key network activities being design, construction, commissioning, operations, maintenance and decommission. Our ESMS as required by the section 99 and section 108 of the Electricity Safety Act 1998 demonstrates how CP-PAL meets the obligations of section 98 of the Electricity Safety Act 1998 and the Electricity Safety (Management) Regulations 2009 by specifying AS 5577 - *Electricity Network Safety Management System 2013* as the electricity network safety management system.

The objective of our ESMS is to demonstrate ongoing commitment to risk based network management providing for safe, affordable and reliable supply of electricity. The ESMS is integrated with other business management systems, in particular the Asset Management, HS&E Management and Risk Management Frameworks that forms part of the strategies and plans for management of network assets.

Our ESMS complements our Safety Case to inform stakeholders being customers, employees, governments, regulators, retailers and other business partners as to how CP-PAL meets its electricity safety obligations to ensure the safety of public and its employees (including contractors). The ESMS outcomes inform decision-making within the business regarding the activities associated with design, construction, operations, maintenance and decommission.

1.2 ESMS Scope and Legislative Framework

The scope of our ESMS is to address the regulatory obligation and compliance requirements as stipulated in the:

- Electricity Safety Act 1998
- Electricity Safety (Management) Regulations 2009 and
- AS 5577:2013, Electricity Network Safety Management Systems

The scope of the ESMS does not include non-network related operations and activities, such as depot facilities, corporate offices and general business activities.

The following legislative framework is applicable to CP-PAL's ESMS which assist CP-PAL to safely design, construct, operate, maintain and decommission its network.

1.2.1 Acts and Regulations

- Electricity Safety Act 1998
- Electricity Safety (Management) Regulations 2009
- Electricity Safety (Bushfire Mitigation) Regulations 2013
- Electricity Safety (Electric Line Clearance) Regulations 2015
- Electricity Safety (Installations) Regulations 2009
- Electricity Safety (Cathodic Protection) Regulations 2009
- Occupational Health and Safety (Victoria) Act 2004
- Occupational Health and Safety Regulations 2007
- Electricity Industry Act 2000
- National Electricity Rules

1.2.2 Legislated Plans

The following plans form part of the CP-PAL ESMS:

- CP-PAL Bushfire Mitigation Plan[1] (Five yearly plan)
- CP-PAL Electric Line Clearance[2] (Annual plan)

1.2.3 Regulatory Environment

CP-PAL operates within the regulatory environment managed by the following regulatory bodies:

- Energy Safe Victoria
- Work Safe Victoria
- Essential Services Commission
- Department of Environment, Land, Water and Planning
- Australian Energy Regulator
- Australian Energy Market Operator
- Australian Energy Market Commission
- Energy and Water Ombudsman Victoria

The ESMS references many business policies and procedures, which provide further details of demonstration of compliance to the regulatory obligations.

1.3 ESMS Structure

CP-PAL meets the applicable duties of Electricity Safety Act 1998 and demonstrates its compliance to the Electricity Safety Act, Electricity Safety Management Regulations, AS 5577 and ESV ESMS Development Guidelines via this documented Electricity Safety Management Scheme (ESMS).

This ESMS complies with the structure and content of AS 5577 - *Electricity Network Safety Management System 2013*.

This ESMS is structured into six sections as summarised in Table 1-1 – Six Sections of Electricity Safety Management Scheme (ESMS) below:

1 Bushfire Mitigation Strategy Plan- Powercor 2014- 2019 BFMP (05-M810) V4.1: CitiPower 2014- 2019 BFMP (05-M800) V2

2 2017 to 2018 Electric Line Clearance (Vegetation) Management Plan - PAL 2017-2018 ELCMP V1.4

No.	Element	Content	ES Act Reference	AS 5577 Section Reference	ES (Management) Regulations Reference	ESV ESMS Development Guidelines Reference	System Concept
1	Basis of ESMS	ESMS Responsibilities, purpose, objectives and scope CP-PAL network description	Part 10, Division 1, Section 98 Part 10, Division 2, Sections 99, 106 & 107	4.1 – Basis of Section	7 – Person responsible for supply network 8 – Person responsible for electricity safety management scheme 10 – Scheme description – network operators		Intro
2	Policy and Commitment	Policies and safety commitment	Part 10, Division 1, Section 98 Part 10, Division 2, Sections 99, 106 & 107	4.2 – Policy and Commitment	25A – Safety management system - MEC	2 – Asset Strategy & Performance Management	Intro

No.	Element	Content	ES Act Reference	AS 5577 Section Reference	ES (Management) Regulations Reference	ESV ESMS Development Guidelines Reference	System Concept
3	Planning	Planning for safe operations Identification of network safety risks, including the methodology for the risk identification, assessment and treatment process Planning and preparation for abnormal operations Identification of relevant Published Technical Standards and Industry Codes	Part 10, Division 1, Section 98 Part 10, Division 2, Sections 99, 106 & 107	4.3 – Planning 4.3.2 – Planning for safe operation 4.3.3 Planning and preparation for abnormal operations 4.3.4 – Standards and codes	25A – Safety management system - MEC	1 – Formal Safety Assessment of Risk 3 – System Planning & Design	Plan
4	Implementation	Risk control measures for the risks and how they are formulated and subsequently approved, maintained and reviewed Key risk controls for design, construction, commissioning, operation, maintenance and decommission of the networks. Control assessments and actions leading to minimising risks to As Far As Practicable (AFAP) levels	Part 8, Division 2, Subdivision 1, Sections 84 Part 10, Division 2a, Sections 113A, 113B & 113S	4.4 – Implementation 4.4.1 – General 4.4.2 – Resourcing 4.4.3 – Management structure 4.4.4 – Responsibilities, accountabilities and authorities 4.4.5 – Training and competency 4.4.6 – Consultation, communication and reporting	25A – Safety management system - MEC	3 – System Planning & Design 4 – Asset Construction, Maintenance, Commissioning 5 – Network Operation	Do

No.	Element	Content	ES Act Reference	AS 5577 Section Reference	ES (Management) Regulations Reference	ESV ESMS Development Guidelines Reference	System Concept
5	Measurement and Evaluation	Network safety performance reviews and corrective actions.	Part 12, Division 2, Section 142	4.5 – Measurement and evaluation 4.5.1 – Monitoring and measurement 4.5.3 – Records 4.5.4 – System audits	26 – Records 27 – Asset operator and network operator requirements for reporting of serious electrical incidents 28 – Asset operator and network operator reporting of incidents other than serious electrical incidents	6 – Safety Governance & Management	Check and Act
6	Management Review and Change Management	Governance and assurance including how changes to the ESMS and supporting plans are managed, controlled and governed.	Part 10, Division 1, Section 98 Part 10, Division 2, Sections 99, 106 & 107	4.6 – Management review and change management 4.6.1 – Management review 4.6.2 – Change management	25A – Safety management system - MEC	6 – Safety Governance & Management	Governance

Table 1-1 – Six Sections of Electricity Safety Management Scheme (ESMS)

1.4 ESMS Responsibilities

The ultimate responsibility for the management, control and safe operation of the CitiPower and Powercor (CP-PAL) electricity supply networks reside with the distribution licensees. Details of the responsibility are listed below.

Companies' Names:	CitiPower Pty Ltd & Powercor Australia Limited
ABN:	76 064 651 056 (CitiPower) & 89 064 651 109 (Powercor)
Address:	40 Market Street, Melbourne 3000
Telephone:	132 206

Person(s) responsible for ultimate responsibility for the management control and safe operation of the applicable asset:	
Position:	Chief Executive Officer
Address:	Level 9, 40 Market Street, Melbourne 3000
Telephone:	132 206

Position responsible for scheme implementation:	
Position:	General Manager, Electricity Networks
Address:	Level 7, 40 Market Street, Melbourne 3000
Telephone:	(03) 9297 6935

CitiPower and Powercor Emergency Contact Number	
For immediate action (24hrs):	132 412

Position responsible for scheme preparation and submission:	
Position:	Network Safety & Bushfire Mitigation Manager
Address:	Level 7, 40 Market Street, Melbourne 3000
Telephone:	(03) 9683 4357

Position responsible for scheme administration:	
Position:	Network Safety Manager
Address:	Level 7, 40 Market Street, Melbourne 3000
Telephone:	(03) 9683 4294

The Electricity Network's business unit has the delegated responsibility for the activities associated with planning, design, construction, commissioning, operation, maintenance and decommissioning of the network assets. This responsibility includes the development, and management of the policies, processes, standards and instructions applicable to the operation and management of the CP-PAL networks.

While this document focuses on electrical safety, CP-PAL also recognises that it has other statutory Occupational Health and Safety obligations.

1.5 Business Overview

Our business objective is to deliver a safe, reliable and affordable supply of electricity to our customers.

CP-PAL has five key ***strategic focus areas***, which include:

- Improving Stakeholder Engagement – Working with communities, government and partners
- Optimising Regulatory Outcomes – Secure the revenue we need to run our business
- Driving Operational Excellence – Be smarter about how we do things
- Delivering Customer Outcomes – Make it easy for our customer
- Building a Network for the Future – Ensure the network remains competitive

Our five company ***values***, as listed below, underpin everything that is done, every day. They give even greater focus to understanding and supporting our customers, doing what is right and helping our people and business strive for excellence.

- 1. Live safely – Safety is our first priority. We never compromise health and safety, either at work or at home. We are constantly aware of the risks to others and ourselves and actively manage them. We share our experiences so that we all learn
- 2. Be customer and community minded - We listen to our customer, strive to meet their needs and keep them informed. We make a positive contribution to our communities. We deliver on our promises.
- 3. Succeed together - We work together as a team and value the diversity and contribution of our workmates. We always act in a fair and responsible manner and show each other respect. We strive for success as a business while upholding the values that underpin everything we do.
- 4. Be the best you can be - We strive for excellence in everything we do and are always accountable for our own performance. We give our best at all times and help our workmates do their best as well.
- 5. Improve our business - We drive and lead change to be more efficient and effective for the benefit of our workmates, shareholders and other stakeholders.

We distribute power to 64% of Victoria, comprising approximately 1.2 million homes and buildings across the Melbourne CBD and the western districts of the State. We are proud of this role and of our success in consistently delivering a safe, affordable and reliable service.

An Executive Management Team, led by the Chief Executive Officer, manages the CP-PAL business.

CP-PAL is owned by VPN which is 51% owned by Cheung Kong Infrastructure Holdings Limited and Power Asset Holdings Limited. Both form part of the Cheung Kong group of companies based in Hong Kong. Spark Infrastructure Group, a publicly listed infrastructure fund, owns the remaining 49% of the company.

Cheung Kong Infrastructure (CKI) has purchased the listed entity DUET Group comprising a 66% share of United Energy as well as Multinet Gas, the Dampier to Bunbury Pipeline and Energy Developments Limited. As of 15 May 2017, ownership has formally transferred to CKI with the United Energy Board appointed CP-PAL Chief Executive Officer (CEO) as United Energy (UE) CEO as well.

This ESMS only applies to the CP-PAL networks.

1.6 Network Description

Our CP-PAL networks distribute power from the national transmission grid to our customer's point of supply, as summarised by the dark blue in Figure 1-1. The figure provides with simplified overview of CP-PAL network. The network, including our distribution network, has evolved over 100 years.

CP-PAL assets supply customers, including industrial (some supplied at High Voltage), commercial and residential.

We have approximately 1,980 employees at CP-PAL, which includes around 120 trainees and apprentices. These resources are situated across head office and 12 depots throughout our distribution areas.

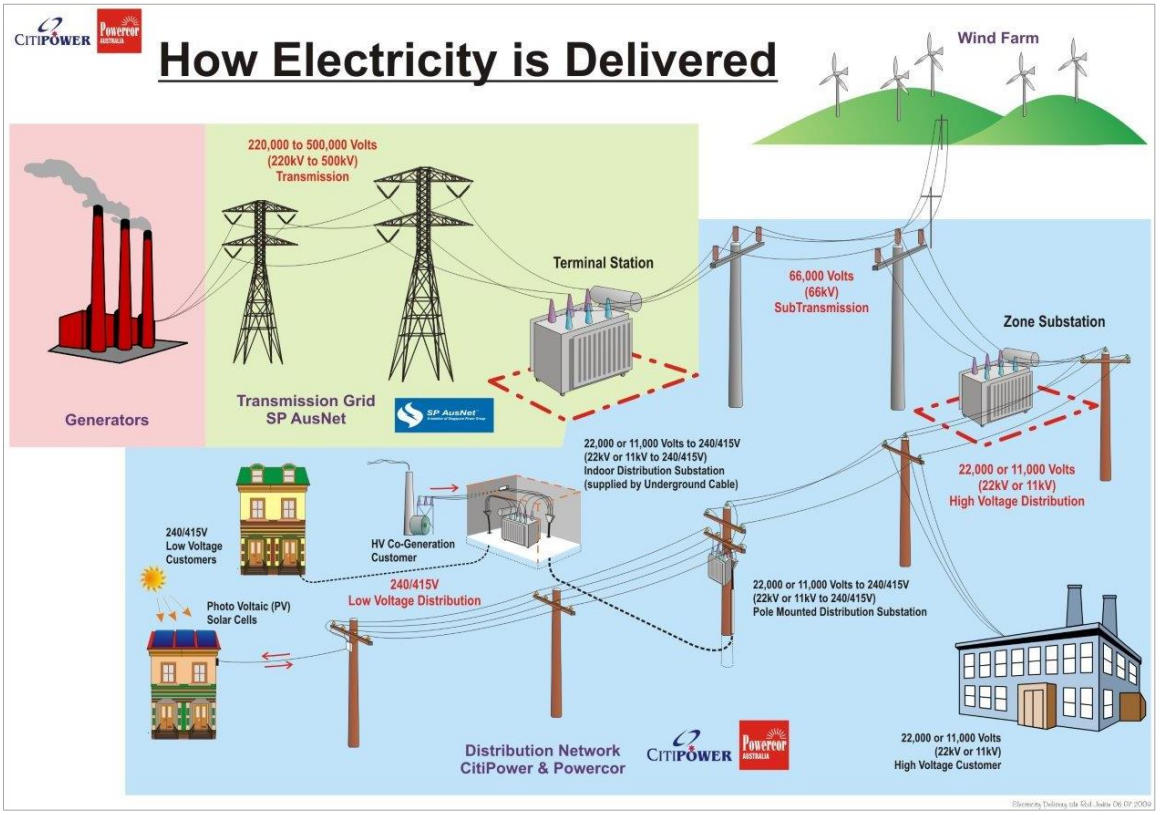


Figure 1-1 – CP-PAL's electricity distribution assets (dark blue)

1.7 Location, Size and Boundaries

CP-PAL distribute power to the Melbourne CBD and the western districts of the State, over 145,000 square kilometres, as shown in Figure 1-2. Our eastern boundary borders with Jemena and AusNet Services (which are also electricity distribution businesses) generally following the Hume Highway to the New South Wales border. Our western boundary borders the South Australian border generally from Nelson to Meringur North. We operate in just about every type of environment including cities, towns, deserts, national parks, farms, mountains and coastal environments.

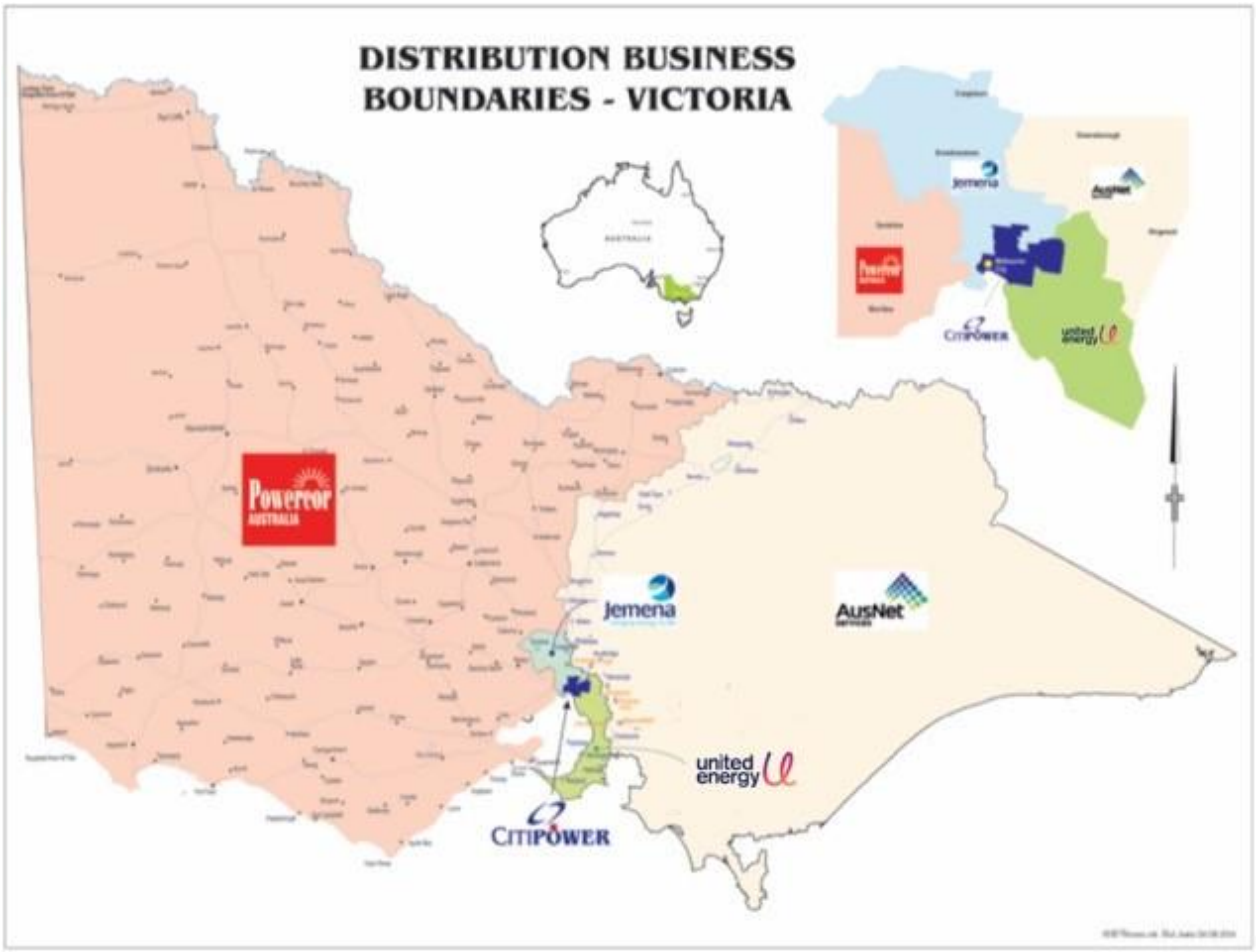


Figure 1-2 – CP-PAL's distribution business boundaries across Victoria

1.7.1 CitiPower's Network

Our CP network covers the area of the Melbourne Central Business District (CBD) and inner northern, eastern and southern metropolitan suburbs and is represented in Figure 1-3. Much of our CP network is underground (42.1%), which has considerable advantage for reducing fires and public hazards and also for providing higher reliability.

Key statistics about our CP network are also included in Figure 1-3. Whilst the network is considerably smaller than the PAL network, the customer density is considerably higher (approximately 10 times), due to the high-density living and industry in the CBD and suburbs.

CitiPower Network Statistics	
Network line lenth	7,503km
Network area	157km sq
Customers	330,000+
Zone substations transformers	102
Distribution transformers	4,797
Poles	58,123
Underground lines	43.5%
Network availability	99.99%

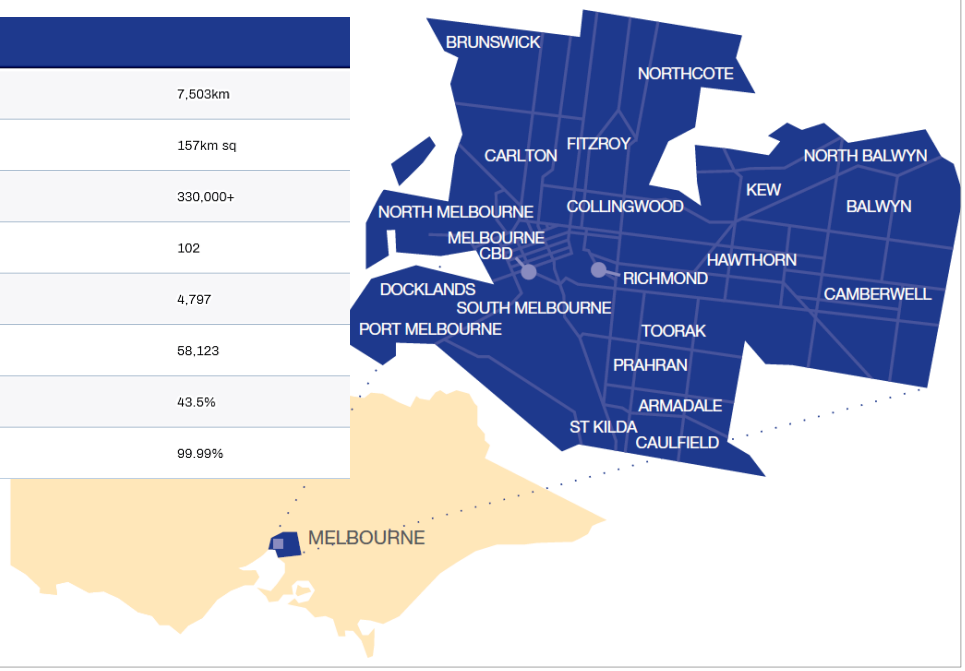
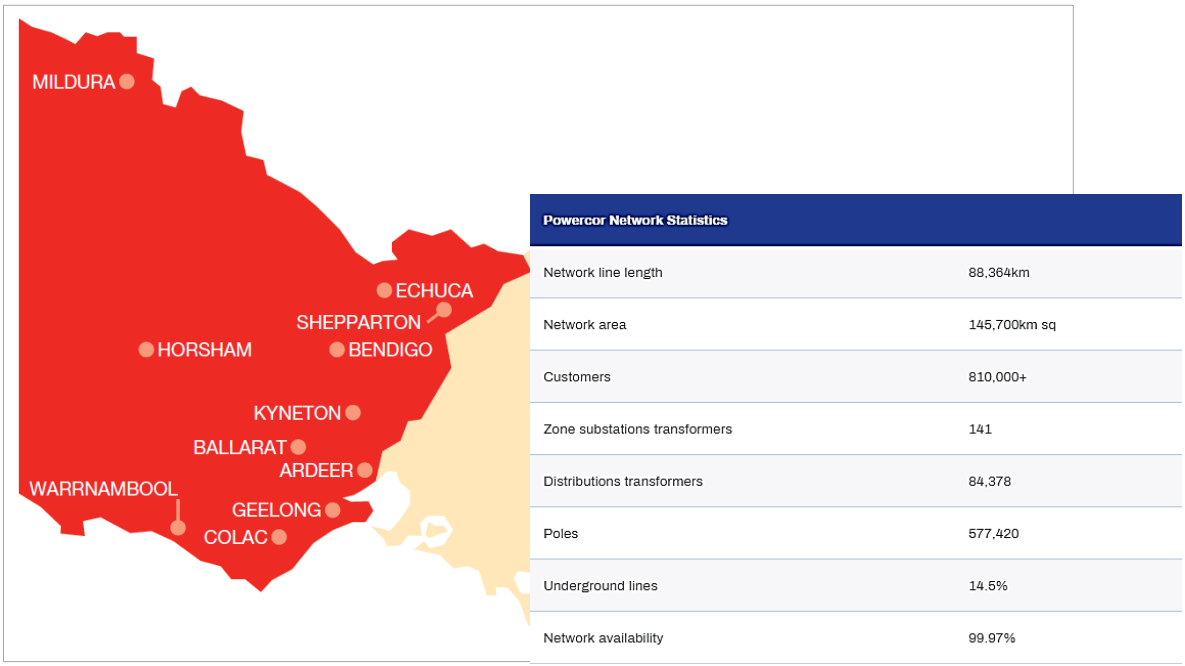


Figure 1-3 – CP Network area and overview of network statistics

Interaction between CitiPower and other adjoining Victorian Distribution Businesses is managed via the System Control Centre (SCC).

1.7.2 Powercor's Network

Our PAL network is the largest electricity distribution network in Victoria, servicing customers in central and western Victoria, as well as in Melbourne's outer western suburbs, as shown in Figure 1-4 below. Most of the network is overhead powerlines and the total length of the network is more than 67,000 kms. Key statistics about the network are also included in Figure 1-4. The network covers more than half the State and a lot of this is in Hazardous Bushfire Risk Areas (HBRA) in regional Victoria. The majority of our bushfire mitigation activities occur in our PAL network because of the large areas of HBRA.



Powercor Network Statistics	
Network line length	88,364km
Network area	145,700km sq
Customers	810,000+
Zone substations transformers	141
Distributions transformers	84,378
Poles	577,420
Underground lines	14.5%
Network availability	99.97%

Figure 1-4 – PAL network area and overview of network statistics

Interaction between Powercor and other adjoining Victorian Distribution Businesses is managed via our System Control Centre (SCC).

1.7.3 CP-PAL Network Assets Register

The network assets breakdown of CP-PAL assets is presented in Figure 1-5 below.

Company	Powercor Australia Limited
Reporting year	2018
Data consolidation	Consolidated Data
Data refresh date	10/01/2019
Report run date	10/01/2019
Status	in service
Asset group	**Total quantity installed**
Pole By Material Type	
Wood	365,142
Concrete	129,647
Steel	82,631
Total Poles	**577,420**
Overhead Conductors (excluding Services)	
Subtransmission - 66kV OHL conductor - (cct km)	3,186.37
Subtransmission - 22kV OHL conductor - (cct km)	0.00
HV - 22kV OHL conductor - (cct km)	34,544.23
HV - 12.7kV OHL conductor - (cct km)	21,386.28
HV - 11kV OHL conductor - (cct km)	54.86
HV - 6.6kV OHL conductor - (cct km)	0.00
LV - OHL conductor - (cct km)	9,557.06
PL - OHL conductor - (cct km)	22.29
Unclassified OHL	0.00
Total length of Overhead Conductors (Excluding services)	**68,751.09**
	59,171.74
Underground Cables (excluding Services)	
Subtransmission - 66kV UG Cable - (cct km)	3.50
Subtransmission - 22kV UG Cable - (cct km)	0.00
HV - 22kV UG Cable - (cct km)	1,939.27
HV - 12.7kV UG Cable - (cct km)	312.16
HV - 11kV UG Cable - (cct km)	17.60
HV - 6.6kV UG Cable - (cct km)	0.00
LV - UG Cable - (cct km)	4,410.84
PL - UG Cable - (cct km)	1,387.09
Unclassified UG C	0.00
Total Length of Underground Cables (Excluding Services)	**8,070.46**
Distribution Transformers	
Total number of Distribution Transformers	**86,044**
Zone Substation Transformers	
Total number of Zone Substation Transformers	**143**

Company	CitiPower Limited
Reporting year	2018
Data consolidation	Consolidated Data
Data refresh date	10/01/2019
Report run date	10/01/2019
Status	in service
Asset group	**Total quantity installed**
Pole By Material Type	
Wood	42,514
Concrete	4,622
Steel	10,987
Total Poles	**58,123**
Overhead Conductors (excluding Services)	
Subtransmission - 66kV OHL conductor - (cct km)	142.86
Subtransmission - 22kV OHL conductor - (cct km)	10.36
HV - 22kV OHL conductor - (cct km)	6.85
HV - 12.7kV OHL conductor - (cct km)	0.00
HV - 11kV OHL conductor - (cct km)	378.53
HV - 6.6kV OHL conductor - (cct km)	92.15
LV - OHL conductor - (cct km)	1,637.10
PL - OHL conductor - (cct km)	292.21
Unclassified OHL	0.00
Total length of Overhead Conductors (Excluding services)	**2,560.05**
	630.74
Underground Cables (excluding Services)	
Subtransmission - 66kV UG Cable - (cct km)	70.36
Subtransmission - 22kV UG Cable - (cct km)	88.35
HV - 22kV UG Cable - (cct km)	50.53
HV - 12.7kV UG Cable - (cct km)	0.00
HV - 11kV UG Cable - (cct km)	1,271.34
HV - 6.6kV UG Cable - (cct km)	135.25
LV - UG Cable - (cct km)	652.32
PL - UG Cable - (cct km)	397.43
Unclassified UG C	0.00
Total Length of Underground Cables (Excluding Services)	**2,665.58**
Distribution Transformers	
Total number of Distribution Transformers	**4,864**
Zone Substation Transformers	
Total number of Zone Substation Transformers	**98**

Figure 1-5 – CP-PAL network assets register

1.7.4 Vegetation Management

CP-PAL is responsible for vegetation management around overhead distribution lines and other electricity assets on its network. A principal objective of the vegetation management program is to minimise fire risk and ensure reliability by achieving and maintaining compliance with tree clearance requirements. Further information on our approach to vegetation management is provided in section 4.2.3.8 of the ESMS and within the CP-PAL ELCMP[3].

1.7.5 Network Configuration

Our network configuration and the location of critical assets such as zone substations and sub-transmission lines is shown in Figure 1-6 for our CP network and in Figure 1-7 for our PAL network.

[3] Electric Line Clearance (Vegetation) Management Plan - JEQA4UJ443MT-150-27661

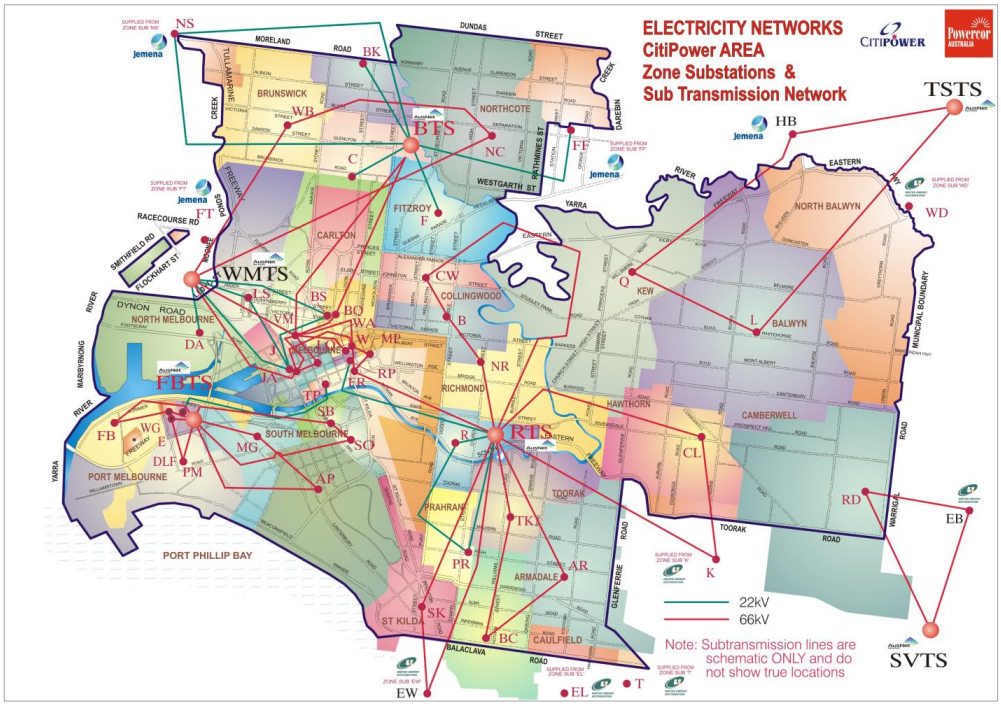


Figure 1-6 – Map of CP network configuration

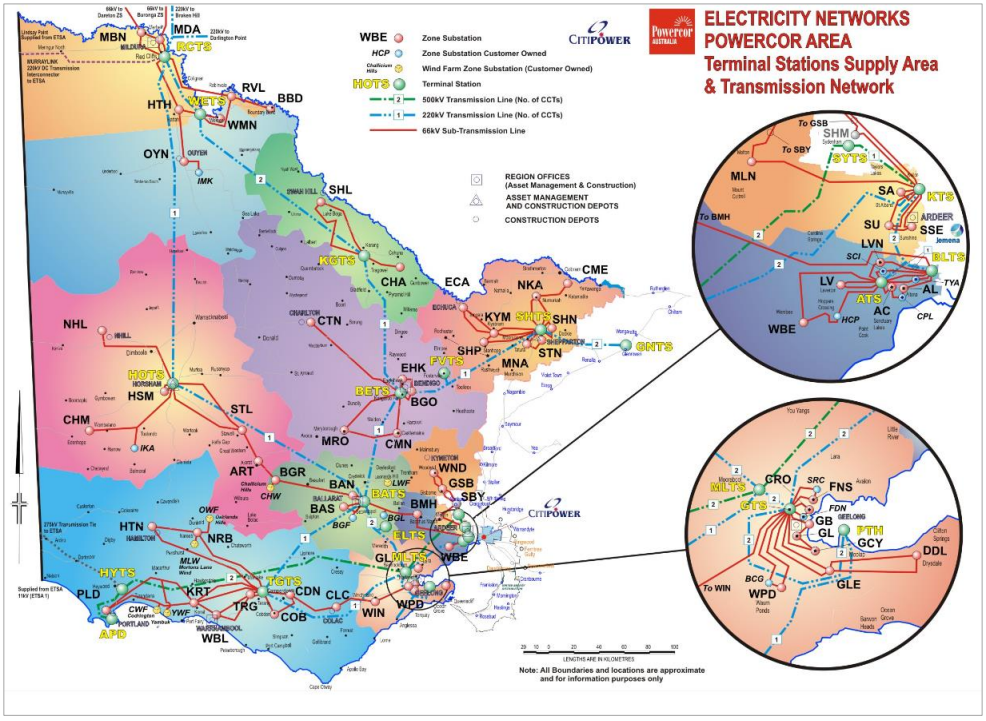


Figure 1-7 – Map of PAL network configuration

Sub-transmission network

The sub-transmission network supply electricity to zone substations, which then transform (step down) the voltage to one suitable for the distribution to the surrounding area. The Distribution Network consists of both overhead and underground lines connected to distribution substations, switchgear, and other equipment to provide effective protection and control.

The sub-transmission network is supplied from a number of Terminal Stations, which typically operate at a voltage of 220 kV. This Transmission Network, including the Terminal Stations, is owned and operated by AusNet Services. We have operational control of feeder circuit breakers from the terminal stations.

Our CP sub-transmission network in the CBD nominally operates at both 66kV and 22kV where:

- The 66kV Sub-transmission Network is generally configured in a multiple loop configuration for higher reliability than the suburban and rural networks and hence a higher level of supply reliability is achieved. Usually, three separate sub-transmission lines supply a zone substation.
- There is a 66 kV Switching Station at Waratah Place located near the centre of the CBD which provides a limited capacity transfer capability between CBD zone substations that are normally connected to two different Terminal Stations; and
- The 22 kV sub-transmission network is generally configured so that dedicated radial feeders supply each zone substation. Usually, three separate sub-transmission lines supply a zone substation.

Our PAL sub-transmission network in our rural areas consists of predominately overhead lines which operate at 66kV.

HV distribution network

Distribution feeders across CP-PAL networks are generally operated in a radial mode from their respective zone substation supply points and operate at either 11kV or 22kV. Most feeders can be configured in parallel to provide for load movement and other operational contingencies.

Customer connections

Our CP customer base comprises large commercial, industrial and residential customers, through to small domestic consumers, plus small unmetered supplies for communication equipment and public infrastructure like bus shelters. Our PAL customer base comprises large industrial and commercial customers through to small domestic and rural consumers in remote areas.

Supply to our smaller consumers is provided through low voltage distribution systems that nominally operate at 230 V or 400 V. These voltages are supplied from distribution substations located throughout the distribution network and typically range in size from 100 kVA to 8000 kVA for CP and from 5 kVA to 2000 kVA for PAL. Both overhead and underground low voltage reticulation, including service arrangements, completes the final connections to the low voltage consumer's points of supply. For long rural supply distribution, our PAL network also utilises Single Wire Earth Return (SWER) system as an efficient means of delivering power to our remote customers in low population density areas.

Supply to HV customers may occur at system voltages up to 66 kV depending on the capacity required. HV supplies for commercial or industrial customers are commonly configured in a radial arrangement from the feeder supplying other customers in the local area. Some HV customers with more critical supply requirements may also be supplied from dedicated feeders or from

multiple HV feeders with various changeover arrangements. These more critical supplies typically concern major hospitals, water supply or major chemical processing facilities. Some HV installations have the capability to provide generation capacity back into the local network from their normal or back-up generation capacities. The supply to HV customers can be overhead or underground and the customer is responsible for the installation of the HV metering equipment, isolation and electrical protection arrangements.

Interconnections

There are also a number of small areas in the west that are supplied from the South Australian network. These exceptions are a result of the customers remaining geographically isolated from Victorian supplies by large tracts of national parks or state forest. These areas are:

- In the far southwest of the state, there is a small SWER system operating at 19kV that supplies some nine low voltage customers north of Nelson;
- PAL also imports supply from the South Australian network at 33kV to supply the small township of Nelson in the far southwest of the state. We convert this supply to 22kV at the state border.
- We also have a number of interconnection points for embedded networks and embedded generation.
- In the far northwest of the state, supply is provided to some 50 customers in the Lindsay Point area directly from the South Australian three phase 33kV network. PAL has arrangements with SA Power for fault response and most maintenance activities.
- At Mumbannar, adjoining the South Australian border there is a complex of some 19 private poles. This is supplied from the South Australian system at low voltage. ESV had previously ruled this to be both a complex electrical installation and private overhead electric line.
- A number of remote area power supplies exist and operate independently from the PAL network.

Demand patterns

Climatic conditions have an impact on electricity demand, for example we experience a high demand for electricity during high temperature days due to the high use of air-conditioning.

Demand patterns vary between CP and PAL given the difference in customer profile. The customer load type, criticality of loads and the seasonal variances affect the demand.

Load types

CitiPower: Base load comprises high-rise domestic and commercial customers (CBD and Southbank precincts), some industrial customers (Port Melbourne facilities) through to small domestic consumers (inner suburbs of Melbourne). Customers can be connected at low voltage of 230/400 V, high voltages of 6.6/11/22 kV or sub-transmission at 22/66 kV voltage levels.

Powercor: Base load comprises large industrial and commercial customers (Altona and Laverton industrial areas) through to small domestic (regional cities) and rural consumers (western and northern veteran agricultural regions). Customers can be connected at low voltage 230/400V, high voltage of 22 kV or sub-transmission at 66 kV voltage levels.

Critical Loads

Due to their activity and importance to the wider community, the following customers are designated as having critical loads:

- major hospitals
- water sewage pumping stations
- critical transport traction supplies
- major buildings in Melbourne CBD such as Rialto, Eureka Tower, Crown and financial institution buildings (banks and ASX etc.)
- sports centres during special events, such as MCG (Grand Final) and Tennis Centre (Australian Open)
- terminal and zone substation service supplies
- feeders with interconnected co-generation customers
- life support customers

Electricity supply interruptions to these critical loads could lead to significant health impacts, significant financial losses and/or supply system security issues. Maintaining supply to Melbourne CBD is crucial due to the population within a small area and disruption it would cause including transport, infrastructure, retail sectors and movability within high-rise buildings.

Occasionally load shedding is used to assist in maintaining system stability and the balance between supply and demand on the national electricity supply system. It involves reducing consumption by specific amounts by turning off supply to groups of customers.

The Australian Energy Market Operator (AEMO) and the electricity industry work together to minimise load-shedding impacts on the community, particularly major health facilities, emergency services and public transport. However, these services can still be affected and are encouraged to have business continuity arrangements in place.

Life support customers registered with CP-PAL require greater notice and consultation regarding planned and unplanned outages. Information regarding life support services are located on the CP-PAL website[4].

1.7.6 Asset Types

CP-PAL both have a large population of assets distributed through the areas illustrated in Figure 1-6 and Figure 1-7. These assets include:

Poles and towers	Distribution transformers
Pole top structures	SCADA and communications
Overhead conductors	Zone switchgear
Underground cables	Protection and control
Zone transformers	Property and facilities
Distribution substation plant miscellaneous	Metering
Public lighting	Distribution switchgear
Zone substation plant miscellaneous	Service lines

Zone Substations are used to transform sub-transmission voltages (usually 66 kV) to HV distribution voltages (typically 11 kV or 22 kV) and to act as controlling points between differing HV networks. Zone substations usually have much greater capacities than distribution substations and supply a larger load area. There are 104 and 140 zone substation transformers in CP-PAL networks respectively. A typical zone substation is shown in Figure 1-8 below.

[4] https://www.citipower.com.au/our-services/life-support-services/

Figure 1-8 – Typical Zone Substation

Distribution substations transform HV distribution voltages (typically 11 kV or 22 kV) to power that can be used by households and most businesses (230/400 V nominal voltage[5]). These substations are mounted on poles (as shown in Figure 1-9 below), within buildings or inside small freestanding enclosures.

Figure 1-9 – Picture of a typical pole mounted distribution substation

Switchgear is used on both high and low voltages to control the flow of electricity and to take sections out of service for operational needs. They are located at various locations along the line to minimise customer disruption for planned or unplanned outages of electricity supply, such as circuit breakers as shown in Figure 1-10.

[5] AS/NZS 60038 and referenced in section 4.2 of the Electricity Distribution Code v9 Essential Services Commission

Figure 1-10 – Picture of a Circuit Breaker within a Zone Substation

Secondary, control and protection equipment is used to detect and isolate faults from the system. For example, protection relays detect faults by comparing the currents and voltages against pre-determined voltage, current and time settings. After a fault condition is detected, the relay will issue a command to open a circuit breaker. Other common protection equipment includes current and voltage transformers, fuses and surge diverters. The primary role of these systems is to prevent or minimise damage to circuits and apparatus. Control equipment enables the communication, monitoring and remote switching activities of switchgear. This includes SCADA (Supervisory Control and Data Acquisition) systems.

Earthing systems are low resistance connections from electrical assets down to the ground and are generally metal cables, straps or bars. They have several purposes:

- To ensure the safety of all people working in the substation by limiting the step and touch voltages that can occur under fault conditions.
- To allow fault and stray currents to be safely dissipated.
- In Zone substations and SWER isolating substations, they also connect the secondary windings of the transformers to earth in order to help maintain network voltages within the specified values with respect to earth and enable protection circuits to operate.
- To facilitate the return of an earth fault current from faults on the network it supplies to the source of the fault current.

Overhead lines comprise conductors strung on wooden, steel and concrete poles. The conductor materials used are most commonly aluminium, steel or copper. Conductors are usually bare at higher voltages and mostly insulated at lower voltages. The CP and PAL networks have approximately 4,310 km and 75,752 km of overhead lines respectively, which includes high and low voltage lines (including services).

Powercor's assets mainly consist of overhead lines, as illustrated in Figure 1-11.

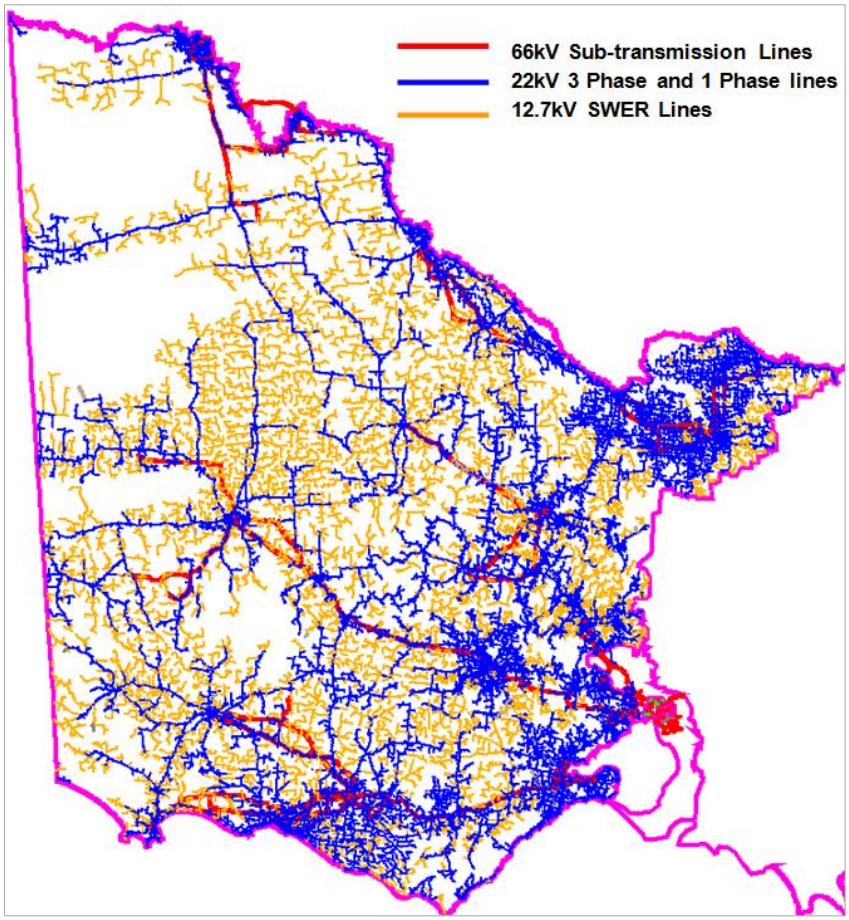


Figure 1-11 – Powercor's HV Overhead Network

Service lines (services) may be insulated with overhead or underground conductors. Most houses are connected to our LV networks via service lines.

Poles support overhead lines and we have approximately 624,972 poles within the CP-PAL distribution areas. This pole population consists of timber, concrete or steel as listed in Table 1-2 below:

Pole Type	CitiPower Network	Powercor Network
Timber	42,514	365,142
Concrete	4,622	129,647
Steel	10,987	82,631

Table 1-2 – Pole Population type for CP-PAL

Consumer metering refers to the electricity meters that are installed to measure the amount of electricity used by individual premises. The vast majority of consumer metering supplied by CitiPower and Powercor is commonly known as 'smart metering' and these devices can communicate, and be read or switched remotely. The Advanced Meter Infrastructure (AMI) is illustrated below in Figure 1-12.

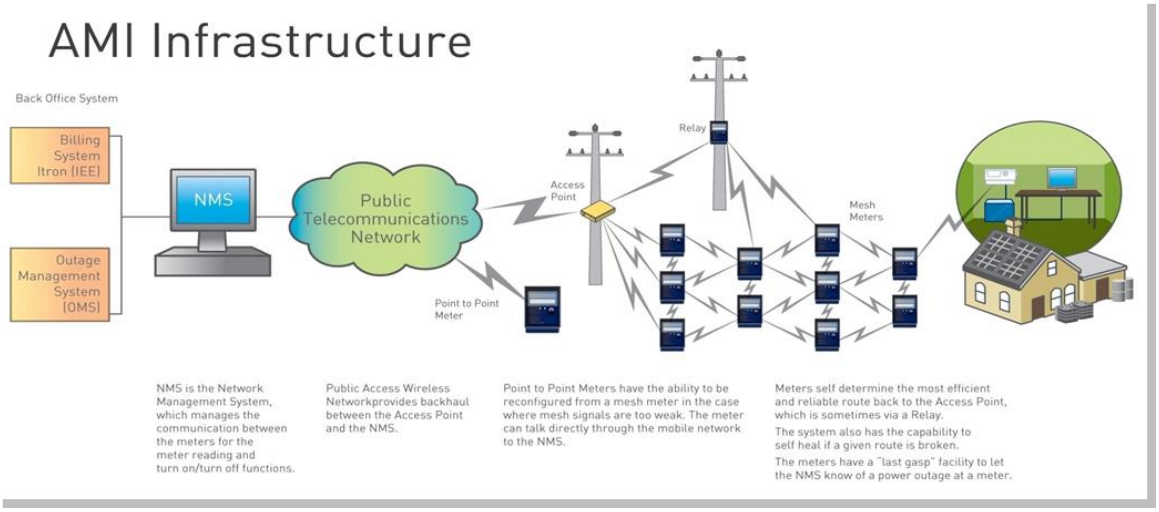


Figure 1-12 – Advanced Metering Infrastructure

Private lines within the geographic area served by CP-PAL are listed as private high and low voltage lines. These are not network assets and are connected at a point of supply. CP-PAL has statutory responsibilities for the inspection and notification of defects for some coverage that may have private lines.

Underground cables are used in areas like the Melbourne CBD or within more recent residential subdivisions. These cables commonly run between substations and supply the immediate area. There is a small volume of underground cabling associated with the sub-transmission system. These cables are buried under the ground to provide some protection against interference. In Powercor network, there are a number of new areas that have regulated requirements based on design standards that include undergrounding of cables to reduce bushfire risk. Undergrounding cables will see a progressive increase over time. Approximately 42% of the CP distribution network cables exist underground and 12% of the PAL cable networks.

Public lighting includes street lighting for vehicle or pedestrian visibility, public space lighting such as (public parks, gardens, car parks, bike paths) and also feature lighting in commercial and industrial areas. Municipalities and road management agencies are usually responsible for the determination of where lighting is required with CP-PAL installing, maintaining or owning the light fittings. Most lighting equipment that is currently installed is energy efficient. A number of municipalities have embarked in programs to change existing public lighting lanterns to accommodate more efficient LED lighting.

1.7.7 Asset Age Profile

Our electricity assets were previously owned and operated by the State Electricity Commission Victoria (SECV) and were privatised in 1994. There was a significant drive to electrify regional Victoria through the 1960's, 1970's and 1980's which resulted in a large volume of new assets being constructed during this period. The volume of constructed assets during the 1960's to the

1980's is shown in the age profile graphs below (Figure 1-13 and Figure 1-14) for both our CP-PAL networks.

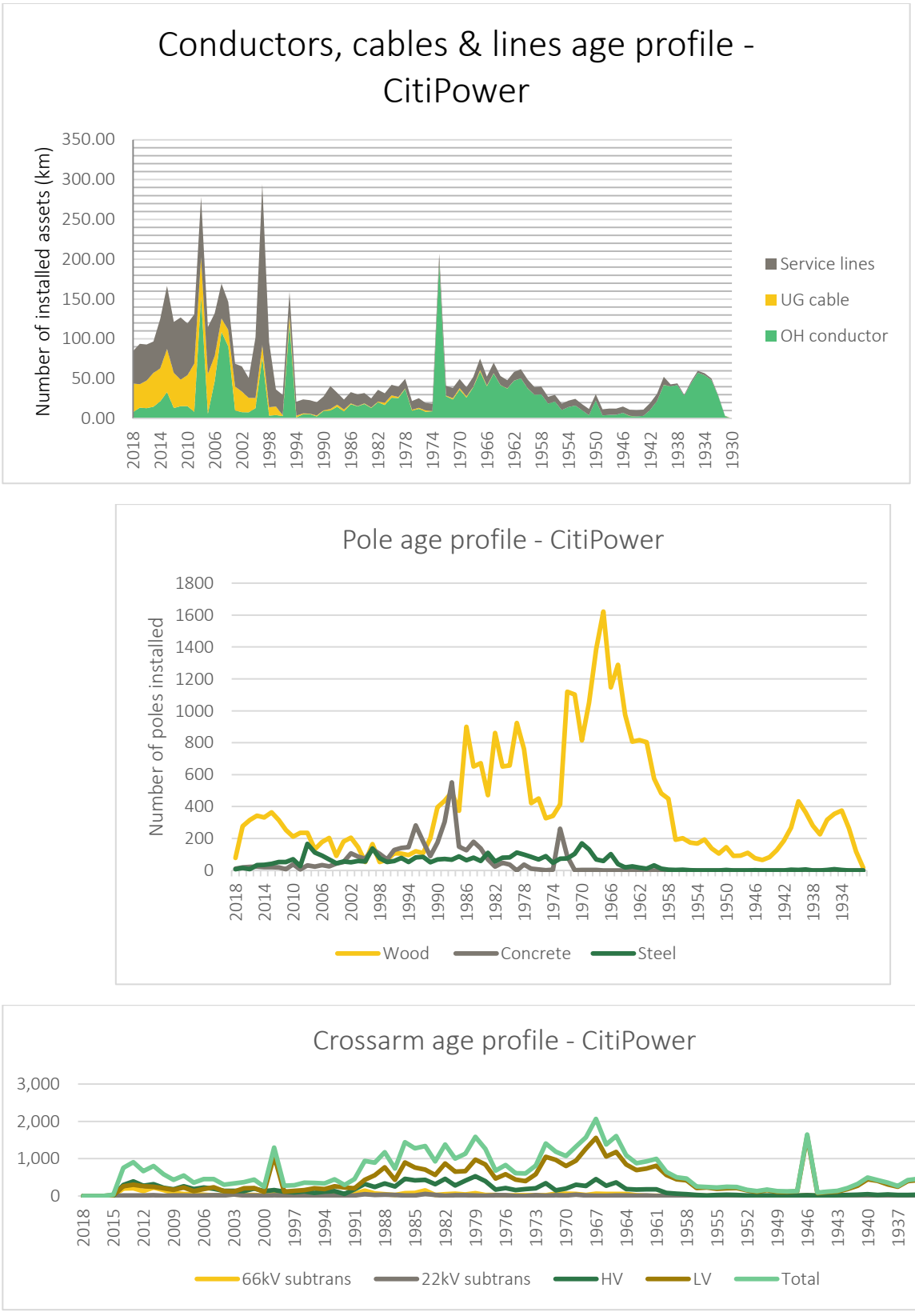


Figure 1-13- CitiPower's asset age profile

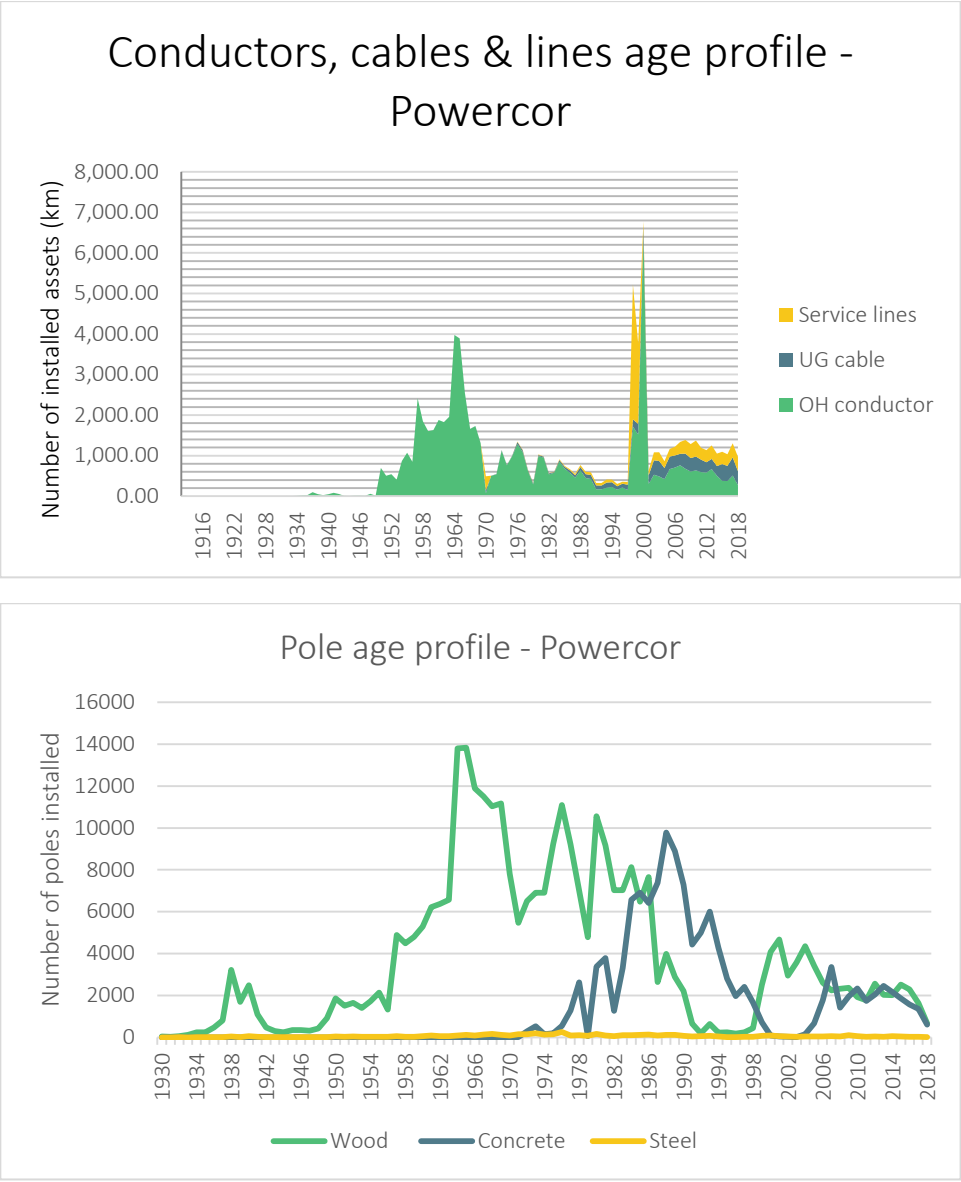


Figure 1-14- Powercor's asset age profile

There was also a considerable surge in investment in the 1930's, particularly for CP's 22 kV sub-transmission network, located in inner Melbourne (see Figure 1-13).

Much of this network is still in use today. These older assets are now reaching an age at which future deterioration could pose a reliability risk, which is why we continue to invest in upgrading the network, decommissioning several smaller zone substations and connecting customers to the more modern 66 kV sub-transmission network.

Our PAL network covers some of the fastest growing regions in Australia (the western suburbs of Melbourne, Greater Geelong and agricultural regions along the Murray River and south west Victoria). As a result, ageing assets such as powerlines and transformers will need to be progressively replaced to maintain safety and to protect the quality and reliability of electricity supply to customers. We need to continuously monitor and assess the overall health and condition of our assets to ensure that investment in asset replacement is timely and prudent.

1.8 Network Interaction with External Stakeholders

1.8.1 Third-Party Interactions

As CP-PAL assets are located in the public domain, we have experienced an increase in physical security incidents including unauthorised entry into substations, graffiti, theft from depots and company vehicles and wilful damage.

Copper conductor theft is the most common driver for breaking into and entering network installations and depots. Unauthorised entry to substations gives rise to a number of network safety issues including risk of electric shock and fire ignition.

The great majority of incidents involving serious injuries and fatalities on our network are due to 3rd party contacts with overhead assets involving mobile plant (tip trucks, excavators and farm equipment) i.e. No Go Zone Infringements, vehicles and aircrafts coming into contact with poles and overhead lines respectively.

1.8.2 Infrastructure Works in Road Reserves

In 2004 the Roads Management Act (RMA) was established for the purpose of managing roads with Consent and Completed Works Notifications to Co-ordinating Road Authorities (CRA's within the CP-PAL area being 50 Councils and two VicRoads areas) and subsequent regulations and Code of Practice (CoP) for managing Works and Infrastructure by Utilities, providers of public transport and CRA's. These regulations and CoP can also provide certain exemptions from the consent process for 'Minor' works.

In 2016 CP-PAL processed 1371 Consent applications and 3758 Completed Works notifications to CRA's. To manage the Consent process CP-PAL have dedicated Statutory Compliance Officers to

manage these applications for with the CRA's or make a determination for internal queries as to whether works require Consent or are exempt as Minor Works.

CP-PAL have a Road Management Consent procedure[6]. This procedure ensures the installation and maintenance of CP-PAL Electricity Distribution Business Assets located in road reserves is managed to comply with the requirements of the Roads Management Act 2004 (RMA) and subordinate legislation such as, Regulations and Codes of Practice. To ensure that all stakeholders involved within the process are aware of, and meet, their responsibilities and obligations under the Act.

Also assisting this is a Road Management (exemption statement) form and various work instructions.

CP-PAL actively participate in the Roads Management Steering Committee managed by VicRoads in delivering subsequent Regulation and CoP to the RMA and also the Utilities Infrastructure Reference Panel (UIRP) delivering recommendations to the Roads Minister. CP-PAL also represent the other Distribution Businesses of the Victorian Electricity Supply Industry.

1.8.3 Rail Crossings and Rail Corridor Occupation

Applications for new CP-PAL rail crossings with our underground or overhead infrastructure or maintenance on existing infrastructure requiring works within or affecting the Rail Corridor of VicTrack/Rail Operator assets. In 2016 CP-PAL processed 135 applications for works in the VicTrack Rail Corridor. This is managed through dedicated statutory compliance officers.

To assist are CP-PAL – Railway Crossing Application and Approval Procedure[7] and Construction, Audit and Completion process along with VicTrack guidelines.[8]

1.8.4 Shared Use of Poles

To minimise the amount of street furniture and potentially reduce costs to the community, third parties request to collocate their infrastructure on our poles.

Shared use of poles may result from rights conferred by permits issued under the Australian Communications Act (Cth), through the exercise of carrier rights under the Telecommunications Act (Cth), and contractual arrangements established with the joint user party.

[6] Road Management Consent Process Procedure – 20-30-P0001

[7] Railway Crossing Application and Approval Procedure – JEQA4UJ443MT-173-103

[8] VicTrack Design Drawing Criteria for 'In Principal' Review

Shared user organisations can include anybody requiring access to a pole. Commonly these organisations include road authorities, telecommunication companies and municipalities. Examples of this include:

- Attachment of streetscape signage
- Banners
- Communication cable with steel catenary support
- Telephone leads to customer premises
- Dielectric self-supporting fibre optic communication cabling
- Cellular mobile telephone antennae
- Tramway conductors
- Security cameras
- HV or LV power lines of other network operators
- Private installation power lines
- VicRoads 'Raptor' Barriers at the base of poles for increased community protection against vehicle strikes when VicRoads standard barrier systems are not suitable. CP-PAL has worked with VicRoads on trial areas previously

In these circumstances, we establish a Facilities Access Agreement including applicable Australian Standard requirements. Shared use and access to our poles does pose an increased risk and we have significantly increased efforts to minimise such risks by focusing on establishing audited contractual arrangements with heightened control and minimum technical and training competency requirements[9] for parties installing and removing attachments to our poles.

1.8.5 Community Awareness

Our assets are located on public and private land where other activities such as construction and farming are also undertaken. Therefore, it is important to have processes in place that allow third parties to safely work in the vicinity of our assets.

Community awareness is critical to reduce risk of the public harming themselves by interfering with electrical infrastructure. Our Network Safety group actively promotes public safety in the vicinity of our assets through the 'No Go Zone'[10], 'Look Up and Live'[11] and 'Dial Before You Dig'[12] initiatives, including awareness presentations at various farm field days. The field days involve CP-PAL handing out safety pamphlets and delivering our electricity safety message.

[9] VESI - Safety & Compliance Training Requirements for Telecommunications Work on Victorian Electricity Supply Industry (VESI) Network Operator Assets

[10] CP-PAL, «No Go Zones» https://www.powercor.com.au/electrical-safety/safety-around-our-networks/no-go-zones/

[11] http://www.esv.vic.gov.au/merchandise/look-up-and-live/

[12] https://www.1100.com.au/

CP-PAL works in partnership with ESV attending farm field days promoting joint message of public safety. Before any work is allowed to commence around our assets, a 'Permit to Work' needs to be obtained using the online application process[13] in accordance with the *Permit To Work Procedure*[14]. A permit will only be issued once the work site has been visited, assessed and all potential electrical hazards are mitigated AFAP.

1.9 Other Network Supporting Systems

Information Technology systems are also used to provide critical support to key network assets and their operation. Our CP-PAL systems operate under a common core of IT hardware and software applications:

- The SAP R/3 Mainframe Business Software Solution (SAP) system
- Geographical Information System (GIS)
- Supervisory Control and Data Acquisition (SCADA) systems
- The Advanced Metering Infrastructure network management system
- Map Insights
- Network Fault Data application

1.9.1 SAP R/3

The SAP R/3 system is our integrated business software system that covers the following functions:

- Financial Management
- HR
- Payroll
- Accounts Payable
- Materials Management
- Asset Management
- Non electricity billing
- Business Reporting

The key function being Asset Management, we utilise SAP to record our asset information including inspection records and asset condition. This information feeds into works planning and assists in asset management decision making.

[13] CP-PAL, «No Go Zones» https://www.powercor.com.au/electrical-safety/safety-around-our-networks/no-go-zones/

[14] Permit To Work Procedure – 18-75-P0003

1.9.2 Geographical Information System and Outage Management System

Geographical Information System (GIS) is an electronic mapping system linked to a database of information relating to each item on the map. GIS is the main system for recording the spatial location of all asset records and for the creation and maintenance of asset records within SAP. GIS is updated with all "as built" construction information, which is then sent up to SAP for ongoing asset maintenance.

GIS is also the "database of record" for the electrical connectivity models for the CP-PAL network and provides an update of this model to the Outage Management System (OMS) on a daily basis. It provides near real-time outage information to a number of customer communication channels including SMS messaging to consumers, Interactive Voice Response (IVR) messaging providing automated messaging to consumers who contact our call centre as well as the company website and publicly-available outage app (Apple or iOS based application available from the Apple App Store).

1.9.3 Supervisory Control and Data Acquisition

Supervisory Control and Data Acquisition (SCADA) systems are widely used where complex processes need to be monitored and managed. CP-PAL uses SCADA for 24/7 remote monitoring and control of its network from the permanently manned control room in our Head Office at 40 Market St Melbourne, Victoria.

1.9.4 Advanced Metering Infrastructure

Following the Victorian Government's initiative to equip customers with smart meters, we deployed 1.2M 'smart meters' across all our customers. This shifted the frequency of meter reading from three monthly to daily downloading of 30-minute interval readings.

Our smart meters use an AMI Network Management system to manage the AMI meters and the related Radio Frequency mesh communication infrastructure. Radio Frequency mesh communication infrastructure is a communication network made up of radio nodes that are organised in a mesh topology i.e. in which each node relays data for the network.

The functions performed by the system include:

- Operational management of all AMI devices (including meters)
- Management of the communications devices (Access Points & Relays)
- Meter event reporting
- Collection of interval meter data
- Operational management
- Remote provisioning services (remote connections).

1.9.5 Map Insights

Map Insights is one of our spatial analysis applications used for visualising business information in spatial reference to other business or third party information.

The current functionality of the system includes the following:

- Overlay of CP-PAL's assets
- Zone substation, distribution substation and feeder asset searches
- Streaming of current and historical fire data from CFA and DSE
- Streaming of weather information e.g. radar, lightning and observations
- Fire warnings and alerts
- Property address searches
- Google street view
- Co-ordinate locations at curser positions in Latitude and Longitude
- Fire/non-fire areas (HBRA/LBRA)
- CFA fire footprint overlay.

1.9.6 Network Fault Data Application

Network Fault Data (NFD) application is another of our key IT support systems. It is an iPhone/iPad application developed for use by our employees. NFD contains near real-time fault information sourced from our Outage Management System (OMS) and updates every five minutes. This helps us to respond quickly to faults and incidents on the network and coordinate resources.

Figure 1-15 – 'Network Fault Data' App screenshot (iPhone)

Section 2. POLICY AND COMMITMENT

This section addresses the clause 4.2 of AS 5577:

> *4.2 – Policy and Commitment*
>
> *The Network Operator shall define its policy and commitment towards the various aspects of operating the network safely.*
>
> *A clear commitment by the Network Operator towards specific outcomes shall form the basis of the ENSMS.*

2.1 Network Safety Policy[15]

The Network Safety policy for CP-PAL is:

The health and safety of all employees, contractors, customers and the general public is CitiPower and Powercor's highest priority. CitiPower and Powercor are committed to managing its electricity supply networks to minimise as far as practicable:

- The hazards and risks to the safety of any person arising from the electricity supply network ;
- The hazards and risks of damage to the property of any person arising from the electricity supply network; and
- The bushfire danger arising from the electricity supply network.

CP-PAL has established policies that demonstrate a commitment towards the safe operation of the network, of which are discussed in the following sections.

2.2 Enterprise Risk Management Policy[16]

The Enterprise Risk Management (ERM) policy provides a comprehensive statement of Victoria Power Networks Pty Ltd.'s (the Business') policy, for the management of risk across a distribution business.

[15] CitiPower-Powercor Network Safety Policy March 2018

[16] Enterprise Risk Management Policy - JEQA4UJ443MT-154-85

2.3 HS&E Policy[17]

The health and safety of employees, contractors, customers and the general community is CP-PAL's highest priority.

We live safely. We never compromise health and safety.

To achieve this safety commitment, all employees strive to adopt a 'whole of life' approach to safety in the workplace, placing specific emphasis on:

- Strong and visible leadership
- Promoting a culture of cooperation, commitment and responsibility, where safe behaviours are recognised, promoted and rewarded
- Ensuring adherence to health and safety policies, systems, practices and expectations
- Intervening when unsafe acts or conditions are observed
- Proactively identifying hazards and minimising risk during all aspects of the planning, design and construction of projects
- Ensuring all employees understand the hazards associated with their work, the relative risk associated with each hazard, and the controls required to minimise risk exposure
- Ensuring our contractors understand, follow and promote this policy and all relevant sub-policies
- Regularly and effectively consulting with each other about health and safety
- Adhering to all relevant laws and management system requirements
- Preserving the safety of the public in all matters under our operational control
- Holding all employees accountable for achieving challenging and transparent health and safety targets and objectives
- Driving continuous improvement and innovation in health and safety behaviours and performance.

2.4 Asset Management Policy[18]

CitiPower and Powercor are committed to providing our customers with a safe, reliable and affordable supply of electricity through the application of an effective asset management framework. Asset management activities must meet business objectives and benefit the current and future needs of all customers, stakeholders and employees.

[17] Health and Safety Policy - 14-00-CP0001

[18] Asset Management Policy – A-001

2.5 Vegetation Management Policy[19]

The CP-PAL Vegetation Management policy requires to minimise the risk to the community and the environment caused through the interaction of trees and powerlines, CP-PAL are obligated and committed to comply with the requirements of the current Electricity Safety (Electric Line Clearance) Regulations 2015.

2.6 Other Management System Policies

Records Management Policy [20]

This Policy identifies the principles which govern the management of records for CitiPower Pty, Powercor Australia Ltd, Powercor Network Services Pty Ltd (PNS) and CHED Services Pty Ltd. Records management must support business operations, cater for future expansion, enable statutory and other requirements to be met, facilitate secure access to records based information and keep up-to-date with user needs and new ways of record management.

Purchasing and Procurement Policy [21]

The Policy is to establish principles and practices that govern Business purchasing and procurement activities for all goods, materials, services and intellectual property assets ('goods and services') to ensure quality and safety standards are achieved.

How CP-PAL meets the commitments of these policies is further described in sections 3 through 6.

[19] CP-PAL ELCMP – Reference H Vegetation Management Policy

[20] Records Management Policy – JEQA4UJ443MT-153-36

[21] Purchasing and Procurement Policy – JEQA4UJ443MT-156-43

Section 3. PLANNING

This section addresses the clause 4.3 of AS 5577:

4.3 – Planning

4.3.1 – General

The Network Operator shall have appropriate planning processes and procedures for ensuring network safety in any situations that may result from normal and foreseeable abnormal operations including emergencies.

4.3.2 –Planning for safe operations

When developing the ENSMS, the Network Operator shall utilise a Formal Safety Assessment undertaken in compliance with this Standard (see Appendix A).

The ENSMS shall have appropriate processes and procedures for the production of Formal Safety Assessments. The Formal Safety Assessment shall comply with the principles of AS/NZS ISO 31000 and shall include methodologies appropriate to the network under consideration for the following:

(a) Establishing the context of the specific assessment being undertaken and including the setting of risk acceptance criteria.

a. Risk identification—recognising sources of risk external to the electricity network as well as those arising from the electricity network itself.

b. Risk analysis, including consideration of the consequences of the risks and the likelihood of the consequences occurring.

c. Risk evaluation by comparison of the level of risk with risk acceptance criteria.

d. Risk treatment, including where reasonably practicable the elimination of the source of risk and where elimination is not reasonably practicable, the identification of

e. Treatments or controls so that residual risks are reduced to as low as reasonably practicable (ALARP).

Control measures required to reduce safety risks to the public, property, the environment and network personnel to an acceptable level shall be incorporated into the appropriate procedures.

The Network Operator shall ensure that any Formal Safety Assessment carried out considers activities related to the following:

i. *Network planning.*

ii. Site safety management

iii. Network safety management incorporating—

a) network structural integrity
b) external interference management
c) fault condition monitoring and response; and
d) change of operating conditions and remaining asset life review

iv. Substation's operations and maintenance

v. Emergency response.

4.3.3 - Planning and preparation for abnormal operations

The Network Operator shall plan and prepare for operation of the network in foreseeable abnormal circumstances or during significant disruption to normal operations. These circumstances may include the following:

(a) Operating connected to emergency power sources.
(b) Operating without normal supply assets such as powerlines or transformers.
(c) Operating at other than normal voltage levels.
(d) Operating under communication outages.
(e) Operating under changed conditions to avoid further damage to the network.

NOTE: AS 3745, Planning for emergencies in facilities, provides guidance. See also Clause 4.4.7.

4.3.4 - Standards and codes

4.3.4.1 - Published national or international technical standards

A Network Operator shall identify the published national or international technical standards used by it in—

(a) the design and construction of existing network assets;
(b) design and construction of new network assets; and
(c) the commissioning, installation, operation, maintenance and decommissioning of network assets.

If the Network Operator chooses not to use an applicable relevant standard or chooses not to comply with particular provisions of that standard, the Network Operator shall document—

(i) the reason for the non-use of or non-compliance with the standard; and
(ii) the alternative provisions for the design, construction, commissioning, installation,

operation, maintenance and decommissioning of network assets that will ensure a level of safety in relation to those activities that is at least equal to or greater than the level of safety that would ensue from compliance with that standard.

4.3.4.2 - Industry/company codes

A Network Operator shall identify the industry or company codes used by it in—

(a) the design and construction of existing network assets;
(b) the design and construction of new network assets; and
(c) the commissioning, installation, operation, maintenance and decommissioning of network assets.

If the Network Operator chooses not to comply with particular provisions of an industry or company code, the Network Operator shall document—

(i) the reason for the non-compliance with the code; and
(ii) the alternative provisions for the design, construction, commissioning, operating,

maintenance and decommissioning of network assets that will ensure a level of safety in relation to those activities that is at least equal to or greater than the level of safety that would ensue from compliance with that code.

3.1 Planning for Safe Operations

CP-PAL plan for safe operations via effective identification and management of operational hazards and risks, potentially exposing the Business to unexpected variations around objectives. The CP-PAL Corporate Risk Management Framework (as detailed below) assures the Business maximises opportunities whilst avoiding unacceptable levels of risk.

3.2 Risk Management Framework

CP-PAL applies an Enterprise Risk Management Framework (ERM), integrating each component of the company's approach to risk management at all levels of the business, as illustrated in Figure 3-1. This provides a consistent framework for the identification, assessment and control of risks[22], integrating risk analyses from HSE and Asset Management into the safety risks presented in the ESMS. The ERM framework is based on the AS/NZS ISO 31000.

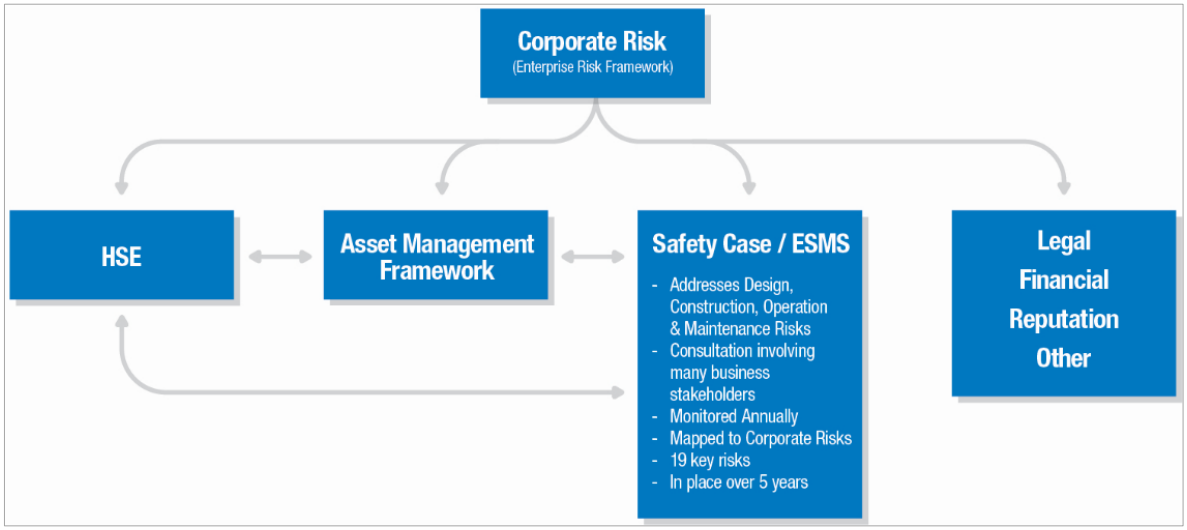


Figure 3-1 – Enterprise Risk Management Framework

The purpose of the ERM is to manage uncertainties that could restrict business performance and achievement of objectives. Implementing an effective ERM provides:

- Oversight: All critical risks have been identified and are being managed and monitored under a holistic approach, consistent with the board approved risk appetite statement.
- Ownership and Responsibility: The ownership of risk is assigned to management personnel responsible for identifying, evaluating, mitigating and reporting risk.
- Assurance: The board and senior management have reasonable assurance that risk is being appropriately managed within defined levels to bring value to the Business.

[22] Enterprise Risk Management Framework – JEQA4UJ443MT-154-354

3.3 Risk and the Planning Process

CP-PAL has two main levels of risks within the Business: strategic level risks and operational level risks. ESMS risks are planned at an operational level.

Strategic risks

Strategic risks relate directly to strategic planning and process and are those risks which could significantly impact the achievement of the businesses vision and strategic objectives. These risks are broad, high level and may be applicable over the longer term, for example, over the next 3 to 7 years. These risks do not often change and are coupled with long term goals. Strategic risks become an input to decision making on the direction of the business.

An analysis of the changes to the PESTEL (Political, Economic, Social, Technological, Environmental and Legal) environment is often useful in reviewing strategic risks.

Operational risks

Risks that are associated with the objectives of a particular department and are an input to decision making at department level. These risks may impact the organisation over the short-medium term, for example, 6 months to 2 years, depending on the objective that the risk relates to. The SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis is useful to apply in identifying these risks.

The process is illustrated further in Figure 3-2:

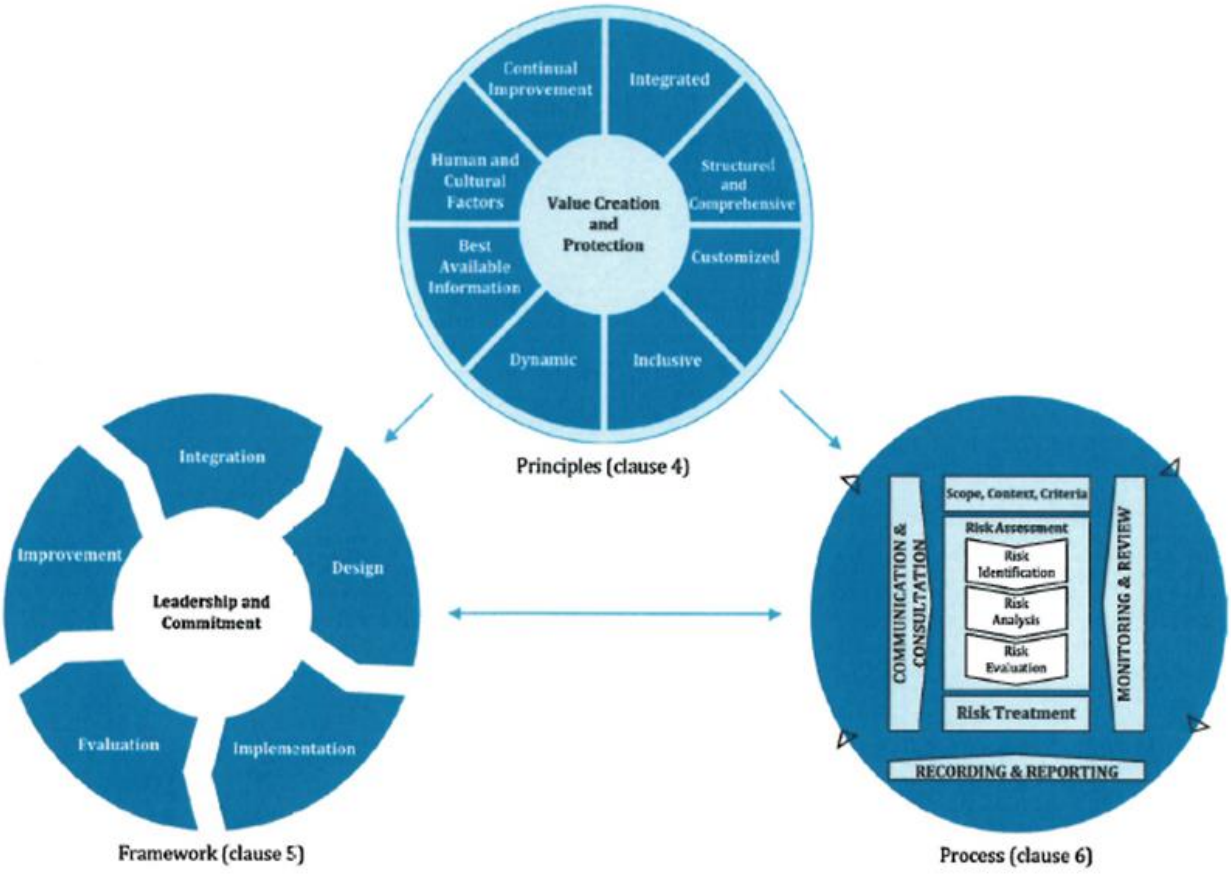


Figure 3-2 – Risk principles, framework and process

The ESMS risk management process follows the ERM framework and complies with the Australian Standard for Risk Management AS/NZS ISO 31000, as summarised in Figure 3-3 below.

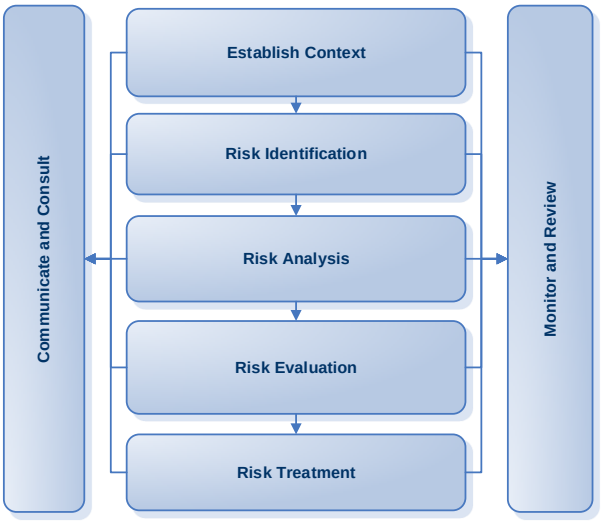


Figure 3-3 – CP-PAL's Risk Management Process

Sections 3.3.1 – 3.4 details planning for safe operations via effective identification and management of operational hazards and risks using the ERM framework.

3.3.1 Establish Context

Prior to risk identification and analysis, it is important to establish the context for the assessment, as per AS/NZ ISO 31000. Section 1 of this ESMS describes the network and key challenges that form the basis for establishing the ESMS Risk context.

Key network challenges (i.e. the internal and external environmental factors) that help to inform risk identification include:

- Technical challenges:
  - Network status/condition and performance
  - Network configuration
  - Geography and climate
  - Asset complexity
  - Asset management and maintenance
  - Vegetation management
  - Resources and training
  - Network for the future
- Management challenges:
  - Changes in commercial arrangements, ownership or budgetary controls

- Contracting arrangement or effects
- Resource management
- Local body jurisdictional issues
- Other management issues such as regulation

Risks were established to meet regulatory requirements with a focus on electrical safety of persons (general public, direct contractors and employees), damage to property (third party and network assets) and fire ignition. Interruption of supply was considered as an interim stage of an event that could lead to further consequences such as fatality (for persons relying on life-support equipment), personal injury or property damage (caused by traffic accidents).

3.3.1.1 Communication and Consultation

As per AS/NZS ISO 31000, communication and consultation with stakeholders takes place throughout the risk management process.

Risk identification and cause determination are completed at Formal Safety Assessment (FSA) workshops, allowing for control procedures to be created and stored in a Risk Register.

Network Safety facilitates these workshops, which include Subject Matter Experts (SMEs) who provide consultation regarding:

- Design
- Planning
- Technical Standards
- Asset Management
- Work Practices and Field Construction
- Network Control and Operations
- Other supporting systems such as: Risk Management, IT and Finance

Upon completion of the FSA process, all outcomes are communicated to management[23].

Risks are verified on a bi-annual basis via a risk profiling process[24], which is completed by Risk and Control Owners. The outcomes of the risk profiling are reported to the Executive Management Team (EMT) and the board.

The criterion for reviewing top ten risk identification includes:

- Any risk, which is residually rated as Extreme, and High will be automatically included in the top risk list, which is consistent with our Framework
- EMT discussion around what risks should be included for review and discussion with board

[23] CP-PAL Full Safety Case Table 1 – 2 - CP-PAL's Management Response to Identified Risks

[24] Enterprise Risk Management Framework – JEQA4UJ443MT-154-354

3.3.2 Risk Identification

CP-PAL identifies the risk by the process highlighting:

- Sources of risk (i.e. hazards) associated with CP-PAL electricity networks.
- Areas of impact, based upon regulatory requirements and operating environments.
- Risk events that lead to specific consequences and their likelihood, assessed by SMEs utilising incident statistic data and historical Risk Register review.
- Causes (i.e. triggering mechanisms) of each risk event, through root cause or fault tree analysis methods.
- Potential consequences (i.e. physical impacts).

3.3.2.1 Risk identification

Risk is defined as "the effect of uncertainty on objectives." (AS/NZS ISO31000:2018 Risk Management – Principles and Guidelines). A risk is an event that could happen in the future which could impact our ability to achieve our objective(s). Current facts are not risks.

Risk identification involves the description of a risk event, the cause/s of that event and the impact/s of that event. Example risk description is noted in Figure 3-4.

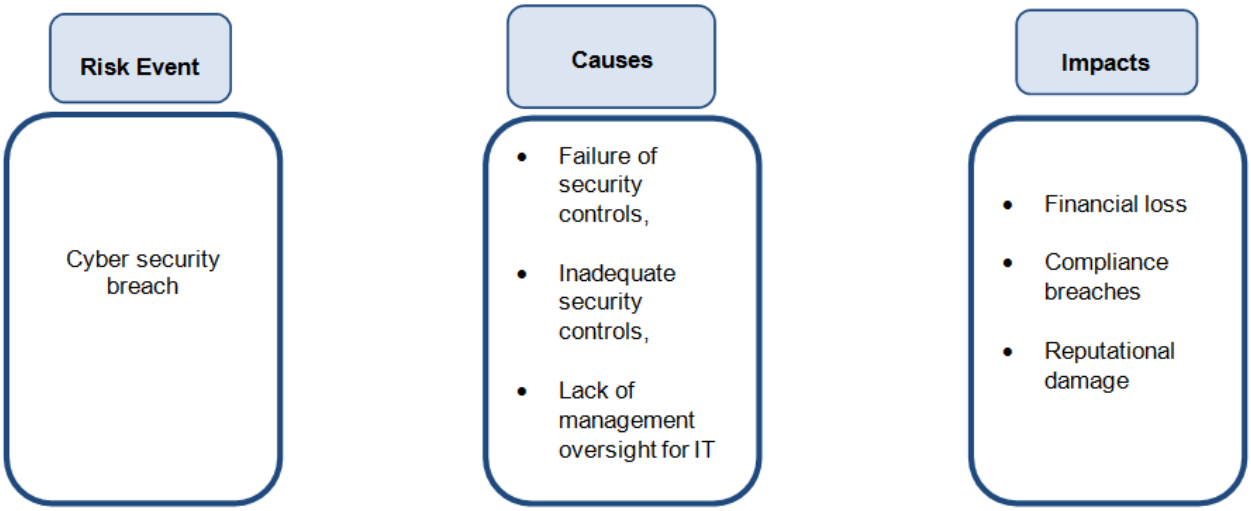


Figure 3-4 – CP-PAL's Example risk description

Identification of risks from various sources

We may identify risks through the analysis of changes in the external and/or internal environment. For example, changes in the legal/regulatory environment or changes in our internal capabilities/resources would impact our ability to achieve our objective(s). We may also identify risks based on past events, through the review of our goals and objectives, audit issues and future trends.

Risks relevant to electricity network safety (e.g. bushfire, electrical shock or injury, property damage and supply interruption) are selected from enterprise risk and are used for ESMS FSAs and reviews.

With network assets installed in the public domain, the following items are considered to be the main hazard groups to electricity networks and/or the general public:

- Network assets in unsafe situations (including activities related to site safety management)
- Persons or equipment in contact or interference (internal and external) with network assets
- Failure of network assets
- Network structural integrity
- Fault condition monitoring and response
- Change of operating conditions and remaining asset life review
- Substations operations and maintenance
- Emergency response
- Bushfire resulting from fire ignition associated with network assets.

3.3.2.2 Significant Risk Impact Areas

An isolated incident could lead to multiple consequences. After analysing the consequences associated with historical incidents using Cause-Event-Consequence analysis, four significant risk impact areas were identified:

- Fire ignition
- Electric shock or personal injury (including fatality)
- Property damage and
- Interruption of supply

Figure 3-5 – Risk Impact Areas

3.3.2.3 Initiating Causes and Risk Events Identified

By analysing historical incidents up to 2004, the following possible causes were identified:

1. Personal and equipment contact or interference:

- 3rd party work or equipment in proximity
- Employee or direct contractor work in proximity

- General public lack of understanding of electrical hazard
- Vandalism, sabotage or unauthorised access (copper theft)

2. External interference

- Animal, bird or termite interference
- Aircraft contacting OH assets
- Tree or vegetation contact
- High vehicle contacting OH assets
- Severe lightning storm or high wind events
- Water ingress or flooding
- External fire
- Natural disaster or major event
- Electricity loading increased
- Vehicle collision
- Impacted by adjacent infrastructure or utility: accumulated fume or flammable gas

3. Network internal factors

- Asset internal defect, corrosion or deterioration
- End of asset service life
- Movement of asset over time
- Equipment unfit for purpose
- Design deficiency
- Inadequate clearance
- Poor workmanship or work practices
- Operational or human error
- Incorrect asset location, depth or records
- Work order (instruction) error or misinterpretation

4. Other factors

- Open trench work
- Ground surface level of assets changed
- Assets at ground level in vulnerable location

Nineteen ESMS risk events/scenarios were then developed to describe particular sets of circumstances (based on four main hazards) with possible causes and relevant consequences linked in groups for risk assessment purposes. Context of each ESMS Risk Event is presented in Appendix 4.

3.3.2.4 ESMS Risk Impact Matrix

The Impact Matrix shown in Table 3-1 summarises the significant risk impact areas from the 19 ESMS risks identified.

ESMS Risk Events and Risk Descriptions	Significant Risk Impact Areas			
A service insulation, neutral conductor, meter and/or connection fails				
Third party contact or interference with elevated network assets				
Third party contact or interference (including 'dig-in') with underground assets, pillars, pits and cabinets				
Connection/restoration/removal of supply to an installation is not performed correctly				
Interference with network assets [other than overhead lines] (unauthorised/forced access, other utilities/3rd parties working near or on network assets)				
Conductive pole or network structure becomes energised.				
Employee inadvertently makes contact with live equipment.				
Damage to network assets associated with natural disaster or major event				
Failure of overhead network assets e.g. surge arrester, fuse, pole, conductor, joints, cross-arm and insulator, etc.				
Overload of network assets				

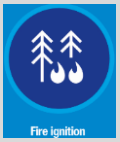
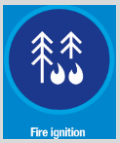
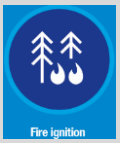
ESMS Risk Events and Risk Descriptions	Significant Risk Impact Areas			
Poles and assets (transformers on poles, stays and pillars at ground level, etc.) struck by vehicles				
Failure of underground network assets				
Cables, trenches, enclosures and/or pit lids in unsafe condition				
Failure of equipment in zone substations				
Failure of electrical protection				
Contact made or interference with earthing systems including SWER				
Distribution substation equipment failure.				
Network impacted by adjacent infrastructure failure or works, including customer installations, e.g. solar systems				
Fire starts involving overhead network assets				

Table 3-1 – ESMS Risk Impact Matrix

Risks that are not directly related to electricity networks (HSE and Finance) are addressed in other risk assessment procedures (e.g. HSE Change Management Procedure, use of "Manual Handling Detailed Assessment" Form, etc.) across the business and are captured within the corporate Risk Register.

Section 3.3.4 describes how these risks are analysed and evaluated, with control and risk prioritisation detailed in Section 3.3.5.

3.3.3 Risk Analysis

The Corporate Risk group is responsible for the management, coordination and facilitation of network asset risk within the business.

As part of this ESMS risk assessment process, relevant SMEs were consulted to ensure that:

- Key messages are delivered appropriately to relevant stakeholders.
- Relevant stakeholders (i.e. risk/control Owners) are engaged (during FSA workshops and/or follow-up emails with summary of outcomes from FSA workshops) to ensure an effective exchange of information.
- Feedback and reporting is undertaken as part of an on-going communication and consultation process.

3.3.3.1 ESMS Risks - Formal Safety Assessment

The ESMS Formal Safety Assessment (FSA) process (as shown in Appendix 13) identifies risks in accordance with the *Electricity Safety (Management) Regulations 2009* and the Australian Standard AS5577 *Electricity Network Safety Management System 2013*. The FSA involves assessment of the electricity network risks with specific focus on the safety of employees, contractors and the public. A semi-quantitative methodology is used to rank and analyse the risks as part of the FSA. The risk identification methodology used is in accordance with ERM.

To ensure that all risks associated with network assets are analysed comprehensively and effectively, hazards (causes) and potential risk events/scenarios are mapped with consequences grouped as follows:

- Asset Performance (i.e. failure of network assets)
- Human Factors (i.e. interference with network assets)
- Incident Based - operation or construction related
- Outcome Based - bushfire

For details, refer to Appendix 6 - ESMS Causes - Risk Events / Scenarios – Consequences Mapping

After the components of electricity network risk (as described in Section 3.3.2 above) were identified, ESMS risk events and scenarios were established by mapping the possible causes and consequences based on four hazard event or scenario groups. Network Safety Work Groups carried out the initial analysis and mapping works.

For examples of Bow-Tie diagrams refer Appendix 3.

Each of the identified ESMS risk events/scenarios were further assessed with preliminary likelihood and consequence ratings assigned for further reviews during subsequent FSA workshops with relevant stakeholders and SMEs involved.

The ESMS risk register has been continually updated over the past ten years from the results of risk assessment workshops attended by a wide range of internal and external stakeholders,

including senior managers, SMEs and field representatives. The 19 ESMS risks are described in Table 3-1.

3.3.3.2 FSA Workshops

FSA workshops are prepared by seeking relevant information (such as policies, procedures, incident data) from subject matter persons ahead of conducting a formal safety assessment. Preliminary risk events, causes and consequences are identified along with corresponding preventative and corrective controls[26].

The process of selecting controls for ESMS risks is in accordance with the process for identifying risk treatment options as outlined in ISO 31000. Below is a summary of the process used for each ESMS risk scenario.

- Identify all possible Causes (based on Root Cause analysis principles) that could trigger / lead to the risk scenario (event).
- Identify all possible Consequences (based on the four Risk Impact Areas, i.e. Health & Safety, Fire, Property Damage and Supply Interruption) if such risk scenario (event) occurred.
- For each of the identified causes, identify possible controls, i.e. business strategies / policies, management processes and/or programs (initially from the corporate control register) that could eliminate / change the likelihood from that cause leading to occurrence of the associated risk scenario (event).

  Note: Additional controls identified during FSA workshops would be included as required.

- Similarly, for each of the identified consequences (risk impact areas), identify possible business strategies / policies, management processes and/or programs that could eliminate / change the consequences if such risk scenario (event) occurred.

  Note: Additional controls identified during FSA workshops would be included as required.

- Tabulate all identified controls in a spreadsheet format and/or present the identified controls in a BowTie diagram.

Below is an example on how ESMS risk mitigation controls were selected:

- ESMS Risk Scenario ID 32 – Failure of Distribution Substation Equipment

Possible Causes identified:

- Design Deficiency

[26] FSA workshop preparation and facilitation guidelines (*draft document*). Refer Appendix 16.

- Equipment Not Fit for Purposes
- Poor Workmanship or Work Practices
- Operational / Human Error
- Asset Defect, Corrosion or Deterioration
- End of Asset Service Life
- Unauthorised Access / Vandalism / Sabotage / Copper Theft
- 3rd Party working in proximity
- 3rd Party Equipment contacting Substation Assets
- Water Ingress / Flooding
- External Fire

Possible Consequences identified:

- Electric Shocks
- Personal Injury / Death (Public / 3rd Party)
- Personal Injury / Death (Employee / Direct Contractor)
- Fire
- 3rd Party Property Damage
- Network Asset Damage
- Supply Interruption

Preventative controls identified (as example) for Cause “Poor Workmanship or Work Practices”:

- Competency Management
- Health & Safety Auditing and Safety Review Processes
- Construction Policies and Procedures (Asset Services)
- Construction Policies and Procedures (Major Projects)
- Construction Compliance Audits
- Asset Failure Investigation Process
- SAP Registers and Tracks Asset Maintenance
- Asset Management Policies, Strategies, Standards and Plans (O/H)
- Asset Management Policies, Strategies, Standards and Plans (U/G+Sub)
- Asset Inspection Policies and Program (O/H)
- Asset Inspection Policies and Program (U/G+Sub)

Corrective controls identified (as example) for Consequence “Fire”:

- Operational Processes and Procedures
- Fault Response
- Operational Contingency Plans
- Crisis & Emergency Management System
- Emergency Services and/or Fire Agent Liaison

Once the controls are identified, the stakeholders relevant to the topic and responsible for those controls are included in the workshop attendance list. Controls are verified through the formal risk assessment workshop.

Workshops are scheduled with stakeholders and their representatives whereby a formal safety assessment is undertaken.

Risk Assessments made during the FSA workshops are based on:

- Incident statistic data and trends (only last five-years data was used in order to avoid possible errors in data entry during the early stage of Network Incident Database)
- Personal or organisational experience
- Local (Australian) or overseas experience (if applicable, i.e. with similar network environment) and
- Expert judgement (i.e. based on SMEs' knowledge and experience)

A risk rating for each ESMS risk event/scenario is determined, based on the highest risk score derived from the following criteria:

- The most likely or most realistic impact (consequence) to CP-PAL
- The possible worst case consequence due to a single fatality or serious injury from network assets that may occur to either the public or employee
- The potential worst case (most severe) consequence due to multiple fatalities relating to bushfire or vehicle incidents that may occur (based on industry, Australian and overseas experience)

From ESMS risk assessment results, risk ratings based on 'potential worst case' consequences are always below the risk ratings of 'most realistic' or 'possible worst case' consequences.

After risk ratings of all ESMS risk events/scenarios are determined, risk mitigation controls for each are reviewed, with reliance and confidence ratings assessed during FSA workshops. Possible control improvement ideas were also discussed and recorded for subsequent reviews, so too the results from investigations completed by relevant ESMS Control/Risk owners.

The ESMS Risk Register is updated with the relevant outcomes at the conclusion of each FSA workshop.

A summary of the outcomes are then forwarded after the FSA workshops to relevant Risk Owners and management for final review and/or recommendation of required action items.

3.3.3.3 Assignment of Risk Owners and Control Owners

To ensure effective administration of ERM, responsibilities are assigned to employees to manage the risks associated with their roles and positions. For Risk Management purposes, a Risk Owner is assigned to each of the identified ESMS risk scenarios and events, and an ESMS Control Owner assigned to each of the identified risk mitigation controls.

ESMS Risk Owners are generally senior managers (refer Section 4.2.4.1 for details), reporting directly to the General Manager – Electricity Networks. The responsibilities of a Risk Owner (for the assigned ESMS risks) includes:

- Determination of appropriate risk responses and management capabilities.
- Ongoing management and monitoring of risks for changes in their severity or likelihood through:
  - Communication with Control Owners to put in place sufficient control activities appropriate to the nature of the risk
  - Collating and analysing relevant data indicating risk likelihood and impact
  - Ensuring effective implementation of risk treatment plans (if any).

ESMS Control Owners are employees accountable for the management of controls to which they are allocated. Their responsibilities include:

- Ensuring effective and efficient control design, managing the impact and likelihood of the risk (in conjunction with the risk owner)
- Effective performance and delivery of control activities
- Provision of information and reporting related to control performance
- Sourcing and analysis of relevant data pertaining to control performance
- Reporting information on a regular and timely manner to the Risk Owner and other relevant stakeholders
- Creating and implementing corrective action driven by the risk information
- Immediate reporting to the Risk Owner and other relevant stakeholders of any control weaknesses and/or breakdowns
- Assurance of outcomes relating to control treatment plans

When control improvement actions are considered necessary (based on outcomes from FSA workshops), the relevant ESMS Control Owners are responsible for determining resource requirements (e.g. financial, labour, material and equipment) and establishing work schedules for the associated implementation activities. Control Owners are also required to monitor and to report work progress to relevant ESMS Risk Owners and Network Safety personnel and to update the ESMS Risk register for future reviews.

3.3.4 Risk Evaluation

3.3.4.1 Methodology Overview

CP-PAL operates an ERM Framework as described in Section 3.2. This provides a consistent framework across the business for the identification, assessment and control of risks[27].

[27] Enterprise Risk Management Framework – JEQA4UJ443MT-154-354

This element is structured to provide an overview of such methodology (and some worked examples) as follows:

- Data sources
- Cause or 'Bow-tie' analysis
- Consequence, likelihood and risk rating
- Controls and residual risks and
- Outcome of ESMS risk assessment process

3.3.4.2 Data Sources

i. Historical Incident Data

Consideration of historical incident data provides insight into the cause, consequence, and likelihood of risks identified. It can also inform decisions on how to implement control measures to mitigate the risk consequence and avoid recurrence.

Historical data are collected from several sources for use within the risk assessments and reviews, including CP-PAL databases and broader industry sources. These databases include:

- Historical ESMS Risk Register
- Corporate Risk Register
- Incidents database (Cintellate)

An example of the type of data tracked and analysed was the number of fire starts by cause, as shown in Figure 3-6. These fire starts are categorised as follows:

- Human or animal contact
- Vegetation contact
- Third-party contact (e.g. vehicle)
- Lightning
- Asset failure

The majority of fire starts are caused by asset failure. Overall, a downward trend of total fire starts has been observed over recent years, primarily due to a reduction in asset failures.

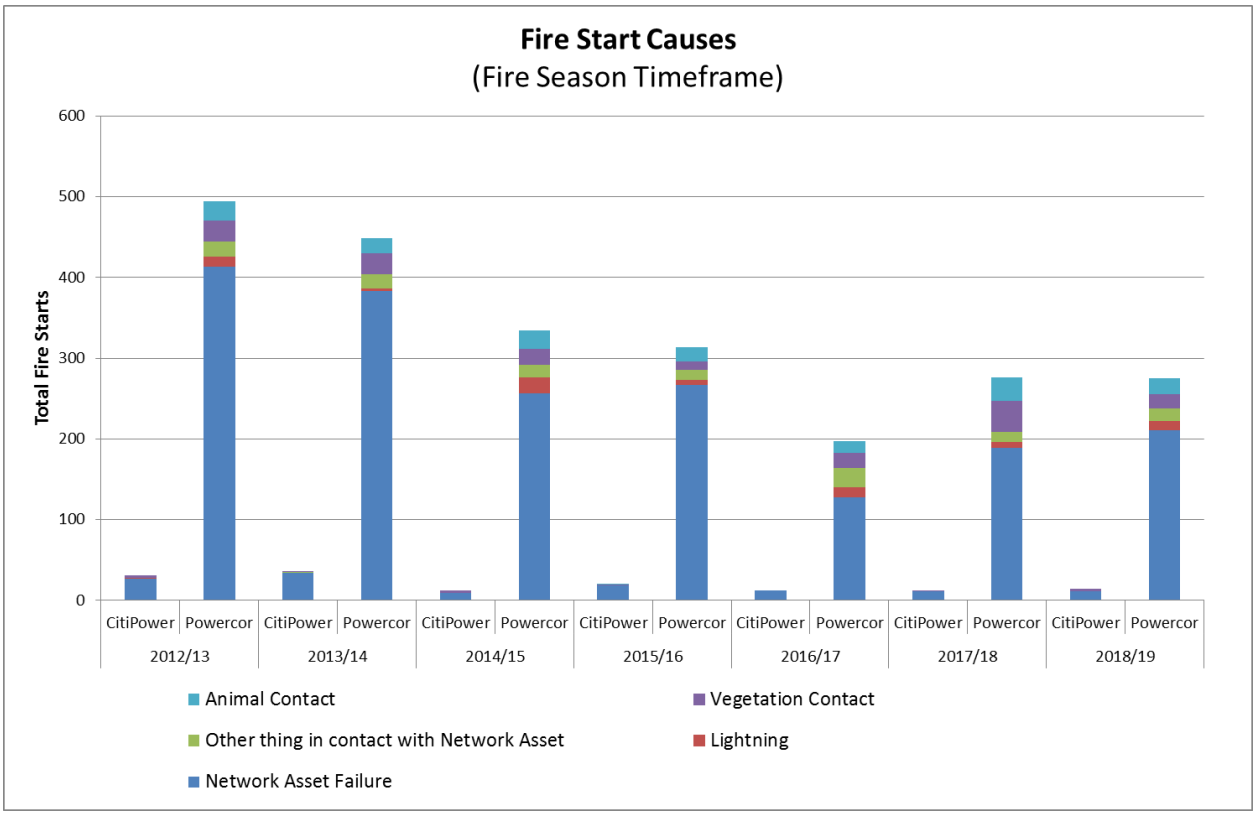


Figure 3-6 – Causes of fire starts between FY 2013 and 2019

In some cases, there is no historical or statistical data on a known risk event and SMEs are consulted instead for the required risk analysis.

ii. Fire Loss Consequence Maps

Each year the state government produces Fire Loss Consequence (FLC) maps for Victoria, as shown in Figure 3-7. The coloured sections indicate the worst case house losses likely within that area. The consequence loss is shown in two km squares, with a corresponding likely house losses ranging from 0-50 (yellow) to above 7000 (purple). Figure 3-7 is modelled with the Code Red conditions applicable to Black Saturday, which is a temperature of 46°C or above, with winds in excess of 100 km per hour.

Each year, the fire loss consequence map is incorporated within the CP-PAL asset map. These fire consequence maps help to understand the range of fire risk profiles across the network and to prioritise works and maintenance activities as to minimise bushfire risk.

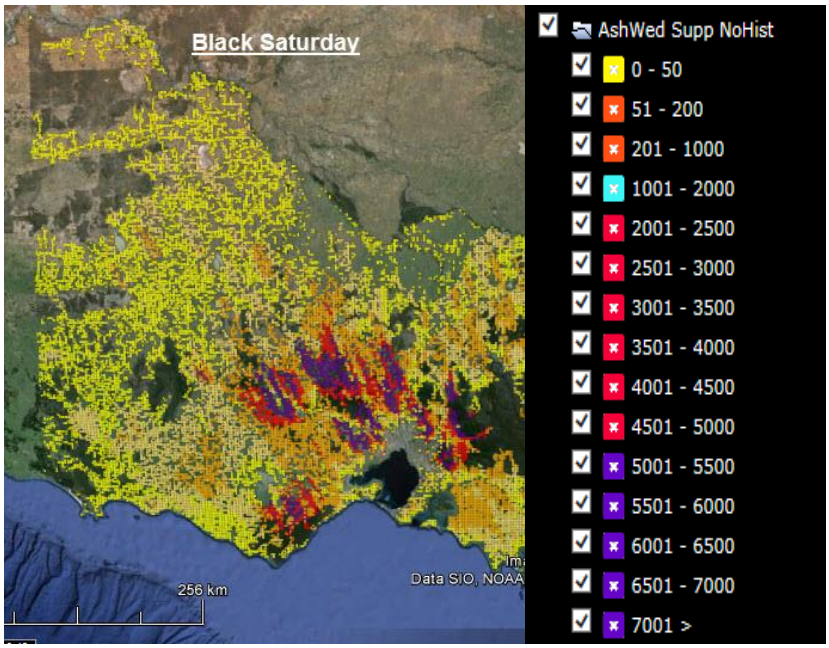


Figure 3-7 – Fire loss consequence map with Black Saturday conditions (left) and fire loss index (right)

3.3.4.3 Cause and 'Bow-tie' Analysis

The range of data described above was then fed into the systematic analysis. The 'Bow-tie' risk analysis method enables multiple causes to be reviewed, including a review of the controls to prevent each from occurring and also those required to correct the event should it occur.

A single risk event, such as a fire start, can have a range of causes. The 'Bow-tie' example shown in Figure 3-8 demonstrates a range of possible causes on the left, including asset failure, vegetation, weather, and third-party contact events. Each possible cause leads to the potential fire start risk event in the centre of the 'Bow-tie'.

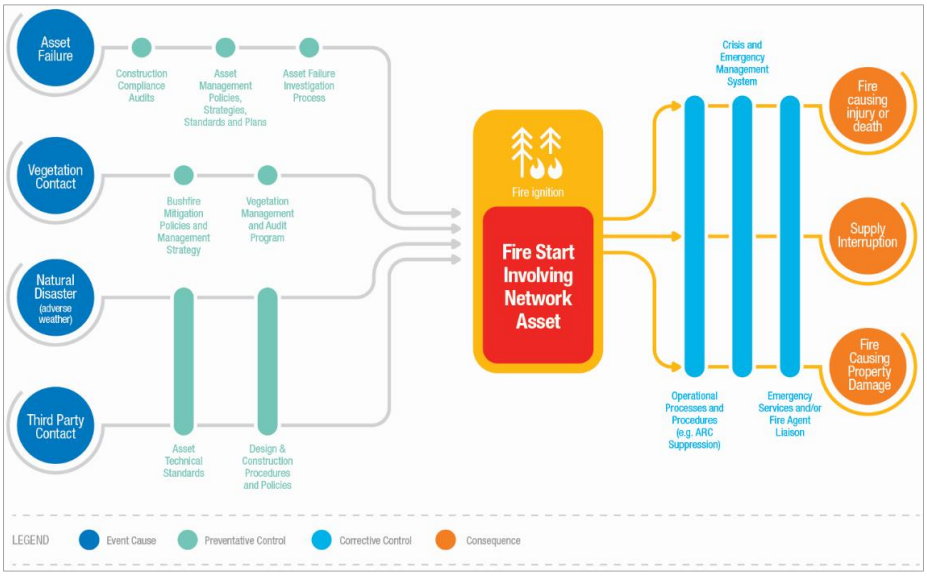


Figure 3-8 – 'Bow-tie' example for fire start risk event

Once these causes are established, further analysis is then conducted on consequence, likelihood and the controls for each, as described in the following sections. This assessment draws on the expertise of SMEs and draws upon industry experience. These risk events are then tested (during FSA workshop with SMEs involved) and challenged to further enhance their validity and accuracy.

Further 'Bow-tie' examples are provided in Appendix 3.

In late 2016, bow-tie analyses were undertaken on the following major company risks:

- Catastrophic bushfire
- Vegetation contact
- Hazard tree contact
- Third party interaction
- Failure of network or sub-optimal performance

3.3.4.4 Consequence, Likelihood and Risk Ratings

i. Consequence Rating

To ensure that the specific nature of the risk is considered appropriately, the possible risk outcomes are broken into the following eight consequence categories:

- Financial
- Health and Safety
- Customer Service
- Reputation
- Reliability
- Environment
- Compliance and
- Employee Satisfaction

Each consequence (by category) was assigned with a rating, as shown in Table 3-2. An overall consequence rating is taken based on the highest consequence category rating:

Further information, including an example calculation of an overall consequence, is shown in Appendix 8.

The consequence ratings are based on the current controls that are in place at the time of assessment and the overall consequence score is used to determine the risk rating of the risk event.

Rating, Consequence & Numeric / Category Values	Minimal	Minor	Moderate	Major	Catastrophic
Financial (ESMS) **Cash Loss (Net Present Value)** **Earnings i.e. Net Profit Before Tax**	Less than A$100k	A$100k or more, but less than A$1m	A$1m or more, but less than A$10m	A$10m or more, but less than A$75m	A$75m or more, recapitalisation by shareholders
Health & Safety **Employees** **Public** **Contractors**	Slight injury, does not affect work performance or daily life activities	Minor injury that affects work performance in the short term (e.g. restricted work activities or affecting daily life activities for up to five days).	Major injury that affects work performance in the longer term (e.g. absence from work or restricted work activities for more than five days; daily life activities affected for more than 5 days).	Single fatality Permanent disability	Multiple fatalities Multiple permanent disabilities

Rating, Consequence & Numeric / Category Values	Minimal	Minor	Moderate	Major	Catastrophic
Customer Service/ Reputation/Reliability Media Coverage Customer Satisfaction Stakeholder Satisfaction e.g. Suppliers Regulators Government Shareholders Supply Reliability and Quality	Negative local media coverage. Possible local community concern. Localised customer complaints. Informal follow-up by stakeholders due to actions by the Company. Insignificant decrease in quality of supply or increase in the quantity and/or duration of interruptions to customers' electricity supply and/or number of customers' off-supply. Rectified within six hours.	Negative regional media coverage. Local community concern. Sustained or ongoing localised customer complaints. Concern expressed by stakeholders due to actions by the Company. Sustained decrease in quality of supply or increase in the quantity and/or duration of interruptions to customers' electricity supply and/or number of customers' off-supply. Rectified within 12 hours.	Negative state and/or national media coverage. Widespread customer complaints or complaints to the Regulator or Ombudsman Stakeholders impose operating conditions and/or threaten to withdraw funds, services or contracts as a result of actions by the Company. Significant decrease in quality of supply or increase in the quantity and/or duration of interruptions to customers' electricity supply and/or number of customers' off supply. Rectified within 24 hours. Results in internal event escalation	Adverse media campaigns by customers, media, and industry groups causing short term loss of customer and/or public support. Formal intervention by the Regulator or Ombudsman and/or litigation. Stakeholders impose operational control and/or withdraw or cancel funds, services or contracts. Significant decrease in quality of supply or increase in the quantity and/or duration of interruptions to customers' electricity supply and/or number of customers' off-supply. Rectified in excess of 24 hours. Results in industry event escalation.	Prolonged media criticism and long term loss of customer and/or public support. Repeated formal intervention by the Regulator or Ombudsman and/or litigation including class action. Business unable to continue operations and/or attract future Business opportunities. Major blackout (e.g. Melbourne CBD or major provincial city) without supply for longer than 24 hours. Results in industry event escalation.

Rating, Consequence & Numeric / Category Values	Minimal	Minor	Moderate	Major	Catastrophic
Environment Land Vegetation Groundwater Waterways Ecosystems Atmosphere *Immediately recoverable: clean up can be completed at site extent well defined and; no further site investigation required.	Insignificant damage that has no detectable impact on the environment. By way of additional guidance such a spill is likely to be immediately recoverable*.	Minor damage that has a detectable temporary impact on the environment where without any remedial action, area would be expected to self recover within 12 months. By way of additional guidance such a spill is likely to be immediately recoverable*.	Medium damage resulting in loss to the environment where without any remedial action, area would be expected to self recover within 1 to 5 years. By way of additional guidance such a spill is not likely to be immediately recoverable*.	Serious damage resulting in loss to the environment where without any remedial action, area would be expected to self recover within 5 to 10 years. By way of additional guidance such a spill is not likely to be immediately recoverable* and/or the spill causes pollution to a waterway or groundwater.	Very serious damage resulting in loss to the environment where without any remedial action, area would be expected to self recover in excess of 10 years. By way of additional guidance such a spill is not likely to be immediately recoverable* and/or the spill causes extensive pollution to waterway or groundwater.
Compliance Legislation Regulation Industry codes Licences	Non-compliance resulting in immediate rectification without involvement from external bodies.	Non-compliance resulting in external request for immediate rectification and/or minor Company or Officer fines.	Non-compliance resulting in external request for immediate rectification and severe Company or Officer fines.	Regulator threatens loss of distribution licence and/or Company Director(s) stood down.	Prison sentences for Directors or Officers and/or Loss of Distribution Licence.
Employee Satisfaction Engagement Motivation Morale	Minimal impact on employee satisfaction. Can be resolved independently of management.	One or more employees express a level of workplace dissatisfaction that can be resolved with informal management input.	Formal complaint made by one or more employees requiring formal management action to be taken	Breakdown in workplace relations between employee(s) and the Business resulting in an industrial action e.g. strike.	Severe breakdown in workplace relations between employee(s) and the Business resulting in litigation including class action.

Table 3-2 – Risk Category and Rating (Measures of Consequences) reference table

Likelihood Rating

Once the consequence rating for the risk has been determined, the likelihood rating of that consequence arising from the risk event is identified. Probabilities are provided as a guide to assist in the assessment of likelihood. The data and performance information of network assets and incident data are used to determine the likelihood of each type of risk event and consequence.

The likelihood is chosen based on the current controls in place, i.e. residual risk, as per Table 3-3.

Likelihood Descriptor	Indicative Frequency
Almost Certain	One or more event per year
Likely	At least one event every 2 years
Possible	One event per 2 – 5 years
Unlikely	One event per 5 – 20 years
Rare	One event every 20 – 40 years

Table 3-3 – Likelihood Reference Table

Risk Rating Determination

Under the Corporate Risk Management Framework[29], the level of risk (Risk Rating) is defined as a function of consequence and likelihood.

For a qualitative assessment, the Risk Profiling Matrix shown in Table 3-4 is used to determine the level of risk of a risk event, by the intersection of the corresponding consequence and likelihood ratings in the table. For example, a risk event of 'Major' consequence and 'Possible' likelihood is given and a risk rating of 'High'.

[29] Enterprise Risk Management Framework - JEQA4UJ443MT-154-357

Likelihood	Consequence				
	Minimal	Minor	Moderate	Major	Catastrophic
Almost Certain	Medium	High	High	Extreme	Extreme
Likely	Low	Medium	High	High	Extreme
Possible	Low	Low	Medium	High	High
Unlikely	Negligible	Low	Low	Medium	High
Rare	Negligible	Negligible	Low	Medium	High

Table 3-4 – Risk Profiling Matrix

For example, a risk event with highest consequence rating of Major and a likelihood of Possible), the established risk rating is “High”.

Risk ratings of the identified risk events are subject to an annual review process to maintain their relevance. This is completed by the EMT, assisted by BU Risk Co-ordinators and all relevant stakeholders. The process involves obtaining feedback from stakeholders on the likelihood/consequence categories, descriptions and ease of application.

The risk rating is used for developing effective controls, the extent of monitoring and the level of management review and reporting required.

Refer Appendix 7 for Determining the Likelihood Rating of a risk.

ii. Risk Controls and Residual Risk

As illustrated in the Figure 3-8, CP-PAL’s risk analysis process involves an assessment of the controls that are put in place to reduce the likelihood or consequence of a risk event.

A control includes the structure, system, process, procedure, policy or any other action designed to modify the risk. Controls focused on prevention of the risk event occurring or on correcting the consequence should the event actually occur. The majority of focus is placed upon preventative controls to reduce the risk of an event occurring.

The risk ratings are used for developing risk treatments that are further subjected to AFAP assessment.

3.3.4.5 Limitations, Validity and Accuracy Assessment

As the risk assessment process predicts possible future scenarios, it has inherent limitations. The process of risk identification and management is complex but essential in countering limitations and providing stakeholders with confidence that the risks identified are valid and accurate.

To ensure a comprehensive risk analysis is carried out (by consulting relevant stakeholders and SMEs, prior to and during FSA workshops), the ESMS risk scenarios are based on the three hazard groups: contacts/interference, asset failure and assets in unsafe situations, and the four risk impact areas: fire ignition, electric shock/injury, property damage and interruption of supply.

To minimise personal preferences and subjective decisions, the electrical network safety risks that the ESMS considers are assessed with consideration of:

- Incident statistic data and trends
- Corporate Risk Registers
- Personnel and organisational experience
- Asset performance data
- Operational HSE risks and trends
- Local (Australian) or overseas experience
- Expert judgement/experience

The diverse range of staff (e.g. managers, workgroup leaders, field personnel, SMEs, etc.) involvement and the risk review cycle help to increase validity and accuracy.

3.3.4.6 Outcomes of ESMS FSA

Based on of ESMS FSA process, the assessed residual risk ratings of the identified ESMS risks (with controls in place) are shown in Table 3-5.

There is one risk rated as Extreme, 16 High (including two with potential for multiple fatalities), and two Medium. The Extreme and the two rated as High with potential for multiple fatalities are described in further detail as follows:

Extreme:

- Vehicle strikes to assets are unfortunately almost certain to occur in future and can result in single or multiple fatalities. Whilst the circumstances associated with this risk, including speed, drink driving and inclement weather are beyond the control of a Distribution Business (DB), this risk remains at an Extreme residual rating.

High:

- Fire starts involving overhead network assets have the potential to cause major bushfire events, resulting in multiple fatalities. However as this event is unlikely, it is rated at a High residual rating.
- Third-party contact events with either overhead or underground assets have the potential for multiple fatalities, however is again unlikely, and so it is also rated High.

ESMS risks inform the relevant corporate strategic risks. The relationship of ESMS risks to the relevant corporate risks are listed in Table 3-5.

Risk ID	Description	Overall Consequence Rating	Likelihood	Residual Risk Category
CORP ID 222	**Catastrophic bushfire**	**Catastrophic (Potential for Multiple Fatalities)**	**Unlikely**	**High**
ESMS ID 34	Fire Starts from O/H Network Assets			
CORP ID 95	**Third party property damage or personal death or injury from our network or activities**	**Moderate (Potential for Multiple Fatalities)**	**Likely**	**High**
ESMS ID 19	Poles and assets (transformers on poles, stays and pillars at ground level, etc.) struck by vehicles			
ESMS ID 03	Third party contact or interference with elevated network assets			
ESMS ID 05	Third party contact or interference (including 'dig-in') with Underground assets, pillars, pits and cabinets.			
ESMS ID 10	Interference with Network assets [other than overhead lines]. -- (Unauthorised / forced access, other utilities / 3rd parties working near or on network assets)			
ESMS ID 31	Contact made or interference with earthing systems including SWER.			
ESMS ID 26	Cables, trenches, enclosures and/or pit lids in unsafe condition.			
ESMS ID 08	Connection/restoration/removal of supply to an installation is not performed correctly.			
ESMS ID 01	A service insulation, neutral conductor, meter and/or connection fails			
ESMS ID 11	Conductive pole or network structure becomes energised.			
CORP ID 284	**A significant health, safety or environmental incident that affects one or more employees, contractors or visitors, or impacts the environment during or following work undertaken for the Business' at properties, on assets or worksites.**	**Moderate**	**Possible**	**High**
ESMS ID 13	Employee inadvertently makes contact with live equipment.			

Risk ID	Description	Overall Consequence Rating	Likelihood	Residual Risk Category
CORP ID 93	**Failure of network or sub-optimal performance**	**Moderate**	**Possible**	**Medium**
ESMS ID 15	Failure of overhead network assets, for e.g. surge arrester, fuse, ACR, pole, conductor, joints, cross-arm and insulator, etc.			
ESMS ID 30	Failure of electrical protection and/or control system			
ESMS ID 27	Failure of equipment in zone substations			
ESMS ID 25	Failure of underground network assets.			
ESMS ID 32	Distribution substation equipment failure.			
CORP ID 110	**Failure or inadequate capacity of transmission connection terminal station assets**	**Minor**	**Likely**	**Medium**
ESMS ID 16	Overload of network assets.			
CORP ID 101	**Damage to our network from natural disasters (bushfires, flood, storm, lightning, earthquake, etc.) or theft, sabotage or vandalism**	**Minor**	**Likely**	**Medium**
ESMS ID 14	Damage to network assets associated with natural disaster or major event			
ESMS ID 33	Network impacted by adjacent infrastructure failure or works, including customer installations, e.g. solar systems.			

Table 3-5 – CP-PAL's Relationship of ESMS Risks to Corporate Risks

These 19 ESMS risks have a range of preventative and corrective controls in place, which are subject to continual review to assess the effectiveness of each control item. This process is described further in Section 3.3.5.

3.3.5 Risk Treatment

As described in Section 3.2, CP-PAL operates an ERM Framework, which provides consistency across the business for the identification, assessment and control of risks[30].

This section provides an overview of the risk control and treatment methodology, detailing the:

- Risk acceptability

[30] Enterprise Risk Management Strategy – 13-10-CP0007

- Control effectiveness
- Control reliance
- Control improvement planning
- Monitoring and review
- Summary of risks and controls

3.3.5.1 Residual Risk Acceptability

The first step in assessing potential control measures was to consider the risk acceptability and determine which risks require further risk treatments.

Table 3-6 provides guidance to management on acceptable risk levels. Extreme risks are considered to be in an unacceptable region and require risk controls and treatments to reduce the residual risk to an acceptable level. The risk can only be allowed to continue 'as-is' under extraordinary circumstances and with approval from the Risk Management and Compliance Committee (RMCC), which includes Board representation. There is one residual risk with a rating of Extreme, being assets struck by vehicles. This is due to the associated fatalities that occur each year due to vehicles colliding with power poles, which is acknowledged as an uncontrollable risk. Given CP-PAL assets are involved, the business is working with VicRoads to implement 'Raptors,' which are impact absorbing devices that can be placed around poles that have been deemed hazardous from road management reviews.

On the contrary, medium or low risks are generally considered acceptable. Reasonable steps are still to be taken however to ensure that appropriate resources are provided for implementation of control improvement, to eliminate or minimise risks based on AFAP principles.

For ESMS, the risk rating helps to prioritise risks that require immediate controls and treatments. It is not be used by itself to determine whether further actions are required or not, however it assists in identifying the highest priority for action.

Residual Risk Rating	Risk Acceptability
Extreme (Risk could cause or is causing major adverse effects on the achievement of Business objectives)	Unacceptable Region – Risk can only be allowed to continue under extraordinary circumstances and with approval from the Risk Management and Compliance Committee (RMCC).
High (Risk could have or is having a significant adverse effect on the achievement of Business objectives)	Tolerable Region – Increase risk mitigation efforts to reduce risk as reasonably practicable unless cost significantly outweighs the benefit or reduction is impracticable.
Medium (Risk could have or is having an adverse effect on the achievement of Business objectives)	Tolerable Region – Increase risk mitigation efforts to reduce risk as reasonably practicable unless cost would exceed the benefit gained.
Low (Risk has minimal impact on the achievement of Business objectives)	Broadly Acceptable Region – No further risk reduction measures are usually required unless the benefits are substantial.

Residual Risk Rating	Risk Acceptability
Negligible (Risk does not pose a threat to the achievement of Business objectives)	Acceptable Region – Potential over control. Consider reducing risk control measures.

Table 3-6 – CP-PAL Risk Acceptability reference table

Example: The risk of bushfire from a fire start caused by CP-PAL assets is rated as a High residual risk rating. The catastrophic potential consequence of this risk means it will always be rated as High residual risk. As the actual consequences of most incidents associated with fire starts are rated as moderate with the consideration of the numerous controls that are in place, the risk is deemed Acceptable in accordance with the Risk Acceptability criteria in Table 3-6.

3.3.5.2 Risk Assurance Methodology

Assurance is a measure of the effectiveness of risk and control activities, maintaining their performance as intended.

The risk assurance process is summarised in Figure 3-9 below:

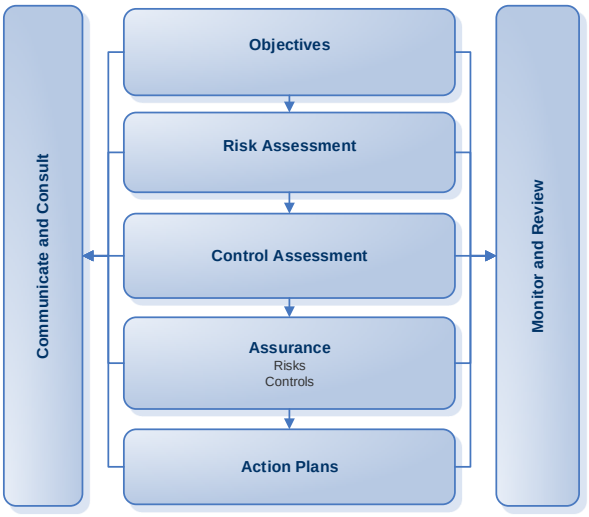


Figure 3-9 – CP-PAL's Risk Assurance Process

The objectives of the risk assurance process were to allow the Business to answer the following questions:

- What confidence does the Business have that the risks and controls are being managed?
- Where is the confidence coming from and based on what evidence?
- Are controls designed adequately and are they complied with?

Outcomes from the risk assurance activities were to be fed back for further control improvements and/or future risk reviews and assessments.

Control Assessment is a process (as described below) whereby internal control effectiveness is examined and assessed. The objective is to provide reasonable assurance that all business objectives will be met. It is a component of risk analysis in the risk assessment process.

3.3.5.3 Risk Control Confidence

Following the risk acceptability assessment, the effectiveness of each control was assessed, including existing and potential controls. This involved assessing whether the controls were appropriately planned, designed and are operating as intended to address the relevant business risks. The assessment provides a level of confidence that the controls were effective and that business objectives will be achieved.

The criterion for assessing the relative level of effectiveness of a risk control is shown in Table 3-7 below:

Control Confidence	Description
Fully Effective	Control is appropriately planned and designed and is operating as intended to address the relevant business risks. The control environment is providing a high level of assurance that business objectives will be achieved.
Mostly Effective	Control is appropriately planned and designed, however there are still additional improvement opportunities in the control environment. The control environment is providing an acceptable level of assurance that business objectives will be achieved.
Partially Effective	Control is not operating as intended or has not been designed appropriately to address the relevant risks. Improvements are required in order to achieve an acceptable level of assurance that business objectives will be achieved.
Ineffective	Control is not yet in place or is fundamentally deficient in addressing the relevant risk. Control is not contributing to an assurance that business objectives will be achieved.

Table 3-7 – Control Confidence Guide

Example: The risk of bushfire from a fire start caused by our assets has numerous controls in place including our Bushfire Mitigation Strategy Plan (which includes the *Total Fire Ban (TFB) Day Action Plan*). The TFB Day Action Plan sets specific operating protocols in place during these higher fire risk days. This plan is well developed, comprehensive and has been assessed as Fully Effective against the Risk Control Effectiveness criteria in Table 3-7.

3.3.5.4 Risk Control Reliance

The level of reliance on each control is assessed to determine how critical each control is in mitigating the individual risks. Some risks have numerous controls, each contributing to risk reduction. In this case, a failure of one control may not be significant in the overall risk profile.

Other risks may rely on a single control, in which case the risk is exposed to a single point of failure if that control does not operate as intended. In this case, it is more important that the control is highly effective and if it is not, further improvements may be required (subject to ESMS AFAP Assessment as described in Section 3.3.5.7).

The assessment provides guidance on the level of importance of each control. The more reliant a risk is on one control, the more important it is to ensure that control is effective.

The relative level of reliance of a control is assessed using the criteria in Table 3-8.

Control Reliance	Description
Critical	Relative to other identified controls, the control: ▰ Considered to be of the utmost of importance (without this control in place the risk would be considered to be uncontrolled). ▰ Dramatically reduces the likelihood and/or consequence of a risk. ▰ Reliance Factor weighting is 1.0.
Significant	Relative to other identified controls, the control: ▰ Has a substantial impact in managing a risk. ▰ Greatly reduces the likelihood and/or consequence of a risk. ▰ Reliance Factor weighting is 0.75.
Important	Relative to other identified controls, the control: ▰ Has a recognised impact in managing a risk. ▰ Reduces the likelihood and/or consequence of a risk. ▰ Reliance Factor weighting is 0.50.
Routine	Relative to other identified controls, the control: ▰ Has a minor impact in managing a risk. ▰ Only marginally reduces the likelihood and/or consequence of a risk. ▰ Reliance Factor weighting is 0.25.
Trivial	Relative to other identified controls, the control: ▰ has minimal impact in managing the risk; ▰ has no recognised reduction in the likelihood and/or consequence of a risk; and ▰ Reliance Factor weighting is 0.05.

Table 3-8 – Control Reliance Guide

Example: The risk of bushfire from a fire start caused by CP-PAL assets has numerous controls, some more critical than others (by comparing individual control criticalities using methodology as detailed in Appendix 14). Vegetation is a significant potential cause of fire starts and as such, the Vegetation Management Program and Electric Line Clearance Management Plan are critically important in mitigating the related risks. Vegetation control is consequently assessed as a Critical control in accordance with the Risk Control Reliance criteria in Table 3-8. This rating results in a high focus from the business on ensuring it continues to be resourced and managed effectively.

3.3.5.5 Assurance of Risk Controls

Assurance activities include, but are not limited to the following:

- Adequacy assessment of the critical controls, which are used in managing the risks. The assessment focuses on validating the rated / desired confidence levels of the critical controls.
- Identification and ongoing communication with relevant Risk/Control Owners.
- Regular review and assessment of the effectiveness of relevant controls.
- Identification of recommendations or required actions to address potential gaps in controls.
- Reporting to relevant stakeholders as required.
- Monitoring action plans.

3.3.5.6 Risk Control Improvement Assessment

Once all controls have been rated with confidence and reliance ratings, assessment for control improvement is to be carried out. Table 3-9 is an extract from a CP-PAL guideline, (refer Appendix 9) outlining the level of improvement requirement for each combination of confidence and reliance assessment. For example, if risk control reliance is rated Critical and the confidence of the control is considered to be Effective, then no improvement plan is required.

Control Reliance	Control Effectiveness	Control Improvement
Critical	Fully Effective	No Improvement Plan required.
	Mostly Effective	Improvement Plan to be developed and implemented as required to address control deficiencies.
	Partially Effective	Improvement Plan to be developed and implemented to address control deficiencies.
	Ineffective	Improvement Plan to be developed and implemented as a high priority matter to address control deficiencies.

Table 3-9 – Extract of Control Improvement Planning

Where Improvement Plans are required, the possible control improvements (i.e. risk treatments) for each of our ESMS risks are identified through analysis of the risks as described in the risk identification and assessment processes. The 'Bow-tie' process, described in Section 3.3.4.3, is particularly useful for identifying potential control improvement options as it highlights causes, which then enable preventative controls to be targeted on these route cause pathways. As with the risk identification and assessment process, historical records, subject matter experts and industry experiences are all used to help identify possible options for control improvements.

Identified potential control improvement options are then further evaluated (by relevant Risk/Control owners) based on the degree to which they reduce the likelihood and/or consequence of a risk. This includes an assessment again of their effectiveness and the level of reliance on each control, as described earlier. Assessment of the potential control improvement options also considers whether it is reasonably possible to carry out the control actions, including:

- What is known, or ought reasonably to be known, about the nature of any relevant hazard or risks.
- What is known, or ought reasonably to be known about ways of eliminating or reducing the risk.
- The degree of harm that might result from the hazard or the risk.
- The availability and suitability of ways to eliminate or minimise the risk.
- Whether the cost associated with available ways of eliminating or minimising the risk cost is proportionate to the risk.

After ESMS risk workshops, individual ESMS Risk Control Owners develop control improvement strategies (action plans) for each of the identified control improvement options, containing the following:

- Risk event ID, risk event description and name of risk owner to drive accountability
- Control description and name of Control Owner.
- Confidence and reliance assessment of controls, current and new (i.e. expected ratings after implementation of required actions).
- Action priority.
- Detail of the Control Improvement Analysis with conclusions for taking any further action or no further action.
- Scope of any planned actions and target completion dates.

Through the corporate risk profiling process (being part of the process within the Corporate Risk Management Framework), the CP-PAL Board is advised of the risk treatment plans for Extreme and High risks. Approval must then be sought from the Business Units for acceptance of control improvement plans associated with Extreme and High rated risks[31] (as detailed in Section 3.3.5.7 below).

Example: The risk of bushfire from a fire start caused by our assets has a number of controls rated as Critical and Significant, with several at Fully Effective and Mostly Effective levels. It has a High residual risk rating and given the range of controls, there is always potential opportunity for continued improvement. On an annual basis, the Bushfire Mitigation Team prepares a Bushfire Mitigation Improvement Plan to explore further enhancements to the set of controls, particularly focused on any controls that are below the Fully Effective rating.

[31] ESMS Risk Control Improvement Implementation Procedure

3.3.5.7 Action Plans

Identification of Control Improvement Options

The outcomes from the control improvement assessment are documented (if required, as per Table 3-13) using the Control Improvement Assessment Template, with details of applicable actions in the relevant ESMS Risk Treatment Plan.

ESMS AFAP Assessment

As previously mentioned, CP-PAL took risk mitigation actions based on AFAP principles, with consideration to risk ratings and associated control effectiveness ratings .

'Practicable' as stated in the Electricity Safety Act (1998), consideration of the:

a) Severity of the hazard or risk in question.

b) State of knowledge about the hazard or risk and any ways of removing or mitigating the hazard or risk.

c) Availability and suitability of ways to remove or mitigate the hazard or risk; and

d) Cost of removing or mitigating the hazard or risk

Disproportionality between the cost of removing or mitigating the risk and the benefits of risk reduction is considered to be the measure for 'practicality.' For example, if the cost to implement a control is not significantly higher than the benefits of risk reduction, that control would be considered as not satisfying the AFAP principles and should not be implemented in order to better utilise the limited resources within the business.

Cost and risk reduction benefits are weighted using the Financial Planning and approval process. Refer section 4.2.4.2

CP-PAL has established and published the Network Safety Strategy[32] which is further supported by the AFAP Procedure[33].

Control Improvement Action Plans

Based on Control Improvement Options analysis results, the AFAP assessment is subjected to management approval. Depending on the availability of resources, actions will then be assigned with completion dates for implementation.

The typical process for identification, prioritisation and implementation of the Risk Control Improvement actions is detailed in the ESMS FSA – Risk Owner Procedure[34].

[32] AM Strategy - Network Safety Strategy Oct 2019 - JEQA4UJ443MT-173-121

[33] AFAP Procedure -JEQA4UJ443MT-173-112

[34] ESMS Formal Safety Assessment – Risk Owner Procedure – JEQA4UJ443MT-173-78

3.3.6 Monitoring and Review

3.3.6.1 Risk Performance and Profiling

Risk performance and profiling enables assessment of the effectiveness of risk controls in place.

This review includes a range of incident trend data analyses related to specific risks. Some examples of incident trend charts are provided below.

Detailed analysis of incident trend data could be one of many other ways to identify the need for new controls and improved mitigation measures, such as introduction of intruder detection & alarm to minimise unauthorised access incidents within secured substations.

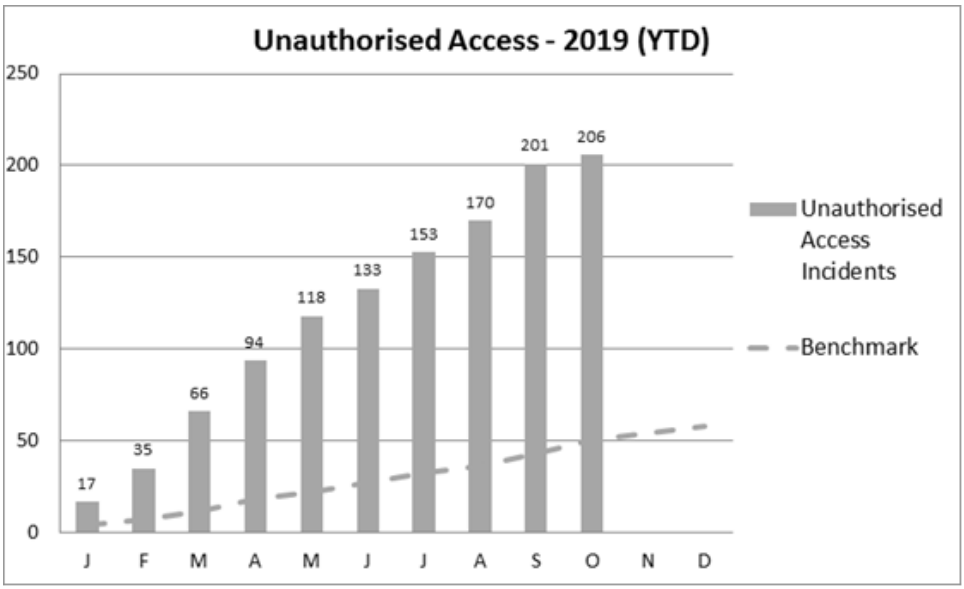


Figure 3-10 – Part Risk # 296 Incident Trend

Outcomes from the risk profiling are reported to the relevant CP-PAL Business Units. This feedback is important to ensure that the risk profile, including controls and assessments, is up-to-date and representative of the present risk environment. Upon receiving feedback, Business Units undertake a review of the associated risk controls, which may include implementation of actions.

3.3.6.2 Operating Environment Changes and Risk Review Triggers

The ESMS and associated risk processes are subject to a continuous improvement cycle, focused on managing the network safety risks to AFAP. The continuous improvement cycle enables the identification of potential deficiencies in achieving business objectives, resulting in alterations to plans, processes and procedures. Table 3-10 defines the frequency of Committee Review for continuous improvement.

Risk Review Process / Forum	Frequency
Major event of change in operating environment	As required
Bushfire pre-season and post-season review	Annual
Strategic Asset Management - Asset Maintenance Committee	Quarterly
Corporate Risk Profiling	Bi-Annual
Incident Review Committee	Monthly
Strategic Asset Management – Network Safety Committee	Bi-Annual
Asset Management Plan Review	5-yearly
Electric Line Clearance Management Plan Review	Annual
Strategic Asset Management - Bushfire Mitigation Committee	Bi-Annual

Table 3-10 – Risk Reviews and Continuous Improvement

Major events and changes in the operating environment can impact the effectiveness of relevant risk controls. Reviews can be triggered at any time and can be outside the periodic cycle described above. The types of considerations or changes that may trigger a risk review include (but are not limited to):

- Major events (internal or external)
- New product or technology introduction
- Changes in the specific environmental conditions
- Changes in regulations/legislation, such as the new Bushfire Construction Areas
- Changes in business policies, processes or procedures which impact current risk mitigation controls
- Asset failure events

3.4 Summary of Risk and Critical Controls

From the ESMS FSA, the following Critical Controls (across the 19 ESMS Risk Scenarios) are listed below indicated by the symbol  :

Critical Control	Referenced in ESMS Section
Technical Standards	3.6.2 Technical Standards Compliance Hierarchy
Secondary Design (Protection & Control) Policy	4.2.3.7 Network Planning and Development
Load Growth Forecasting (HV+Sub-	4.2.3.7 Network Planning and

Critical Control	Referenced in ESMS Section
transmission)	Development
Operational Processes and Procedures	4.3.3 Operations
Operational Contingency Plans	4.3.3 Operations
Application of Green Book	4.2.3.7 Network Planning and Development
Safe Work Practices and Procedures	4.2.2.2 Operational Delivery - Works Practices
Competency Management	4.2.2.1 Training and Competency
Asset Management Policies, Strategies, Standards and Plans	4.3.4 Asset Maintenance
Asset Failure Investigation Process	4.3.4 Asset Maintenance
Asset Inspection Policies and Program	4.3.4 Asset Maintenance
SAP Registers and Tracks Asset Maintenance	4.3.4.10 Asset Data Management
Vegetation Management and Audit Program	4.2.3.8 Vegetation Management
No Go Zone Guidelines	1.8.5 Community Awareness

Table 3-11 – Critical controls and ESMS references

The significant ESMS risks and their associated control measures are summarised in Table 3-12, along with their residual risk rating.

ESMS Risk Scenarios	Significant hazard and risk impact area				Control Measures			Residual Risk rating
					Sample of Relevant Critical Controls	Control Effectiveness	Control Reliance	
Poles and assets (transformers on poles, stays and pillars at ground level, etc.) struck by vehicles					Technical Standards	Mostly Effective	Critical	Extreme[35]
Fire Starts involving overhead network assets					Vegetation Management and Audit Program	Mostly Effective	Critical	High (Potential for Multiple Fatalities)
Third party contact or interference with OH Assets					No Go Zone Guidelines	Fully Effective	Critical	High (Potential for Multiple Fatalities)
A service insulation, neutral conductor, meter and/or connection fails					Asset Management Policies, Strategies, Standards and Plans (O/H)	Mostly Effective	Critical	High
Distribution substation equipment failure (other than electrical protection)					Asset Inspection Policies and Programs (U/G+Subs)	Mostly Effective	Critical	High
Employee inadvertently makes contact with live equipment					Safe Work Practices and Procedures	Fully Effective	Critical	High

[35] This ESMS risk has been rated as Extreme, however it is not fully controllable by CP-PAL as it is dependent on external factors (vehicle impacts to assets).

ESMS Risk Scenarios	Significant hazard and risk impact area				Control Measures			Residual Risk rating
					Sample of Relevant Critical Controls	Control Effectiveness	Control Reliance	
Interference with Network assets [other than overhead lines]. - (Unauthorised/forced access, other utilities/third parties working near or on network assets)					No Go Zone Guidelines	Fully Effective	Critical	High
Third party contact or interference (including 'dig-in') with underground assets, pillars, pits and cabinets					No Go Zone Guidelines	Fully Effective	Critical	High
Connection/restoration/removal of supply to an installation is not performed correctly					Operational Processes and Procedures	Mostly Effective	Critical	High
Conductive pole or network structure becomes energised					Asset Inspection Policies and Programs (O/H)	Mostly Effective	Critical	High
Damage to network assets associated with natural disaster or major event					Operational Contingency Plans	Mostly Effective	Critical	High
Failure of overhead network assets, e.g. Surge Arrester, Fuse, pole, Conductor, Joints, Cross-arm and Insulator, etc.					Secondary Design (Protection & Control) Policy	Mostly Effective	Critical	High
Overload of network assets					Load Growth Forecasting (HV and Sub-transmission)	Mostly Effective	Critical	High

ESMS Risk Scenarios	Significant hazard and risk impact area				Control Measures			Residual Risk rating
					Sample of Relevant Critical Controls	Control Effectiveness	Control Reliance	
Cables, trenches, enclosures and/or pit lids in unsafe condition					Asset Inspection Policies and Programs (U/G+Subs)	Mostly Effective	Critical	High
Contact made or interference with earthing systems including SWER					No Go Zone Guidelines	Fully Effective	Critical	High
Failure of electrical control and protection systems					Secondary Design (Protection & Control) Policy	Mostly Effective	Critical	High
Network impacted by adjacent infrastructure failure or works, including Customer installations, e.g. solar systems					Technical Standards	Mostly Effective	Critical	High
Failure of underground network assets					Asset Inspection Policies and Programs (U/G+Subs)	Mostly Effective	Critical	Medium
Failure of equipment in zone substations (other than electrical protection)					Asset Inspection Policies and Programs (U/G+Subs)	Mostly Effective	Critical	Medium

Table 3-12 – ESMS Risks and sample of controls

The ESMS document describes how CP-PAL achieves and maintains a safe electrical network that minimises significant risks from occurring. The outcomes of the risk identification and assessment process reflect a commitment to the core values of ***Live Safely*** and ***Be Community Minded.*** The ESMS risk controls and cycle of continuous improvement demonstrates effective network management, protecting employees and the community from significant hazards AFAP, including:

- Bushfires started by CP-PAL assets, particularly powerlines
- Electric shock from CP-PAL assets
- Damage to property caused by CP-PAL assets

- Interruption of critical electricity supply

Government, regulators and communities within the CP-PAL network have confidence that the essential service provided will continue to be safe and reliable, now and into the future.

3.5 Planning and Preparation for Abnormal Operations

CP-PAL effectively manages a number of adverse conditions including:

- Significant supply disruptions
- Major bushfire
- Major asset failures (such as zone substation transformers)
- Major IT / communication assets outage
- Faults - restoration of supply after a major event

These types of events are managed through our Crisis and Emergency Management System Manual (C&EMS)[36]. This document describes CP-PAL's policy, guiding principles, resourcing, preparedness, response and recovery. The documents within this framework also define respective roles, responsibilities and identify the interface arrangements with outside organisations.

This C&EMS has been developed to meet the following commitment:

To provide the business with the ability to minimise the business impact of an event by creating appropriate strategies to meet the crisis and executing such strategies in a prompt effective and efficient manner.

The C&EMS provides for an effective state of readiness to prepare for, respond to and recover from, a range of credible or potential emergency events with the aim of mitigating the effects of the event AFAP. The system includes provision for:

- The overall plan for an emergency response
- The approach to emergency and crisis management
- Resourcing and maintenance of an emergency response and recovery process

Refer section 4.2.1.1 Emergency Preparedness and Response of this ESMS for further information.

3.6 Standards and Codes

CP-PAL adheres to publish technical standards and industry codes relevant to its network, which contribute to the development and maintenance of internal technical standards.

CP-PAL technical standards are the critical control, which specify safe standards for the design, construction and operation of network assets.

[36] CP-PAL, Crisis and Emergency Management System Manual – 13-40-CP0001

3.6.1 Standards and Codes Commitments

The commitment policies as discussed in *Section 2 Policy and Commitment* enable CP-PAL to establish the following technical standards key commitments:

- CP-PAL will identify and comply with all relevant Published Technical Standards & Industry Codes.
- Where compliance is not reasonably practicable, CP-PAL will ensure an equivalent safety outcome will be achieved.
- CP-PAL will consider the industry precedence and incident history within internal technical standards.

These commitments are further detailed in sections 3.6.2– 3.6.3 demonstrating **how** each are met.

3.6.2 Technical Standards Compliance Hierarchy

The CP-PAL technical standards hierarchy is shown in Figure 3-11.

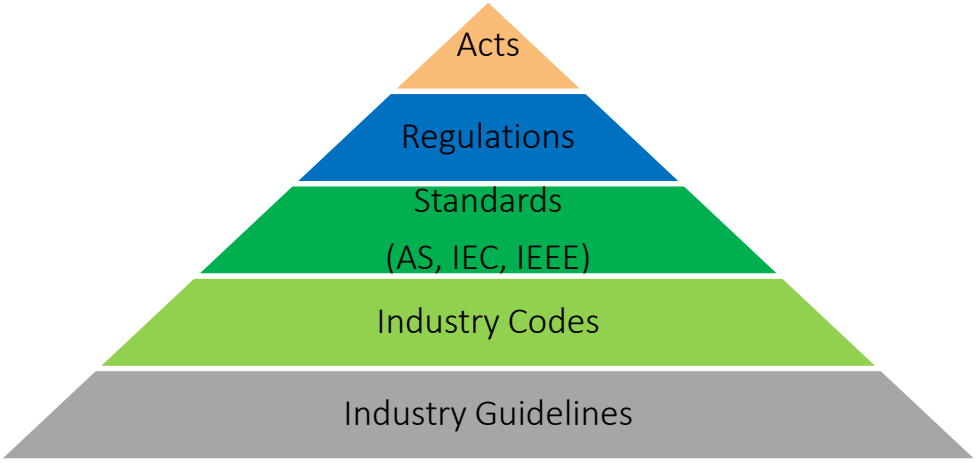


Figure 3-11 – CP-PAL Technical Standards Compliance Hierarchy

CP-PAL recognises the application of technical compliance via Hierarchy of Compliance per the five levels. Those five levels are elaborated below.

Acts

- Building Act 1975
- Electricity Safety Act 1998
- Electricity Industry Act 1998
- Energy Safe Victoria Act 2005

Regulations

- Building Code of Australia (BCA)
- Electricity Safety (Bushfire Mitigation) Regulations 2013

- Electricity Safety (Electric Line Clearance) Regulations 2015
- Electricity Safety (Installation) Regulations 2009
- Electricity Safety (Management) Regulations 2009
  - AS 5577 Electricity network safety management systems
- Essential Services Commission (ESC) Code
- The Blue Book 2017

Standards

CP-PAL recognises all the following published technical standards relevant to electricity distribution networks for the basis of design, construction, operation and maintenance activities on its networks:

- Australian Standards

Where Australian standards do not cover the specific asset need, reference are made to international standards, such as:

- International Electrotechnical Commission
- Institute of Electrical and Electronics Engineers

The *Technical Standards References to External Standards Matrix*[37] is used for identification of all external published technical standards relevant to the CP-PAL networks. The matrix charts the external published standards (e.g. AS1158 Road Lighting) according to their relevance to internal CP-PAL technical standard sections (e.g. 'F – Public Lighting' section of standards).

Network Asset Regulations (1999) are used as a reference for relevant existing technical standards.

[37] CP-PAL, Technical Standards References to External Standards Matrix – JEQA4UJ443MT-224-16

External Standards (including Australian Standards, IEC, EIA, IEEE)
ACA (Australian Communications Authority) TS008
AS1033.1 High voltage fuses (for rated voltages exceeding 1000 V) - Expulsion type
AS1033.2 High voltage fuses (for rated voltages exceeding 1000 V) - Current-limiting (powder-filled) type
AS1158.0:2005 Road lighting – Introduction
AS1243 Voltage transformers for measurement and protection
AS1306 High voltage a.c. switchgear and controlgear - Disconnectors (isolators) and earthing switches
AS1307.2 Surge arresters - Metal-oxide surge arresters without gaps for a.c. systems
AS1675 Current transformers - Measurement and protection
AS1798:2014 Lighting poles and bracket arms - Recommended dimensions
AS1940 The storage and handling of flammable and combustible liquids
AS2067 Substations and high voltage installations exceeding kV a.c.
AS2374.6 Power transformers - Determination of transformer and reactor sound levels
AS2374.7 Power transformers - Loading guide for oil-immersed power transformers
AS2676 Guide to the installation, maintenance, testing and replacement of secondary batteries in buildings
AS2878 Timber - Classification into strength groups
AS3000 Electrical installations (known as the Australian/New Zealand Wiring Rules)
AS3600 Concrete structures
AS4026 Electric cables - For underground residential distribution systems
AS7000 Overhead line design
Building Code of Australia
IEC 1230. Live Working - Portable Equipment for Earthing or Earthing & Short-Circuiting
IEC 61230 Live working - Portable equipment for earthing or earthing and short-circuiting.
IEEE 80 Guide for Safety in AC Substation Grounding
ITU--T (International Telecommunications Union -- Telecommunications Standardisation Sector) recommendationG.652 and IEC Standard 60973--1/2

Figure 3-12 – Extract of the Technical Standards Group References to External Standards Matrix

Industry Codes

Further to the Published Technical Standards, reference may also be made to industry codes or Guidelines including:

- The Code of Practice on electrical safety for work on or near high voltage electrical apparatus (the Blue Book)
- Electrical Safety Rules for the VESI Distribution Networks (the Green Book)
- VESI – Service Installation Rules

Industry Guidelines

- Energy Networks Australia (ENA) Guidelines
- Energy Supply Association Australia (ESAA) Guidelines

CP-PAL ensures compliance to these codes and utilises industry guidelines as reference through employee representation on the relevant electricity distribution committees. Committee representatives[38] are tasked with keeping CP-PAL up-to-date on various requirements and changes that might arise in updates to the codes and guidelines.

We participate as required and co-ordinate with Vic DBs to ensure appropriate representation on relevant committees.

[38] Industry Representatives (By Committee Groups)

3.6.3 Managing Contradictions

Where ever there is contradiction between different levels of the compliance hierarchy as noted in Figure 3-11, CP-PAL align its compliance to the higher level. For example, in an event where the requirements differ between Regulations and Australian Standards, Regulatory requirements take precedence.

Where a technical standard refers to multiple published technical standard references, the technical standard will specify the applicable sections which apply.

3.6.4 CP-PAL Design Construction and Commissioning Technical Standards

The Technical Standards Group is responsible for:

- Providing engineering and technical expertise.
- Managing the delivery of engineering solutions to meet current and future asset management needs.
- Development and approval of Technical Standards and Specifications in accordance with the *Manage Network Technical Standards Procedure*[39].
- Approving the selection of all electrical network assets (i.e. material purchasing specifications for all primary, secondary, overhead, underground and public lighting assets) procedure and how it is done.

3.6.5 CP-PAL Testing Standards

CP-PAL has a suite of testing standards. These testing standards are based on manufacturers' standards that are used to prove Australian Standards compliance.

3.6.6 CP-PAL Operation Standards

CP-PAL has a suite of electrical operating procedures, which are recognised as operating standards, reference is made to the *CP-PAL Operations Procedures Manual*[40]. These standards are compliant to the requirements of the Blue Book, Green Book, VESI Codes and Guidelines.

3.6.7 CP-PAL Maintenance Instruction

CP-PAL use the *Instruction for Replacement Works*[41] for maintenance and fault follow-up works. This instruction lists the asset replacement situations and makes recommendations to undertake

[39] CP-PAL, Manage Network Technical Standards Procedure – JEQA4UJ443MT-150-516

[40] CP-PAL Operations Procedures Manual – JEQA4UJ443MT-185-11385

the replacement in accordance with the specified technical standards. For example, one of the listed situations of the guideline is provided in Table 3-13.

Situations	Recommendations
Insulators (Refer Maintenance Policy Document No. 05–C001.D– 330)	
Replacing a HV pin insulator on a wood cross arm in a delta structure	Select the appropriate codes from Technical Standard EF101. For like for like replacement where phase to phase clearances (DC161) are to be maintained, 5 shed porcelain post insulator is available in Technical Standard material schedule EF312, material # 350700

Table 3-13 – Example: Instruction for Overhead Replacement Works

LV Service Ground Clearances Maintenance – The ground clearances of LV services are maintained in accordance with the Asset Maintenance Policy for Low Voltage Aerial Service Cables (Ground Clearance)[42].

By effective implementation of the abovementioned policy, CP-PAL effectively manages the risk associated with LV aerial service cables ground clearances.

3.6.8 Present Published Technical Standards Deviations

CP-PAL presently deviate from the following published technical standard requirements:

- EG-0 Power System Earthing Guide Part 1: Management Principles, Version 1

CP-PAL has a schedule in place to develop a strategic plan which will implement the requirements of EG-0 into all CP-PAL technical standards. The plan milestones are listed below, to be completed by 31 December 2018.

1. Develop scope for earthing consultant to review standards and provide recommendations
2. Determine all affected technical standards and maintenance policies
3. Receive quote from earthing consultant
4. Provide earthing consultant approval to proceed with review
5. Receive evaluations report from earthing consultant
6. Determine high risk non-compliances from earthing consultants report
7. Develop priority strategic plan to outwork high risk non compliance issues
8. Develop strategic plan to update all technical standards

[41] CP-PAL, Guidelines For Use of Standards in Overhead Replacement Works – JEQA4UJ443MT-150-552

[42] Asset Maintenance Policy for Low Voltage Aerial Service Cables (Ground Clearance) – 05-C001.D-262

- AS 7000 Overhead Line Design, detailed procedures

CP-PAL, in consultation with other VESI representatives have demonstrated that current methods for overhead structures meet the minimum level of compliance required by AS7000 design parameters. CP-PAL has plans in place to be compliant with requirements of AS 7000. Refer Appendix 16.

3.6.9 Standards References Where No Current Applicable Published Technical Standards Exist

Where no current applicable published technical standards exist, CP-PAL established the relevant references of the published technical standards.

Presently there are no current applicable published technical standards relevant to CP-PAL for underground (UG) cable depth requirements on public land. Network Asset Regulations (1999) are used as a reference for specifying the UG cable depth requirements.

3.6.10 New Standards and Initiatives

The CP-PAL Technical Standards group provides information to employees and contractors regarding new or updated standards, specifications and initiatives in the design and construction of network assets. This information is published via internal technical standards, technical bulletins and materials and equipment specifications, which is formally released on a monthly basis and stored for reference in the company's intranet.

When a new item of equipment or new technical standards are introduced, a specially convened information session is conducted.

All contractors or external stakeholders associated with works on CP-PAL assets can apply to the company to gain "read only" access to the technical standards folder. Extract of Contractor Portal is shown in Figure 3-13 below.

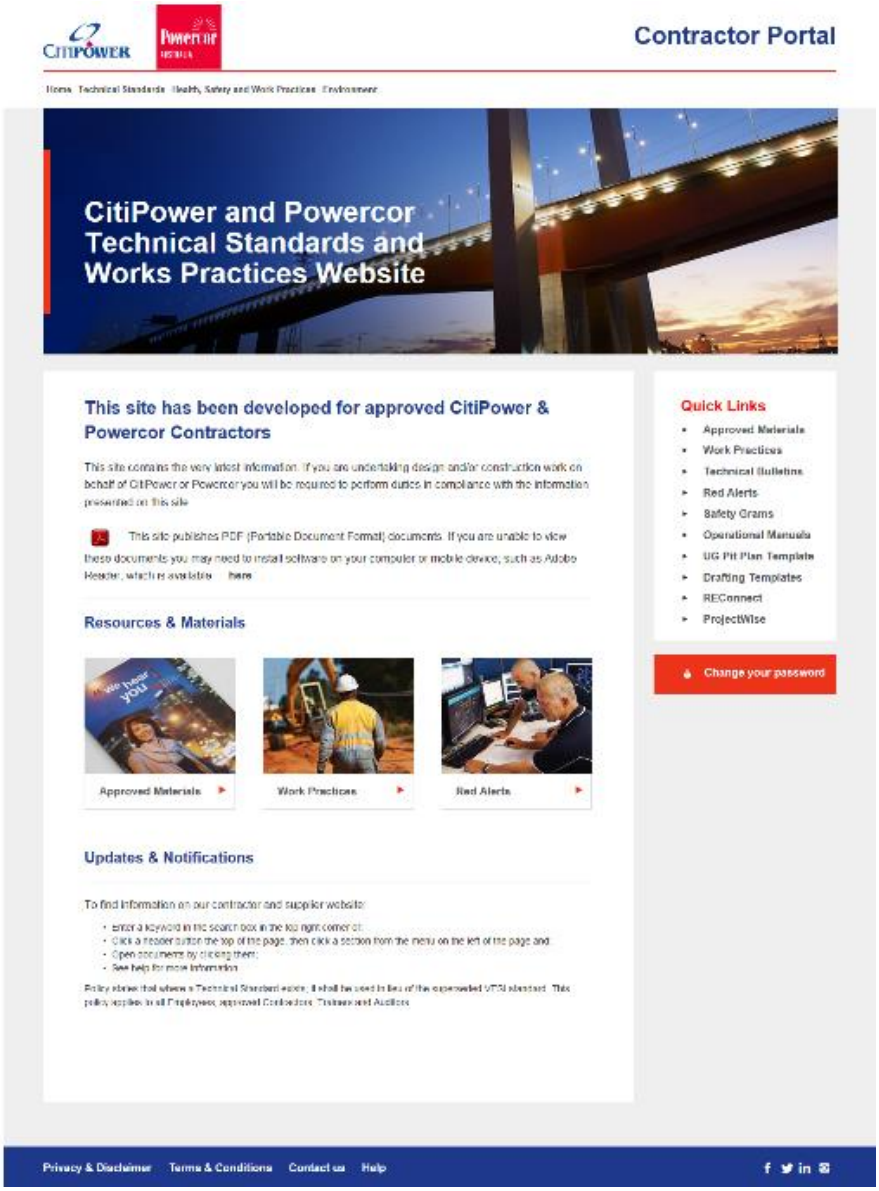


Figure 3-13 – CP-PAL Contractor Portal

3.6.11 Technical Standards Deviation Management

Where CP-PAL is unable to comply with particular provisions of its technical standards, it utilises the *Deviation from Technical Standards Procedure*[43].

The common areas of deviation are:

- Integration with old installations, such as tie-ins.
- Asset clearances to existing assets, such as UG conduit clearances requirements are unable to be met from water mains within existing shared trench.
- Location of existing 3rd party service in shared trench etc.

[43] CP-PAL Deviation from Technical Standards Procedure - JEQA4UJ443MT-173-113

Deviations from standards shall only be an option when all alternative design options have been exhausted. Any alternatives to standards are appropriately developed and reviewed by the Program Design & Delivery and Network Safety groups prior to construction, with any deviation from standards documented. This process ensures that any approved deviations from approved technical standards adhere to an equivalent level of safety and compliance.

The dispensation process is illustrated in Figure 3-14 below.

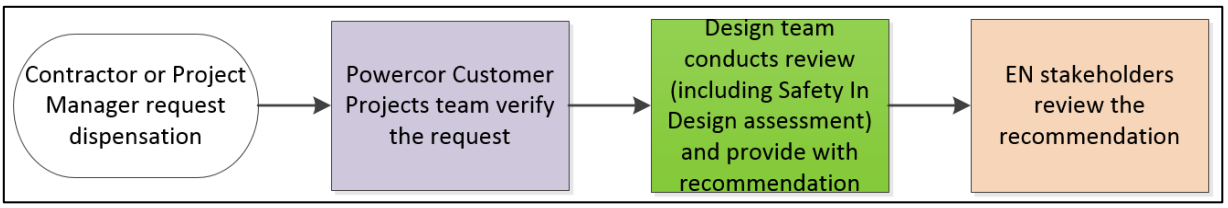


Figure 3-14 – Simplified Dispensation Process

The process is initiated by a Contractor or Project Manager who submits a dispensation request and completes the Dispensation Request Form.

CP-PAL Customer Projects team then verifies the request and relevant information, completes the Design Request Form and forwards the relevant documentation to the Program Design & Delivery division for evaluation.

Program Design & Delivery then conducts their evaluation of the proposed dispensation request and lprovide with recommendations. This ensures all risks, benefits and costs of the proposed solution based on the *Manage Safety in Design Procedure*[44] are considered.

Recommendations are reviewed by relevant EN stakeholders. Any objections to the recommendations are flagged and resolved prior to dispensation request is approved.

The 'Deviation from Technical Standards' procedure require involvement of key stakeholders.

Non-Standard Structures

A non-standard structure is defined as any structure that is not in the CP/PAL technical standards, or VESI standards (where a CP/PAL standard does not exist). In an event where non-standard structure needs to be built, the Non Standard Structure Approvals Procedure[45] is followed. This procedure ensures that non-standard structures are appropriately developed or reviewed before construction.

CP-PAL has implemented a Non Standard Structure Register. From 2019 onwards, all non-standard structures, which are approved and constructed as per the Non Standard Structure Approvals Procedure, will be included in the Non Standard Structure Register.

[44] Manage Safety In Design Procedure – JEQA4UJ443MT-160-162

[45] Non Standard Structure Approvals Procedure – JEQA4UJ443MT-160-43

3.6.12 Introduction of New Plant and Material

The Technical Standards section manages the evaluation and introduction of new equipment. Prior to the purchasing and introduction of new equipment, a detailed assessment is undertaken in line with the *Introducing New Plant and Materials Procedure*[46] to ensure safety and compliance. This procedure is supported by the Asset Lifecycle Checklist Form[47] This procedure also aims to ensure that all plant and materials are introduced into the network within a consistent framework and comply with business requirements. The process of introduction of new equipment includes:

- Identification of need for new equipment.
- Review and consultation with stakeholders including safety, works practices, operations, design, construction and maintenance.
- Establishment of technical team and development of technical requirements (including compliance certifications).
- Field Trial Process to ensure that a structured and consistent asset lifecycle approach for the approval and implementation of trials is followed. The outcome of a trial is a recommendation regarding adoption for an item of equipment.
- Review of recommendations from internal and external sources.
- Preparation, review and approval of technical specifications.
- Issuing specifications to the suppliers as part of tender evaluation process
- Recommendation of awarding contracts,
- Witnessing factory acceptance testings.

The *Manage Network Technical Standards Procedure*[48] ensures that the introduction and/or modification of Network Technical Standards and specification documentation follow a consistent process, ensuring engagement and approval from relevant stakeholders.

3.6.13 Updates to Technical Standards

3.6.13.1 Changes to existing standards

Technical standards are reviewed and updated based on the following triggers:

- Introduction of new materials or updates to materials and equipment (involving the *Introducing New Plant and Materials Procedure*[49])
- Incident investigations

[46] CP-PAL, Introducing New Plant & Materials Procedure – JEQA4UJ443MT-150-27375

[47] Asset Lifecycle Checklist Form - JEQA4UJ443MT-160-222

[48] CP-PAL, Manage Network Technical Standards Procedure – JEQA4UJ443MT-150-516

[49] CP-PAL, Introducing New Plant & Materials Procedure – JEQA4UJ443MT-160-222

- Audit findings
- Project specific needs
- Updates to Australian Standards (and other published technical standards)
- Changes to Regulations

CP-PAL subscribes to SAI Global's 'Standards Watch' for monitoring standard updates. All the relevant Australian Standards are selected for monitoring updates.

The organisation is notified when changes are made to an International or National Standard to ensure internal standards remain compliant. Refer Appendix 12.

Due to the extremely large number of published CP-PAL technical standards, CP-PAL relies on the above mentioned review triggers and monitoring methods to update their technical standards rather than the date of their creation.

3.6.13.2 New Standards

The Energy Networks Australia (ENA) also advises Technical Standards Reference Group of upcoming standard reviews where representatives from CP-PAL are nominated to participate in the development of these standards. Refer .

3.6.14 New Technical Standards

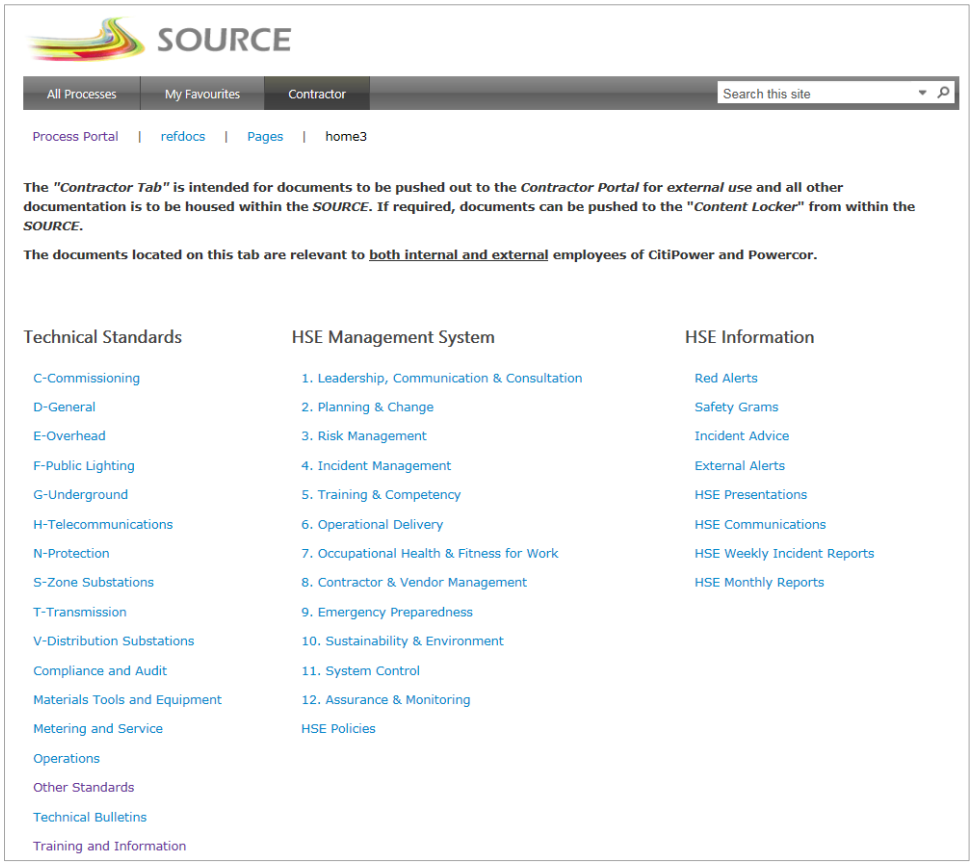
CP-PAL has a Technical Reference Group (reference). This group identifies the relevant new industry standards, which are proposed to be developed. Once the scope of the proposed standards is determined, CP-PAL nominates relevant Subject Matter Experts to be part of the proposed standards development committees.

3.6.15 Storage and Access of Technical Standards

All company standards are housed and accessed via the company's intranet. Each group of technical standards are generally arranged into the following sections:

- Revision history
- Table of contents
- General information
- Design information
- Construction information
- Material information

This information can be accessed via the Source Document system. A capture of the information page is represented below.



Note: This is the screen extract only and is subject to change

3.6.16 Business Wide Communication

CP-PAL Technical Standards issue update e-mail notifications to communicate changes to technical standards. These notifications provide listing of updated Technical Standards, overview of changes made and impacted key stakeholder groups (such as construction, maintenance or design teams). An example is shown below in Figure 3-15.

A message from **Steven Neave**
General Manager, Electricity Networks

4 April 2017

The following message is from the Technical Standards Manager….

CitiPower / Powercor Technical Standards Update

Please ensure that this information is passed on to all field employees and contractors without electronic access.

The following Technical Standards updates are relevant to all technical and construction employees and contractors undertaking design and/or construction activities on the CitiPower and Powercor networks.

A list of the **CitiPower/Powercor Technical Standards March 2017 releases** is available below, including links to summaries and are available to view in full on the Source.

*All new design and construction proposals commenced after the **1 June 2017** are required to comply with these Technical Standards updates.*

If you have further questions, please contact the relevant Technical Standards Engineer associated with the published Standards/Specifications.

Regards

Steven Neave
General Manager, Electricity Networks

Never Compromise Safety Rules

1. Electrical permits
2. Live work
3. Polarity and NST testing
4. Working at heights
5. Plant and equipment
6. Personal protective equipment (PPE) and clothing
7. Drive safe
8. Risk assessment

NEVER COMPROMISE health & safety

Standard Category	Technical Standard	Standard Description	Overview	Impacted Key Stakeholder/s
D - General	DE011	Distribution Construction Standard - Connectors – Application	Standard updated to remove auto splice information and add 3 new full tension compression sleeves as the standard connection for copper and cad copper conductor. **Contact Darren Martini (03) 9683 4738**	CONSTRUCTION DESIGN
	DE131	Distribution Construction Standard - Connectors – Full-Tension Splices	Standard updated to remove all information regarding auto splices. **Contact Darren Martini (03) 9683 4738**	
	DE136	Distribution Construction Standard - Connectors – Full-Tension Sleeves	Standards updated to include 3 new full tension compression sleeves for existing imperial Cad Cu conductors (7/0.073, 7/0.093, 7/0.113) to table 2 & 4. **Contact Darren Martini (03) 9683 4738**	
	DE411-705	Distribution Construction Standard - Splices, Sleeves, Links, Lugs & Misc. Connector Materials	Standard updated to remove DE411 and add 3 new full tension compression sleeves for existing imperial Cad Cu conductors (7/0.073, 7/0.093, 7/0.113) to DE431. **Contact Darren Martini (03) 9683 4738**	
Click here for a SUMMARY of the above standards				

LEGEND
HIGH IMPACT
MEDIUM IMPACT
LOW IMPACT

Figure 3-15 – CP-PAL's Technical Standards Update

3.6.17 Governance

Approvals of technical standards are managed using Technical Standards Update Checklist[50]. This checklist includes the following key topics:

- Identification of stakeholders
- Review of key hazards
- Update Standards / Specifications
- Prepare Standards / Specifications for publishing
- Release Standards
- Communication Plan
- Change Management / Implementation Plan

Head of Network Asset Management approves CP-PAL technical standards using Technical Standards Update Checklist.

CP-PAL Field Audit and Quality section undertakes construction and connections audits to ensure application of CP-PAL Technical Standards and manuals. These audits are undertaken based on the requirements of the CP-PAL Technical Standards and manuals.

Any non-conformances identified during these audits are reported to the party being audited (internal and external). Reported non-conformances are monitored to resolution. The audit results summary is provided to relevant business units on a quarterly basis at the Network Quality Forum.

As mentioned in section 4.3.3.4, CP-PAL has operational standards for accessing and operating the network. The performance of these operational standards is monitored via an Operating Performance Excellence Committee[51] where the findings of the field operating audits, identified hazards and operating incidents are reviewed. Post these reviews corrective actions are developed and implemented.

[50] Technical Standards Update Checklist – JEQA4UJ443MT-150-518

[51] Operating Performance Excellence Committee Charter

Section 4. IMPLEMENTATION - RISK CONTROLS

This section addresses the clause 4.4 requirements of AS 5577:

4.4 – Implementation

4.4.1 – General

The Network Operator shall define how it will implement the ENSMS.

4.4.2 Resourcing

The Network Operator shall identify the resourcing, equipment and material requirements for the network's safe operation and maintenance, including carrying out of hazard controls and mitigation identified in the Formal Safety Assessment. Appropriate resources shall also be identified to ensure the appropriate development, implementation, monitoring and review of the ENSMS.

Sufficient personnel should be available for undertaking planned and unplanned operations and maintenance, taking into account the requirements for leave and training.

4.4.3 Management structure

A defined management structure for the Network Operator shall be established to identify key positions and/or personnel. The management structure shall be appropriate to the size and complexity of the network.

4.4.4 Responsibilities, accountabilities and authorities

The responsibilities, accountabilities and authority levels of personnel and/or contractors, with respect to the various aspects of the design, construction, commissioning, operation, maintenance and decommissioning of the network, shall be detailed in the ENSMS. In particular, personnel shall be identified and documented with the responsibility and authority to—

(a) approve policies and procedures;

(b) initiate action to, so far as reasonably practicable,—

(i) prevent safety issues arising from a loss of supply;

(ii) prevent environmental impact;

(iii) mitigate the impact of such events to the public; and

(iv) correct electricity network safety issues;

(c) identify, record and report on any existing or potential deficiencies within the ENSMS or the network's design, construction, commissioning, operation, maintenance and decommissioning;

(d) initiate, recommend, approve and monitor corrective and preventive actions in relation to identified existing or potential deficiencies within the ENSMS or the network's design, construction, commissioning, operation, maintenance and decommissioning;

(e) evaluate and verify the effectiveness of any corrective or preventive action implemented;

(f) satisfy the mandatory approval requirements of this Standard for specific items to be approved.

4.4.5 Training and competency

The Network Operator shall ensure that all persons involved with the design, construction, commissioning, operation, maintenance and decommissioning of the network are suitably competent and adequately trained to carry out their duties.

The Network Operator shall establish and maintain procedures for identifying, facilitating and/or providing the training needs of all personnel operating the network covered by the ENSMS.

As a minimum, personnel responsible for the operation and maintenance of the network shall, as applicable to their position, be adequately trained in the obligations of the ENSMS and briefed in the requirements of the controls and actions identified during the Formal Safety Assessment (see Appendix A).

NOTES:

1 Competency is the consistent application of knowledge and skill to the standard of performance required in the workplace.

2 Detail on the framework for national competencies for electricity supply can be found at the www.ee-oz.com.au website.

4.4.6 Consultation, communication and reporting

4.4.6.1 Consultation

The Network Operator shall identify individuals, stakeholder groups and organizations that have a relevant interest in the safety aspects of the design, construction, commissioning, operation, maintenance and decommissioning of the network. These may include, but are not limited to, landowners, employees, employee representative organizations, contractors, utilities, accredited service providers, local and emergency authorities, regulatory authorities and government agencies.

4.4.6.2 Communication and reporting

The Network Operator shall establish procedures for regular consultation and communication with, and reporting to, these identified stakeholders during the development, implementation and review of the ENSMS. These procedures need to include statutory reporting obligations in line with jurisdictional regulatory requirements.

4.4.7 Emergency preparedness and response

The Network Operator shall plan and prepare for emergency events resulting from the network's operation and maintenance and also from external events that may affect the safe operation of the network.

In the event of an emergency, the Network Operator shall ensure that any response is performed in a safe manner.

NOTES:

1 Liaison with emergency services and stakeholders may assist the Network Operator to be adequately prepared for an emergency event.

2 AS 3745, Planning for emergencies in facilities, provides guidance.

4.1 Role of ESMS and Integration with Business Management Systems

The ESMS utilises the CP-PAL *Enterprise Risk Management* (ERM) Framework to establish its Formal Safety Assessment (FSA) Framework, which is one of the key processes within the ESMS.

Figure 4-1 illustrates the integration of the CP-PAL ESMS with other Business Management Systems and key network activities.

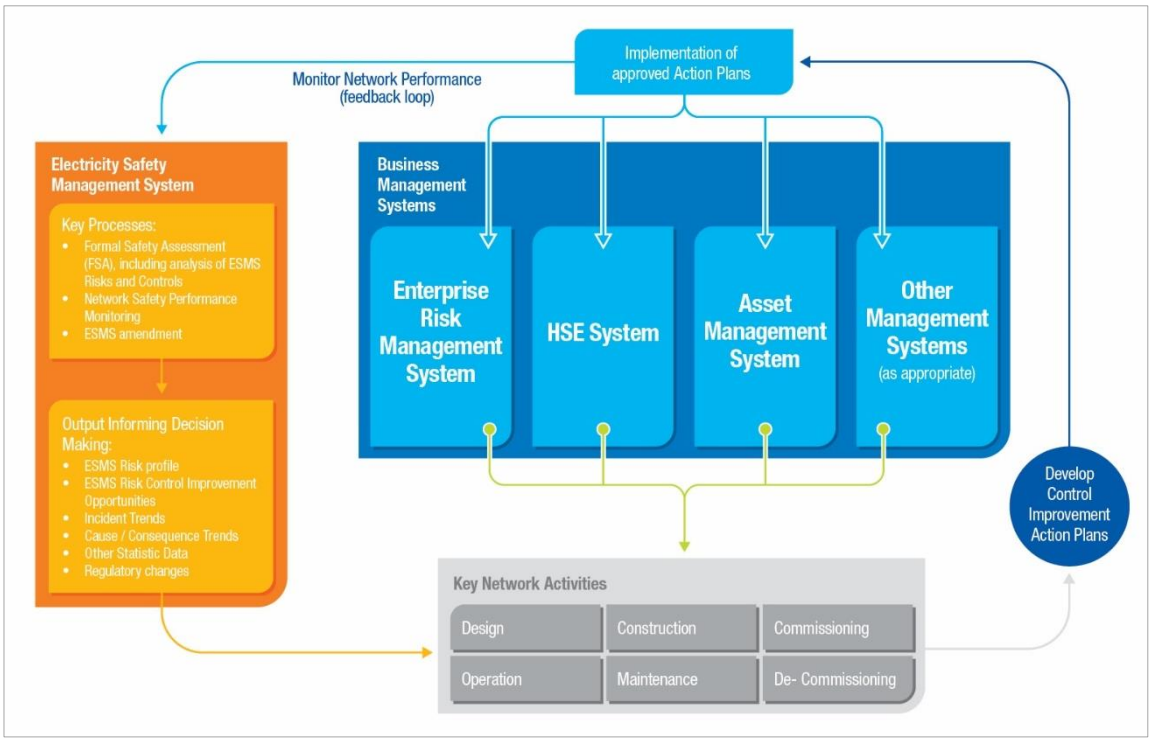


Figure 4-1 – ESMS Interaction with CP-PAL Business Management Systems and Key Network Activities

Enterprise Risk Management System

Topic	AS 5577 Section	ESMS Section Reference
Emergency preparedness and response	4.4.7	4.2.1.1

HSE System

Topic	AS 5577 Section	ESMS Section Reference
Incident management	4.5.2	5.2
Training and competency	4.4.5	4.2.2.1
Operational delivery (including Works Practices)	4.1	4.2.2.2

Asset Management System

Topic	AS 5577 Section	ESMS Section Reference
Asset Management System	4.1	4.2.3
Network Planning	4.3.2	4.2.3.7
Vegetation Management	Foreword	4.2.3.8
Bushfire Mitigation	Foreword	4.2.3.9

Other Management Systems

Topic	AS 5577 Section	ESMS Section Reference
Resourcing	4.4.2	4.2.4.1
Responsibilities, accountabilities and authorities	4.4.3	4.2.4.1
Consultation, communication and reporting	4.4.6	4.2.4.1

The implementation requirements of AS 5577 Section 4.4 are addressed as follows:

4.1.1 Formal Safety Assessment (FSA)

The development of our ESMS involves a FSA of our network risks with specific focus on the safety of employees, contractors and the public. FSA workshops are held every five years with subject matter stakeholders (representatives from the key network activities of design, construction, operation, maintenance) to review and assess the identified ESMS risks and update the risk register with relevant outcomes. Network safety performance and mitigating controls are assessed during an annual risk profiling activity. Subsequent FSA workshops are also held which inform the currency of the Corporate Risk and ESMS Risk Registers.

4.1.2 Network Safety Performance Monitoring

The safety performance of the network is continually monitored and reviewed in accordance with the *Formal Safety Assessment ESMS FSA Monitoring and Review Procedure*[52]. The outcomes of these reviews, plus system audits and incident investigations are critical inputs when undertaking FSA reviews.

The Formal Safety Assessment ESMS FSA Monitoring and Review Procedure involve:

- Establishing the risk context
- Identification of significant risks
- Assessment of risks
- Determination of risk control measures

In addition to safety, a range of other network and operational performance issues are considered namely:

- supply reliability
- asset failure rates
- human errors
- incident trends by causes / consequences

Bushfire Mitigation and Electric Line Clearance requirements are included in the FSA reviews, which includes assessment of environmental changes since the last review (typically within the last five years) as an input.

Implementation of individual control improvements is also considered during an annual risk profiling activity, which includes assessment of the control reliance and effectiveness.

Network safety performance is also monitored and governed via Strategic Asset Management – Network Safety Committee.

4.1.3 Outputs Informing Decision Making

Outputs from the Electricity Safety Management System processes are used to inform relevant Business Management Systems including:

- Enterprise Risk Management System
- HSE Management System
- Asset Management System
- Other Management Systems as appropriate, such as Quality and Environmental Management Systems

[52] Refer document ESMS FSA Monitoring and Review Procedure – JEQA4UJ443MT-173-48

These systems specify requirements of key network activities namely the design, construction, commissioning, operation, maintenance and decommissioning of network assets.

The ESMS considers the key network activities as risk mitigation controls. Any areas for improvement to the existing ESMS risk mitigation controls are identified and improvement action plans are implemented in accordance with our *Enterprise Risk Management Framework*[53] and *ESMS Formal Safety Assessment – Risk Owner Procedure*[54].

Identified *Control Improvement Action*(s) are further investigated to confirm (through budget forecasting and business case) the implementation of the improvement action(s). CP-PAL has commenced implementation of a new asset planning & investment tool (Copperleaf) which will replace the existing Utility Asset Management Performance (UMS) investment tool. Refer Appendix 16.

4.2 ESMS Interaction with Business Management Systems

The ESMS is a key management system that co-ordinates and informs other areas of the business to deliver a safe, reliable and affordable electricity network.

The interaction of the ESMS with the three key management systems namely Risk Management, Asset Management and Health Safety and Environment Management is discussed in the following sections.

[53] Enterprise Risk Management Framework - JEQA4UJ443MT-154-357

[54] ESMS Formal Safety Assessment – Risk Owner Procedure – JEQA4UJ443MT-173-78

4.2.1 Enterprise Risk Management System

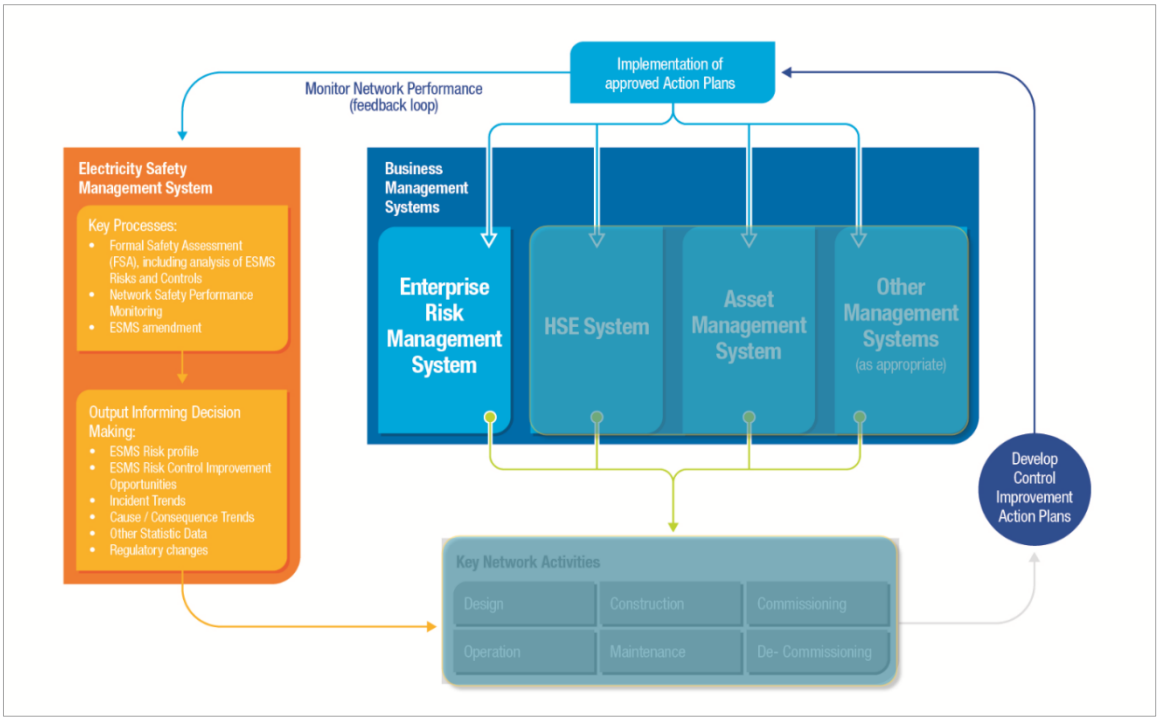


Figure 4-2 – ESMS Integration with Enterprise Risk Management System

The interaction of the ESMS with the Enterprise Risk Management System provides for a consistent framework across the business for the identification, assessment and control of risks. This integrates the HSE and Asset Management risks into the electricity network safety risks with the ESMS and also with the overarching Enterprise Risk Framework. Refer Figure 4-2.

4.2.1.1 Emergency Preparedness and Response

As discussed in Section 3.5 Planning and Preparation for Abnormal Operations, CP-PAL employs the *Crisis Management Plan (CMP)*[55] which is the peak framework and an ESMS control to mitigate any adverse issues that may impact its operation. The CMP comprises of the highest framework document describing CP-PAL's policy, guiding principles, resourcing preparedness response and recovery. These documents also define respective roles, responsibilities and identify the interface arrangements with outside organisations.

The CMP provides an effective state of readiness to prepare for, respond to and recover from a range of potential events, with the aim of minimising the effects of the event AFAP. This capability is regarded as fundamental to maintain a safe network.

[55] Crisis Management Plan - JEQA4UJ443MT-154-386

4.2.1.2 Crisis Management Process[56]

The Crisis Management Process is based on the following high-level process:

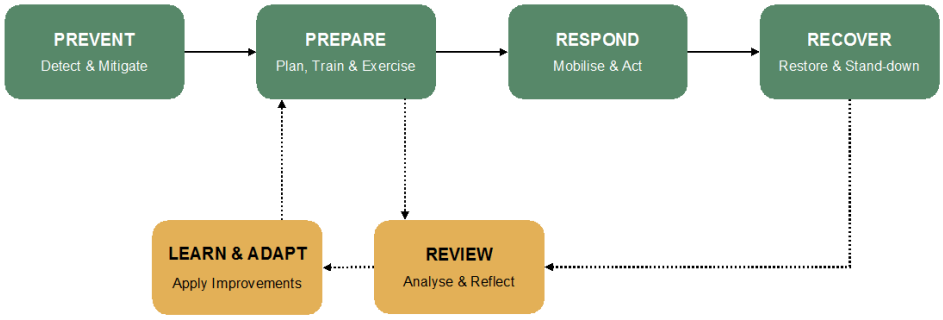


Figure 4-3 – CP-PAL Crisis Management Process

This is a holistic approach involving steps to:

- Prevent (by detecting and mitigating risks);
- Prepare (planning and preparing) by developing documentation, training and testing;
- Respond (making people safe, minimising damage, managing strategic issues and consequences);
- Recover (repairing negative impacts);
- Review the response during an actual incident or an exercise; and
- Learn and adapt (reviewing and improving arrangements).

A successful critical incident management program requires integration and cooperation across all these areas.

4.2.1.3 Emergency Escalation Process

CP-PAL manages its emergency escalation process using crisis management plan[57]. The escalation process consists of three levels, each declared by responsible managers and determined by the teams responsible to control an event. The severity matrix of events are provided in Appendix 11.

The severity matrix categorises three levels, are presented in Appendix 11.

Crisis Management Framework Reporting Structure

The organisation has adopted the Australian Inter-Service Incident Management System (AIIMS) model as the good practice framework for the development of a flexible and scalable incident management structure.

AIIMS was developed as a common methodology by Australian State and Territory governments following recognition that emergency events do not respect arbitrary boundaries, and that many

[56] Crisis Management Plan - JEQA4UJ443MT-154-386

[57] Crisis Management Plan – JEQA4UJ443MT-154-386

agencies from multiple jurisdictions may become involved in the response to emergency events. Consequently, (AIIMS) is an established all-hazards-all-agencies model of incident management.

Where relevant the Crisis Management Framework and Procedures have been aligned to AIIMS model. There has been some modification to some of the role titles and structures to suit existing operational reporting lines, roles and terminology. Refer Figure 4-4 below:

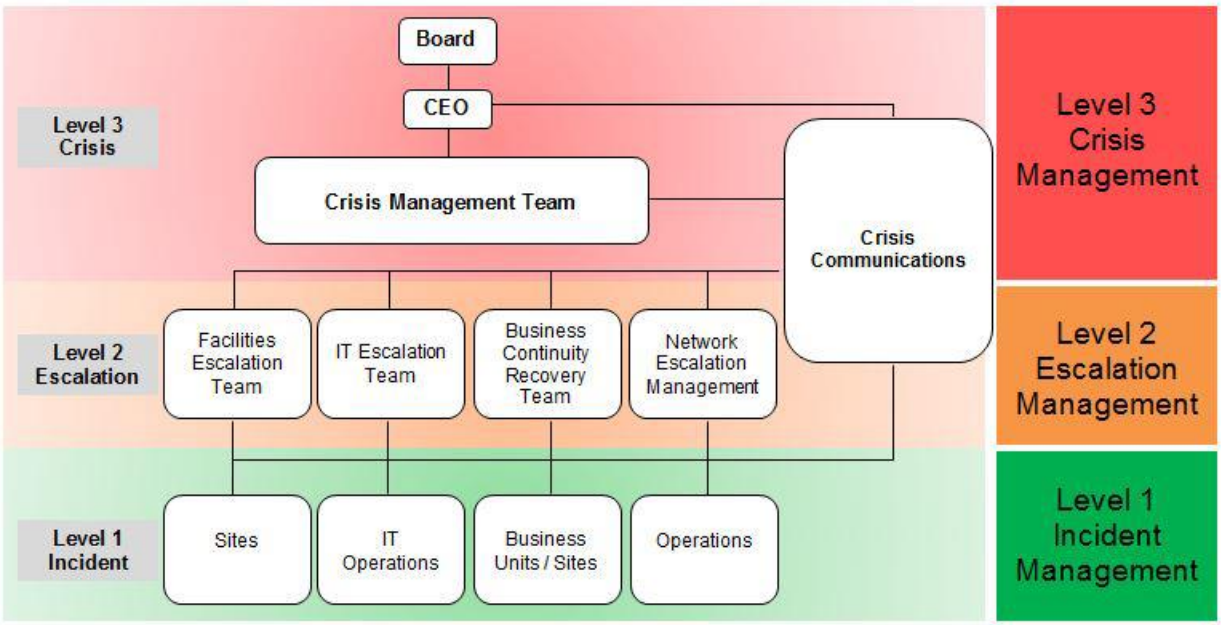


Figure 4-4 – Crisis Management Framework Reporting Structure

4.2.1.4 Structure of Emergency Management

Figure 4-5 demonstrates the structure of Crisis Management Team (CMT).

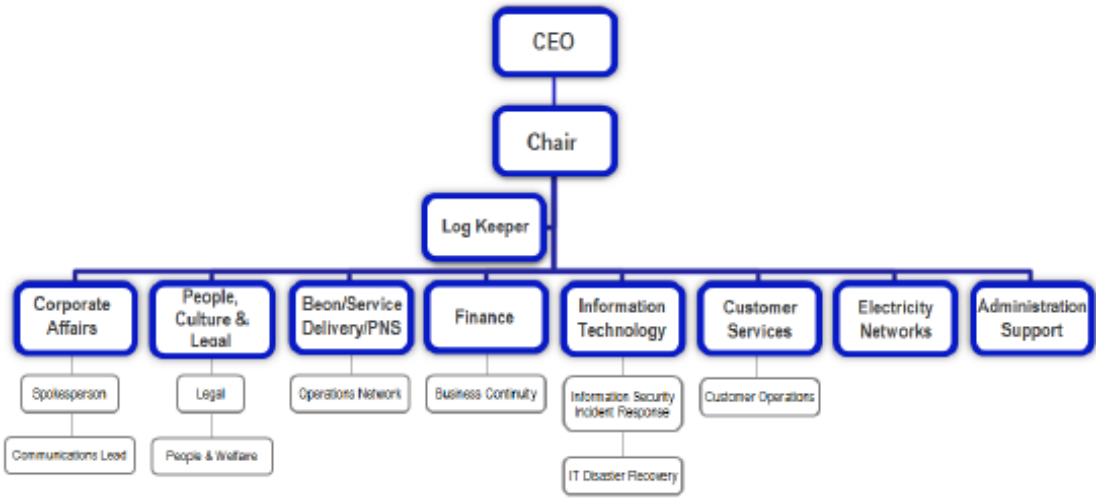


Figure 4-5 – CP-PAL Crisis Management Team structure

The function of the CMT is to manage a crisis at a strategic level. Once activated, the CMT will receive input from all groups involved in the crisis. The crisis is monitored and assessed for the impact on people, statutory and legal obligations, customers, community and corporate reputation. Decisions will be made to address the impact on the Organisations image with the ultimate aim being safe and reliable operations.

The Crisis Management Team (CMT) is the highest-level incident structure and is a scalable, flexible command-and-control structure. The CMT is made up of key senior staff ('Core' CMT) and functions teams ('Full' CMT).

Crisis Management Response Process

The Crisis Management Response Procedures are a set of standard of incident response steps that the CMT members should refer to during an event. There are generally 8 standard steps which are outlined in Figure 4-6 below.

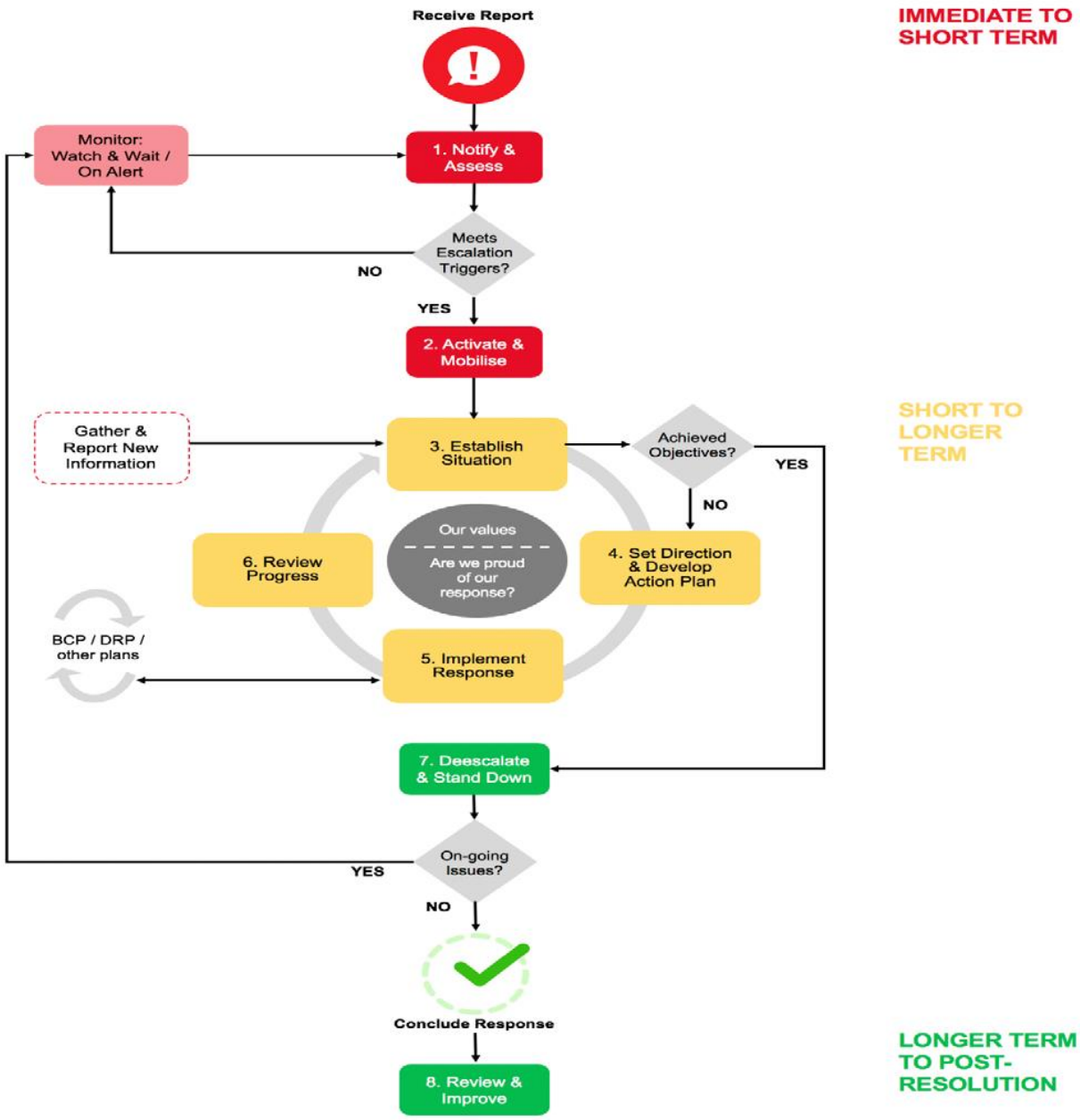


Figure 4-6 – CP-PAL Crisis Management Procedure Steps

Detailed tasks of each step are noted within Crisis Management Procedures[58]

4.2.1.5 Resilience

CP-PAL is committed to effective planning for Organisational Resilience by having a robust Resilience Framework[70] that protects our assets, facilities, systems and people, as well as minimising the impact to our stakeholders.

[58] Crisis Management Plan - Part 2 Procedures - JEQA4UJ443MT-154-388

The key areas of resilience framework are outlined in Figure 4-7 below.

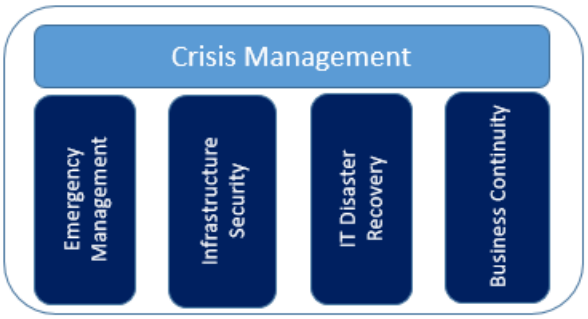


Figure 4-7 – VPN Business Resilience Key Areas

The Framework promotes the use of a common terminology and structure to avoid confusion during the management of disruptive events.

The Event Command Organisation (ECO) Manual[71] supports CP-PAL to be resilient organisations. Resilience is:

- Our ability to resist disruptive events, and to rebound, recover, strengthen and grow should a disruptive event occur.
- A function of our situation awareness, our planning for management of vulnerabilities and our capacity to adapt when business is interrupted.
- A management guideline for minimising the impacts of disruptions which affect our ability to conduct our business as usual might include financial stress, loss of the use of facilities, systems, major assets or people, or actions of government, regulators, or media.

The overall resilience of CP-PAL is measured by our ability to respond to, and recover from events rapidly and efficiently.

Included in the Resilience Framework are the following key plans of Event Command Organisation (ECO) Manual:

Crisis Management

- Crisis Management Plan[72]
- Communications Plans/ Corporate Affairs Support Plan[73]

Emergency Management (Escalation Management)

- Escalation Plan[74]

---

[70] Business Resilience Framework - JEQA4UJ443MT-154-402

[71] Event Command Organisation Manual-Entire Document - JEQA4UJ443MT-154-383

[72] Crisis Management Plan - JEQA4UJ443MT-154-386

[73] ECO Manual Section 8 – Corporate Affairs - JEQA4UJ443MT-154-370

[74] VPN Network Escalation Plan - JEQA4UJ443MT-154-403

- IT Incident Management[75]
- Business Recovery and Facilities Team[76]

Business Continuity

- Business Continuity Plan
- Business Impact Assessments

IT Disaster Recovery

- Disaster Recovery Plan[77]

Infrastructure Security

- Infrastructure Security Plan[78]

.

4.2.2 Health, Safety and Environment Management

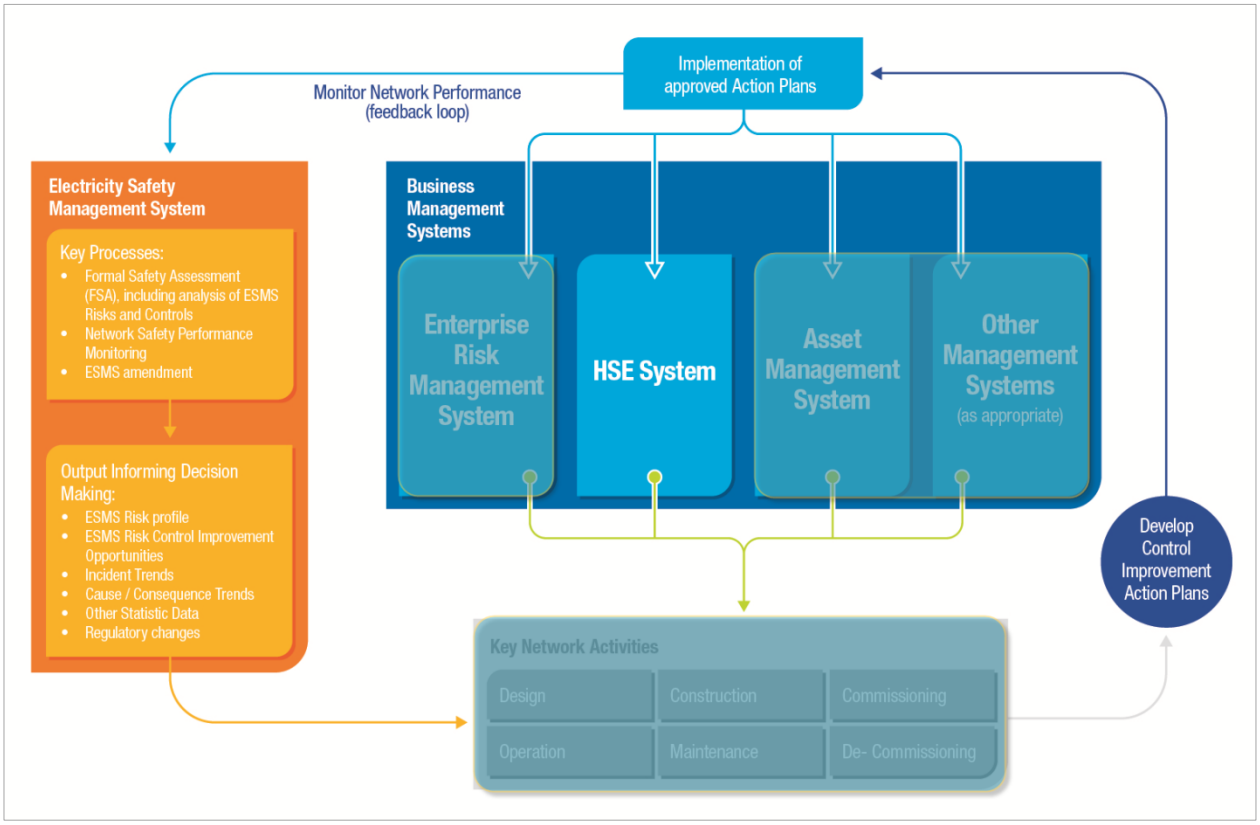


Figure 4-8 – ESMS Integration with Health Safety & Environment System

[75] ECO Manual Section 6 - IT Communications Escalation Team - JEQA4UJ443MT-154-368

[76] ECO Manual Section 7 – Business Recovery Team - JEQA4UJ443MT-154-369

[77] IT Disaster Recovery Policy - JEQA4UJ443MT-155-88

[78] ECO Manual Section 5 - Cyber Security Incident Response Plan - JEQA4UJ443MT-154-359

The purpose of the HSE Management System is to ensure the safety of staff, contractors, members of the public and environment.

The Health, Safety and Environment (HSE) Management System provides a framework by which the processes relating to the company's HSE activities are written, approved, issued, communicated, implemented and controlled. Additionally, the management system is subject to on-going reviews and improvements to ensure objectives and obligations are met.

The HSE Management System is arranged under 12 Elements as shown in Figure 4-9.

Figure 4-9 – HSE Management System

The ESMS interacts with the elements of the HSE system to ensure electrical safety outcomes are achieved. For example, the network performance data associated with third party interactions (No Go Zone infringements, unauthorised entry into substations and copper theft) is integrated with the incident management element of the HSE Management System and monitored at various business levels. This enables strategies to be formed to minimise risks associated with injuries to employees, contractors and third parties working on, or in the vicinity of our network assets.

4.2.2.1 Training and Competency

CP-PAL identify the relevant skills, competencies and where applicable qualifications requirements for a job role. These are documented within each role job description. These

roles include: Engineers, designers, team leaders, managers etc.

In addition, for roles that are required to work on or near the networks, the training requirements are documented in the VESI Skills & Training Matrix and Authorisations.

VESI Skills & Training and Authorisations

All CP-PAL employees and contractors who are working on or near the network are suitably competent and adequately trained in accordance with the ESMS requirements. The training systems provide:

- Application and processing of appointment authorities for persons applying to work on the CP-PAL network, confirming compliance to our training standards.
- Visibility of training status to our field staff via a training App available on the iPhone or iPad.
- The ability to monitor and audit for training compliance.
- Reporting of training compliance status to the business.
- Issue of the Australian ESI Skills Passport to persons working on the network.

CP-PAL sets the training standards for workers who are working on or near the network. The training standards are established through the VESI Skills and Training Reference Committee for consistency within the state, and nationally through the Service Skills Organisation – Australian Industry Standards (formerly the Industry Skills Council, refer https://www.education.gov.au/AISC for more information).

If training is required, specifically for CP-PAL, this is co-ordinated as Enterprise Training for employees. For contractors, additional training would be included in a contract.

Enterprise training is what CP-PAL has determined to be a requirement for a specific job role. This requirement would be for employees only. Examples of Enterprise Training include:

- Leadership
- Computer literacy
- Communication
- HSE

Where it has been identified that training is a business requirement, the requirements is published within company systems, for example, provide first aid is listed within the CP-PAL Health and Safety First Aid Procedure[79].

Audit processes and individual performance reviews are in place to ensure that there is consistent application of knowledge and skill to the standard of performance required.

The Training Framework for the Electricity Supply Industry has many inputs from legislation requirements to national and state industry requirements. For consistency and portability of workers, various bodies (industry and government) set the training standards.

[79] First Aid Procedure Document # JEQA4UJ443MT-185-30727

The Training Framework is shown in Figure 4-10:

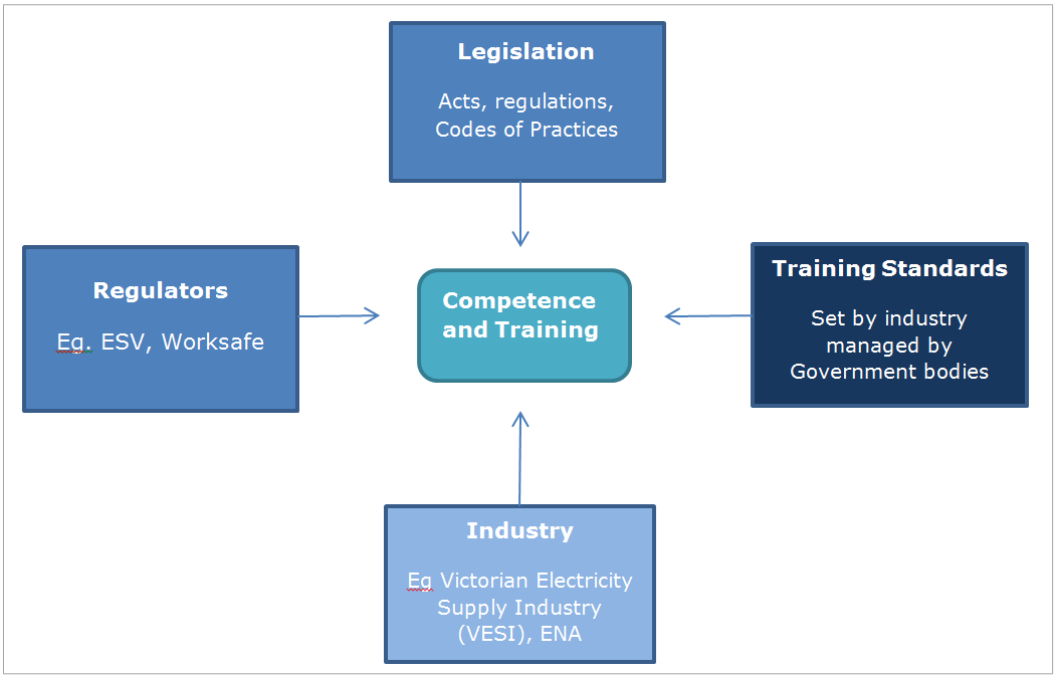


Figure 4-10 – Training Framework

The key steps that CP-PAL have in place to manage competence and training requirements are illustrated in Figure 4-21:

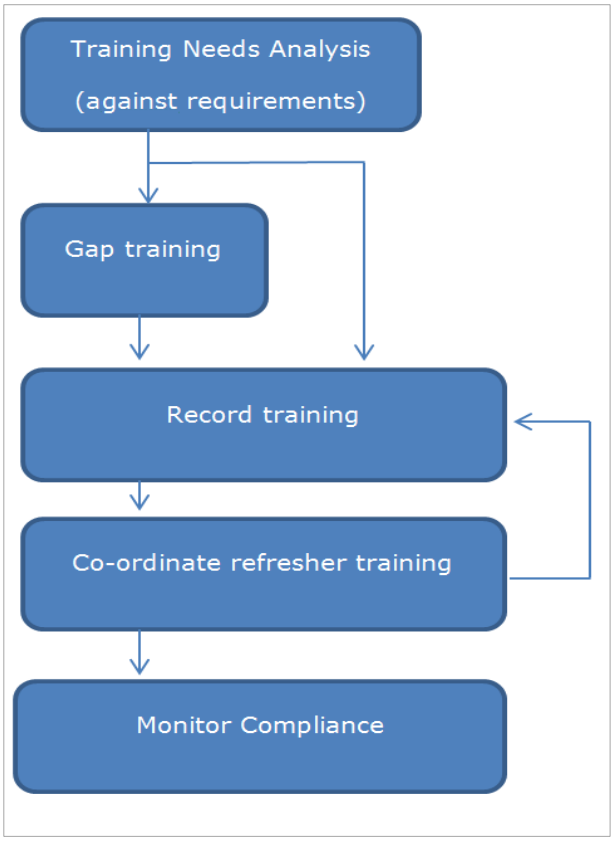


Figure 4–11 – Competency and Training Process

Electricity Networks set the training standards for those working on or near the network.

The process ensures that the training of all workers is sufficient and current. If a worker is found not to be 'competent' or sufficiently trained in their job, further 'gap training' is organised. Failure to complete training to a satisfactory level will prevent the worker from performing the functions associated with that training. The worker and their manager are notified of any expired training. If a worker is not deemed competent, the activity will cease and a suitable development plan will be established to rectify any gaps. The worker may be under supervision through the development period.

CP-PAL have a documented Technical Training Policy[80] and Technical Training Guideline[81], each of which details the mandatory training requirements.

VESI Training

The objective of the VESI Skills & Training Reference Committee is to:

- Provide strategic policy and consistency in the industry for all training and competency related matters.
- Provide common industry tools (journals, guidelines, and training modules) for all relevant industry stakeholders.
- Assure the participating companies are ensuring persons operating or maintaining its network assets have the appropriate qualifications, proficiency and experience to safely perform their duties.
- Establish and maintain the rules and minimum standards for refresher training in the industry.

VESI has established standard training modules and a Skills & Training Matrix, which are agreed upon by all Victorian network operators. All training modules completed are recorded in the Australian ESI Skills Passport.

The VESI Training Modules and Skills & Training Matrix can be found at:

http://www.vesi.com.au/skillsandtraining/skillstraining.aspx

Further details on the VESI Skills and Training Reference Committee can be found at:

http://www.vesi.com.au/SkillsandTraining/SkillsInfoPages/AboutUs.aspx

ESI Worker

CP-PAL implemented the Australian ESI Skills Passport in 2010. This system has enhanced the portability of the ESI workforce by mutual recognition of agreed training standards. Further information can be found at:

www.esipassport.com.au

[80] Technical Training Policy – JEQA4UJ443MT-173-25

[81] Technical Training Guideline – JEQA4UJ443MT-173-28

CP-PAL has implemented the ESI Worker System. ESI Worker System has replaced the Australian ESI Skills paper passport to manage the qualifications and competencies of electricity supply workers in a single online program. This improvement provides CP-PAL to see the current status of all contractor training.

National Training Standards

Qualification standards for personnel accessing the CP-PAL Networks are established in accordance with the Australian Qualifications Framework (AQF).

The AQF was first introduced in 1995 to underpin the national system of qualifications in Australia, encompassing higher education, vocational education and schools. The AQF is an integrated policy that comprises:

- The learning outcomes for each AQF level and qualification type.
- The specifications for the application of the AQF in the accreditation and development of qualifications.
- The policy requirements for issuing AQF qualifications.
- The policy requirements for qualification linkages and student pathways.
- The policy requirements for the registers of:-
  - organisations authorised to accredit AQF qualifications
  - organisations authorised to issue AQF qualifications
- AQF qualifications and qualification pathways.
- The policy requirements for the addition or removal of qualifications in the AQF.
- The definitions of the terminology used in the policy.

Each qualification in the AQF is made up of units of competency. Each unit identifies a discrete workplace requirement and the relevant knowledge, skills, language, literacy, numeracy and OH&S requirements to be deemed competent. These are utilised once qualified to assure competency in a specific skill, e.g. Live HV work and/or HV Operating.

The AQF requirements for CP-PAL and the Electricity Supply Industry are administered by the current government appointed Industry Skills Council (ISC). Registered Training Organisation (RTO) are engaged to deliver the AQF training requirements. RTOs can be validated via www.training.gov.au website which includes verifying the scope of training which can be delivered and validity period for the scope of training.

Individual Training Needs Analysis

Network Safety assures that the training of new workers working on or near the network, is reviewed prior to commencing work and upon a change of role. The training records are checked and any gaps provided to the Technical Training Team, who arrange the training for employees. If a contractor is found with training gaps, the employer is advised and suitable training arranged.

Gap Training

Where gaps are identified against the job role and a person's skills, training is delivered by a Training Provider that meets the requirements of Section 7 of the VESI Skills and Training Guideline[82]. Activities are identified and planned in accordance with the Initiate Technical Training procedure[83] for employees. Contractors are required to complete training requirements before commencing work on the networks.

The VESI Skills & Training Guideline and Matrix outlines the minimum Qualification and Competency Assessment / Refresher Training requirements for VESI workers working on or near Distribution & Transmission Networks in Victoria. Training requirements will be referenced back to this matrix to identify and determine training gaps against individuals' job roles.

Authorities

This procedure describes the authority categories and functional restrictions placed upon CP-PAL employees and contractors who work on, near or in the vicinity of CP-PAL sub-transmission and distribution networks.

In order to work on, near or in the vicinity of the CP-PAL sub-transmission or distribution networks, all CP-PAL employees and contractors shall be current Authority Holders or under supervision while in training for the activity being performed.

Authorities are issued with functional and geographic restrictions, which describe the scope and location of the Authority.

Authority Holders do not conduct functions outside their scope and geographical restriction.

Switching and Access Authorities are supported by refresher training as stipulated by the VESI Skills and Training Guideline.

CP-PAL internal authorities are refreshed on a three-yearly basis.

A Request for Authorisation[84] is completed and submitted to the Technical Training Section for processing.

Switching and associated duties on the CP-PAL High Voltage and LV CBD Network are performed by Authorised Electrical Operators whose training, duties and instructions cover the particular electrical apparatus to be switched.

Induction [85]

[82] VESI - Skills and Training Guideline http://www.vesi.com.au/files/SkillsandTraining/Training_Guideline_Matrix/VESI_Skills_and_Training_Guideline_V8_May_2017.pdf

[83] Initiate Technical Training Procedure Document # 11-25-P0006

[84] Access to Network Form - JEQA4UJ443MT-149-242

[85] Induction Procedure Document - 11-07-P0001

All employees and contractors undertake CP-PAL induction upon commencement of employment. The induction covers the company safety messages as well as company processes and procedures. Where required project specific induction is undertaken to address site requirements.

Performance Management

Employee performance is managed in accordance with Manage Employee Performance Policy[86].

An employee's line manager in consultation with People and Culture, manage employee's performance, which includes any training and competencies to undertake their role. Performance reviews are undertaken every six months where the line manager in consultation with employees assesses performance, including competence.

To support the performance management process, CP-PAL has eight critical safety rules that apply to all employees. These rules are referred as the Never Compromise Safety Rules[87]. To make sure everyone is treated fairly and consistently, we have developed a fair and just process[88] that enables us to apply our existing disciplinary procedure.

[86] Manage Employee Performance Policy - 11-25-CP0001

[87] Never Compromise Safety Rules

[88] Fair and Just Process - NCSR Decision Chart

4.2.2.2 Operational Delivery - Works Practices

Works practices are managed under the operational delivery element of the CP-PAL HSE system. The intent of this element is to ensure that all works that have the potential to cause harm to the health and safety of employees or civilians, the environment, or to cause damage to equipment, are carried out in accordance with plans and documented procedures, so as to ensure safe working environment and practices at all times.

CP-PAL's operational HSE improvement division develops and maintains the Standard Work Practices (SWP) relevant to all major and high risk activities, including construction, commissioning, operations, maintenance and decommissioning.

SWPs provide the worker with the following information:

- Known task related warnings and precautions
- Known task related tools and equipment required
- Task description (Pre Planning, Job Safety Assessment, Work Method action steps)

SWPs are readily available to employees and contractors via the Source Works Practice portal.

CP-PAL has Work Practice Observation programs[89] to ensure that SWPs are understood and correctly followed.

Extracts of the Source Works Practices portal are provided as follows:

Works Practice Document Portal

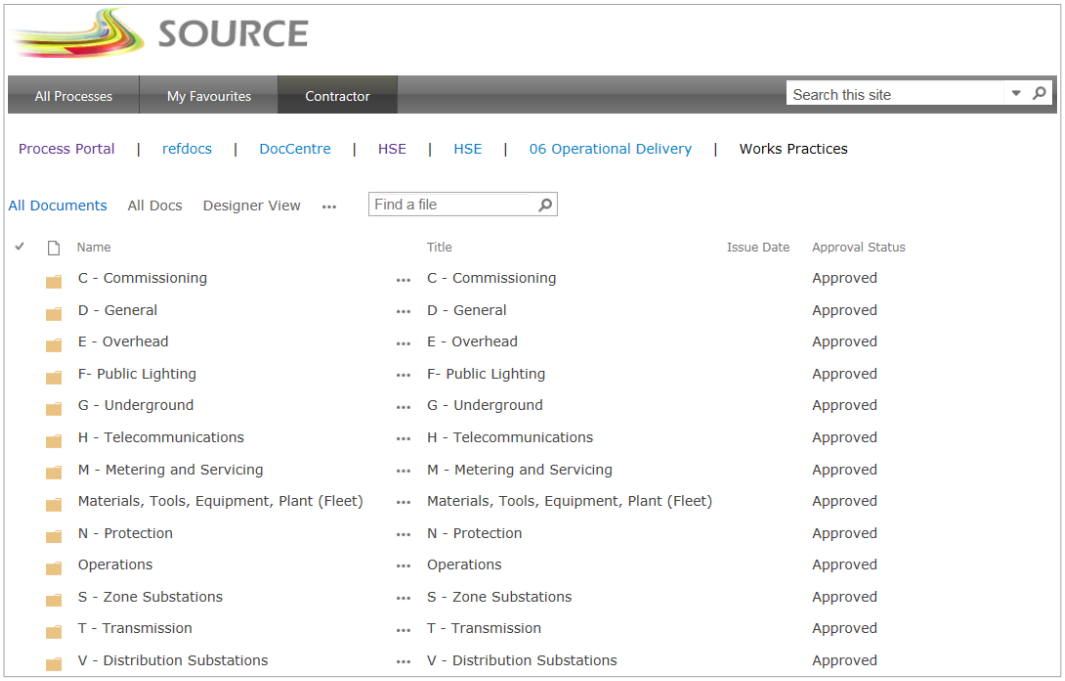


Figure 4-12 – Works Practices Document Portal

[89] Works Practice Observation Program - JEQA4UJ443MT-185-23849

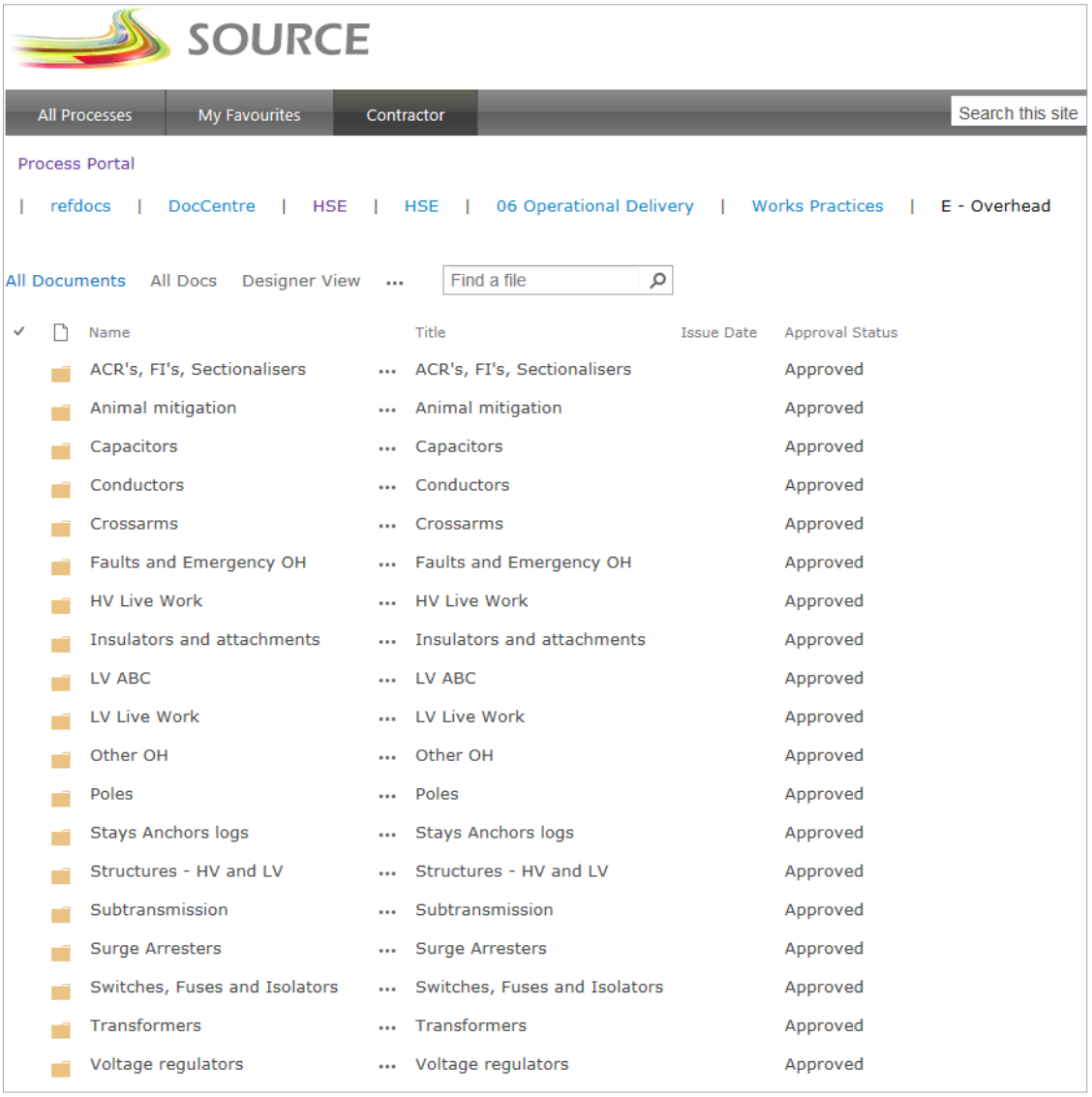


Figure 4-13 – Works Practices Overhead Document Portal

4.2.3 Asset Management System

Asset management is completed with respect to (and with input from) each of the following Electricity Network Divisions:

- Asset Management
- Network Planning and Development
- Network Compliance – Bushfire Mitigation, Network Safety, Vegetation Management
- Network Control and Operations
- Network Technologies

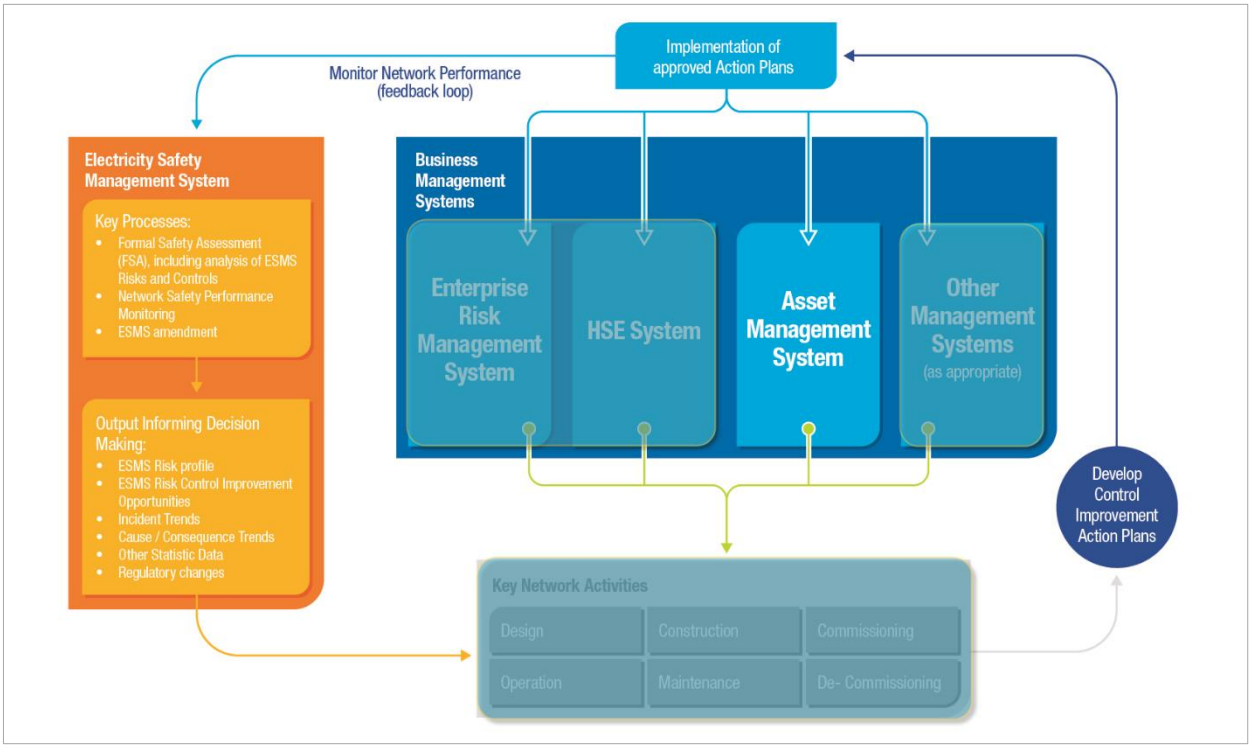


Figure 4-14 – ESMS Integration with Asset Management System

4.2.3.1 Asset Management Commitments

The commitment policies as discussed in *Section 2 Policy and Commitment* enable CP-PAL to achieve the asset management commitments by adopting the following principles:

- Minimise safety risks as far as practicable.
- Enhance our reputation as a trusted service provider through active industry leadership and the delivery of safe and reliable services that meet the needs and expectations of our customers and communities.
- Focus on maintaining a safe, affordable (least long term cost) and reliable network when devising our plans for the development of our network.
- Adopt a risk based approach to managing our network.
- Invest in programs that optimise total lifecycle management.

- Comply with as a minimum all relevant legislative and regulatory requirements as well as Australian, international and industry standards and any other requirements to which CitiPower and Powercor subscribes.
- Develop high performance operations by engaging with our employees and ensuring that they have the right skills and capabilities.
- Embrace innovation and technology to continuously improve our asset management framework and activities consistent with recognised asset management standards for the long term benefit of our employees, shareholders, customers and other stakeholders.
- Monitor and evaluate appropriate metrics to effectively manage the network and customer service performance.

These principles are discussed in greater detail in sections 4.2.3.2 – 4.3.

CP-PAL is continuing to develop and implement an asset management system that is aligned with the requirements of ISO 55000 via the ISO 55000 alignment initiative.

The Asset Management System (AMS) Framework describes the asset management system that CP-PAL applies to its network assets. The AMS Framework identifies CP-PAL's asset management roles, accountabilities and all significant steps and processes involved in the asset life cycle, from the identification of need to creation, operation, maintenance and eventual disposal.

4.2.3.2 Asset Management Process

Figure 4-15 demonstrates the Asset Management Process adopted by CP-PAL, illustrating all significant steps throughout the life of a network asset.

The Asset Management Framework consists of five key levels:

- Level 1: Stakeholder needs and governance
- Level 2: Strategic asset management
- Level 3: Asset management planning
- Level 4: Asset management delivery
- Level 5: Performance monitoring and review

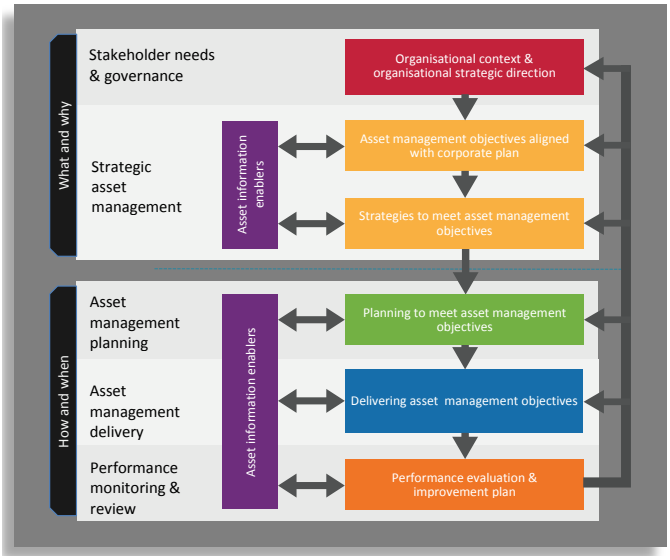


Figure 4-15- CP-PAL's Asset Management System Framework

Levels 1 and 2 describe 'What' asset management strategies and objectives are to be targeted and provide details regarding 'Why' these are required. Level 3 describes the approach taken to plan and budget for the delivery of the asset management activities, while level 4 describes 'how' and 'when' these activities are delivered to meet the strategies and objectives. Level 5 describes CP-PAL approach to performance monitoring and review of the asset management system.

An overview of documents to realise the following elements of Asset Management System (AMS) Framework is provided in sections 4.2.3.3 - 4.2.3.6.

- Strategic asset management
- Asset management planning
- Asset management delivery
- Performance monitoring & review

4.2.3.3 Strategic Asset Management

CP-PAL's asset management strategies and objectives are aligned to the asset management policy and to the needs of our stakeholders, including the direction articulated in our organisational strategic pillars and the asset management-related commitments made in our approved regulatory submission.

The strategic asset management level of CP-PAL's AMS framework comprises the following key components:

- Asset management objectives
- Asset management policy
- Strategic Asset Management Plan (SAMP)
- Asset management strategies
- Asset class strategies

Asset Management Objectives

CP-PAL's asset management objectives form the basis for evaluating the success of the asset management system in delivering against the organisational strategic pillars.

The asset management objectives for CP-PAL are:

- Meet our network reliability performance targets
- Manage our assets on a total life cycle basis at least cost
- Manage our compliance obligations
- Empower and invest in our employees
- Monitor opportunities and drive continuous improvement

The AMS Framework maps the asset management policy principles and asset management objectives to demonstrate the alignment to the organisational strategic pillars.

Asset Management Policy

CP-PAL's Asset Management (AM) Policy drives all asset management activities in our organisation. The AM Policy is a high-level statement providing:

- Our overall approach to asset management;
- The principles to be followed, and direction for establishing asset management strategies and objectives; and
- Management expectations regarding asset management outcomes.

The AM Policy requires asset management activities to meet business objectives and benefit the current and future needs of all customers, stakeholders and employees.

Strategic Asset Management Plan

CP-PAL's strategic asset management plan (SAMP) identifies our high-level strategies and objectives for asset management, and links these to the 'five pillars', providing line of sight to the organisational strategy. The SAMP takes full account of our approaches to network risk and asset investment decision making and provides long-term guidance for the development of the asset management strategies and class strategies.

Asset Management Strategies

Asset management strategies have been developed for twelve subject areas to deliver CP-PAL's SAMP objectives. The Asset Management Strategy subjects are not asset specific and apply across all asset classes. Individual subject strategies are developed by considering:

- The CP-PAL organisational context and key asset management issues of a range of internal stakeholders; and
- The asset management requirements of a range of external stakeholders which may include the AER, AEMO and CFA.

The asset management strategies provide guidance for development of asset operational plans and asset management plans, to prioritise and deliver the asset management objectives and

strategies. Refer to Appendix 17 for a detailed list of asset management strategy subjects and purpose of each strategy.

Asset Class Strategies

CP-PAL has identified sixteen asset class strategies (ACS) for which specific strategies and objectives have been developed, all of which are aligned to the SAMP. Each ACS is formed from analysis of the required performance in terms of reliability and quality of supply, risk profile, functionality, availability and safety. The ACSs provide guidance for development of asset operational plans and asset management plans, which drive inspection, maintenance, condition monitoring, maintenance policies and work instructions. Refer Appendix 17 for a detailed list of ACS documents and corresponding asset coverage.

4.2.3.4 Asset Management Planning

CP-PAL plans their asset management activities to maximise the value realised over the life of its assets. The asset management planning stream of CP-PAL's AM Framework is undergoing further development, with key focusses on asset investment planning, asset maintenance requirements and optimising the asset lifecycle.

CP-PAL has implemented a new value framework that will form the basis for quantitatively prioritising investments. The value framework is being used to configure the Copperleaf C55 asset planning and investment tool to facilitate the quantitative prioritisation of investments going forward. The value framework will be used for the first time informing our 2020 budget and 5 year financial plan.

4.2.3.5 Asset management delivery

CP-PAL's asset management delivery and governance is facilitated via existing standards, policy, procedures and processes that stipulate the requirements for our asset management delivery. Monitoring of compliance is achieved via regular internal audit processes and reporting. CP-PAL's Strategic Asset Management (SAM) committee provides specific oversight and governance to the Asset Management System.

4.2.3.6 Performance monitoring and review

CP-PAL monitors the performance of both network assets and the asset management system as a whole. The components of CP-PAL's performance monitoring and review level of the AMS framework are outlined below:

- Risk assessment and management
- Business continuity planning
- Change management
- Asset performance and health monitoring
- Asset management monitoring and continual improvement

- Audit and assurance
- Stakeholder engagement

Considerable capital investment has been made to configure the network to provide real-time asset performance data that is used to develop a range of high and lower level performance indicators, including those that are required to be reported under the terms of our distribution licence. Additionally, CP-PAL conducts a range of internal and external reviews of the network and asset management system performance through internal audits, external audits and via regular management reviews. Where improvements to the AMS framework are required, these are consolidated into an AMS framework improvement plan.

SAM committee also monitors and governs AMS framework.

AMS framework is further complimented by Asset Maintenance. Refer section 4.3.4 of this ESMS.

4.2.3.7 Network Planning and Development

Network Planning and Development Group mitigates the risk of supply interruptions to the customer and, if supply is interrupted, plans for alternative supply routes. The group provides guidance for the future planning of our networks, developing guidelines to allow augmentation of the network and providing it with capacity to cope with new and existing load and generation changes. It provides the standard requirements that need to be considered for network security, reliability, technical standards, costing, community benefit and compliance within the rules and guidelines from regulators.

i. Network Planning Commitments

The commitment policies as discussed in *Section 2 Policy and Commitment* enable CP-PAL to establish network planning and development key commitments as listed below.

- CP-PAL shall ensure that our network continues to serve the energy needs of the communities we operate in.
- CP-PAL shall comply with the applicable Distribution License and NER (National Electricity Rules) obligations.

The above mentioned commitments are discussed below to demonstrate how these commitments are met.

ii. Network Planning and Development Process Overview

Network Planning interacts with various sectors of the business. Network Planning establishes and develops planning requirements from the following key inputs:

- Legislative requirements
- Electricity industry act
- Electricity distribution code
- National electricity rule
- Essential services commission guidelines

- Distribution license

Network Planning also supplies direction to other sectors of the business such as Design, Asset Management, Operations and Network Services projects. Figure 4-16 below illustrates the overview of Network Planning and Development.

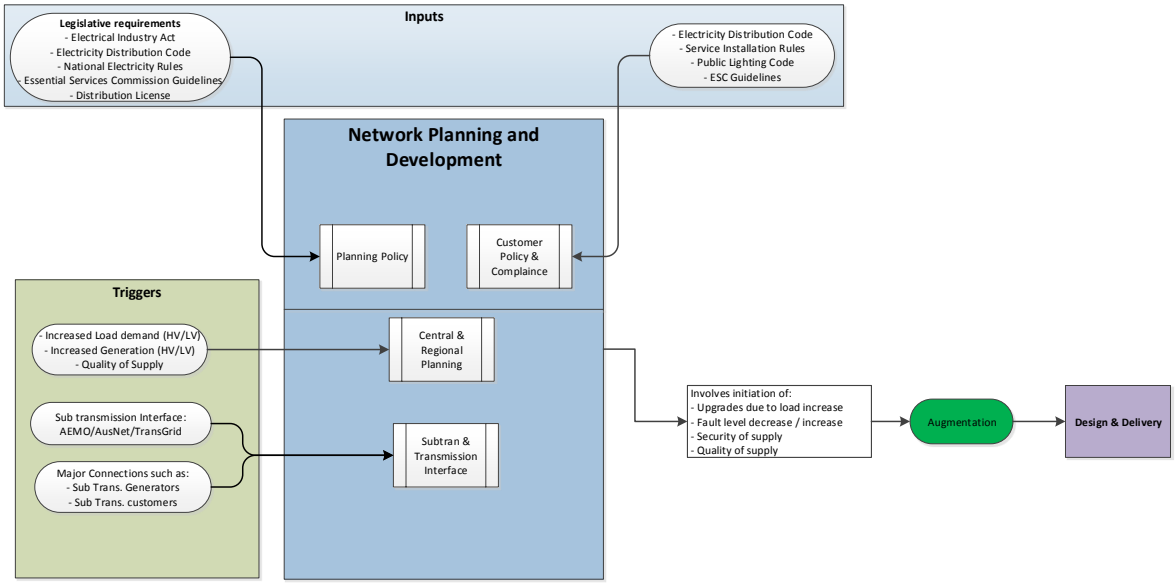


Figure 4-16 – Network Planning and Development Overview

Network Planning and Development as a whole provides policy and guidelines[90] to form a framework for a consistent and considered approach in the development of the CP-PAL network.

This approach takes into consideration the following factors:

- Ensuring network safety
- Maintaining security and reliability of supply
- Setting standards for the operation of the network
- Promoting the re-evaluation of existing principles and proposing improvements
- Promoting standardisation of augmentation design
- Promoting a whole of business approach to the planning and evolution of the network
- Ensuring non-network solutions are considered equally with network augmentations

Network Planning and Development Group establishes the policies for the following:

Network Planning and Policy manages Distribution System Augmentation Planning Policy and Guidelines[91] . These policy and guidelines provide technical oversight of the development of policy and guidelines for the augmentation of the network assets. This

[90] Distribution System Augmentation Planning Policy and Guidelines – JEQA4UJ443MT-150-453

[91] Distribution System Augmentation Planning Policy and Guidelines – JEQA4UJ443MT-150-453

includes terminal station connection assets, sub-transmission lines, zone substations, distribution substations and compliance with the National Electricity Rules and relevant government codes.

- **Customer Policy and Compliance**[92] responsible for the development, review and implementation of Network Connections policies that also provide adherence to regulatory and electrical safety guidelines.

  Connection only proceeds if a Certificate of Electrical Safety has been received. Connection workers complete Connection Standards Compliance Certification CSCC form. Audits of completed connections are undertaken. Complex connections are scoped by Connections Technical Advisors.

  Connections Key guidelines, work instructions, rules, procedures are described in these documents:

  - Connection Worker Manual[93]
  - Green Book[94]
  - Line Worker Handbook[95]
  - Distribution Code[96]
  - Metering Operations Group Reference Manual[97]
  - Service and Installation Rules[98]
  - VESI test procedures[99]
  - Connection Workers Manual[100]
  - LV Planning Requirements[101]

Network Planning and Development provides the business with expertise and guidance via the following main areas:

- **Central Planning** is responsible for managing the development of the distribution network, up to and including zone substations, within the central area of CP-PAL in compliance with the National Electricity Rules and other codes, maintaining all safety requirements.
  Central Planning is also responsible for the scope of all customer connection work and determining network solutions to customer complaints and non-compliances with codes.

[92] Network Customer Policy Manual - JEQA4UJ443MT-160-227
[93] Connection Worker Manual – JEQA4UJ443MT-185-10287
[94] VESI Green Book
[95] VESI Fieldworker Handbook
[96] Electricity Distribution Code (Version 9)
[97] Metering Operations Group Reference Manual – 05-20-M0012
[98] Victorian Service & Installation Rules - 2014
[99] VESI Installation Connection Manual - 2017
[100] Connection Workers Manual – JEQA4UJ443MT-185-10287
[101] LV Planning Requirements - 01-10-CP0001

Central Planning evaluates non-network options and connection of generation to the grid.

- **Regional Planning** is responsible for managing the development of the distribution network, up to and including zone substations, within the Regional Area of Powercor in compliance with the National Electricity Rules and other codes, maintaining all safety requirements.
  Regional Planning is also responsible for the scope of all customer connection work and determining network solutions to customer complaints and non-compliances with codes.

  Regional Planning evaluates non-network options and connection of generation to the grid.

- **Sub-transmission and Transmission (including Load Growth Forecasting) Interface** is responsible for the planning and development of the CP-PAL sub-transmission network, including sub-transmission load or generation connections, in compliance with the National Electricity Rules (NERs) and other codes.
  Provides a planning and contractual interface between CP-PAL and relevant Transmission Network Service Providers (AusNet Services and others) and AEMO.

Network planning documents Library

These documents are located in our digital document library (**My Connect)** as represented by the Figure 4-17 below.

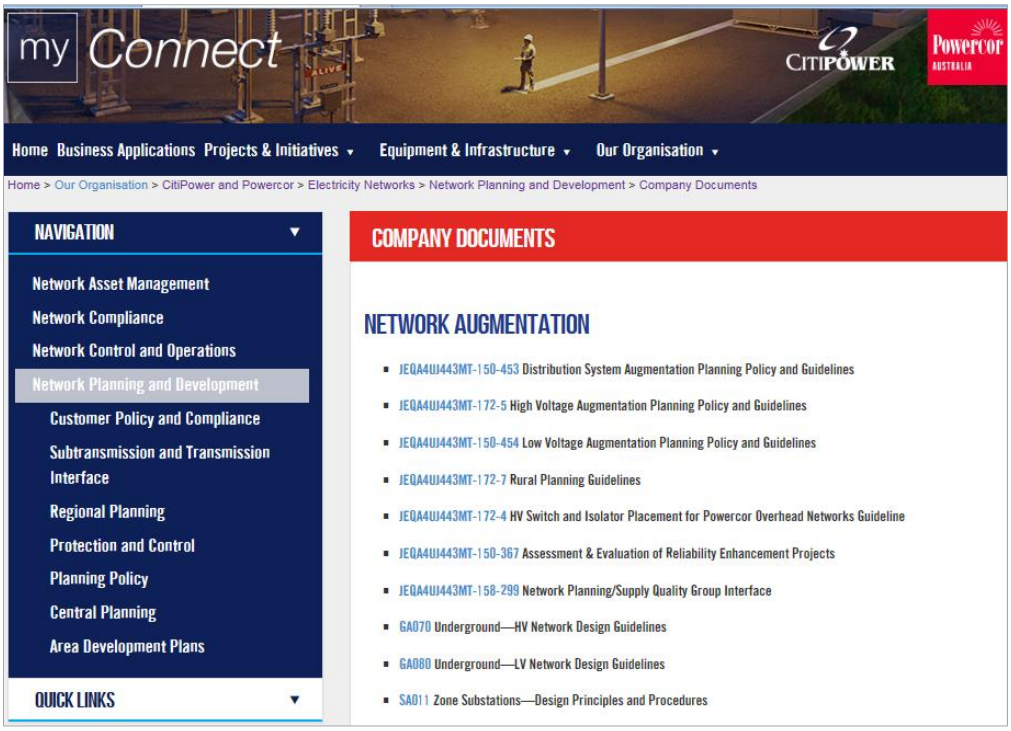


Figure 4-17 – Network Planning and Development Documents

The above codes and rules are regularly updated and often distribute guidelines as well. Network Planning and Development is therefore required to conduct regular planning reviews to update

internal documents with the changing requirements. Planning for future augmentations involves major steps in the business process. This step process is referred to as **The Planning Cycle**[104].

The planning cycle incorporates 10-year terminal station load forecasts using terminal station summer and winter demands and projecting forward based on expected growth rates. This takes into account a range of factors including past growth, economic outlook and future area developments and trends.

The determination of feeder and zone substation load forecasts utilises historical feeder and zone substation demands to project forward based on expected growth rates, known new loads and developments and then adjusting to meet the externally provided and economically driven terminal station forecasts. This is referred to as a 'top down-bottom up' approach and aims to produce more informed and accurate forecasts using both external and internal knowledge.

Terminal station connection and Distribution Asset Augmentation plans are published annually in the TCPR and Distribution Annual Planning Report (DAPR) respectively. Changes to terminal station connection asset bus voltage settings, system arrangements and ties between terminal stations that affect fault levels or sub-transmission loop changes that affect load-shedding plans are communicated annually to AEMO.

The preparation and amendment of 10-year plans for terminal station connection assets, zone substations and feeder line works augmentation and related documentation are undertaken each year. A planning strategy is developed for each major asset groups for example, zone substation, overhead lines (sub-transmission feeders). Planned yearly augmentation work is prioritised per the Financial Planning & Approval process. Refer section 4.2.4.2

Changes to terminal station connection asset bus voltage settings, system arrangements and ties between terminal stations are communicated annually to AEMO. Such changes can have an effect on fault levels and the transmission system line flows.

Terminal Station Connection Assets are jointly planned with AusNet, Transgrid and the Distribution Network Service Providers (Distribution Businesses) that are supplied from the connection assets. AusNet and Transgrid are the Transmission Network Service Providers that own and maintain the assets. Connection assets that supply more than one Distribution Business are jointly planned.

4.2.3.8 Vegetation Management

Vegetation poses a fire and reliability risk if it makes contact with our lines. Hence, vegetation management is a critical control in managing risks of fire ignition (catastrophic bushfire), electric shock/injury and interruption of supply.

[104] Refer to section 2.4 of the Distribution System Augmentation Planning Policy and Guidelines – JEQA4UJ443MT-150-453

Electric Line Clearance (Vegetation) Management Plan

Our Electric Line Clearance Management (Vegetation) Plan (ELCMP)[105] describes how we comply with the legislative requirements of the Electricity Safety (Electric Line Clearance) Regulations 2015, and how we deliver vegetation clearance safety outcomes.

CP-PAL has a Vegetation Management Strategy, which is summarised and detailed within the ELCMP.

CP-PAL has range of vegetation management procedures[107]that help our staff and contractors to achieve the vegetation management objectives, particularly for inspection and cutting works.

Vegetation Management System

Our Vegetation Management System (VMS) is structured set of data to manage vegetation for compliance to the Electricity Safety (Electric Line Clearance) Regulations and corporate strategy.

A combination of the GIS, SAP and VMS data is used to facilitate management of the vegetation program. GIS maintains the key network spatial information, including HBRA and LBRA areas, and the declared area and non-declared area status. SAP is used to program and report the inspection and cutting activity status. VMS is the mechanism used to capture the field delivery aspects of the inspection and cutting program. Spans issued for cutting provide the field crews with access to the span details: HBRA/LBRA area, declared/non-declared area, voltage, pole ID and location. A screen shot of the VMS data is shown in Figure 4-18 below.

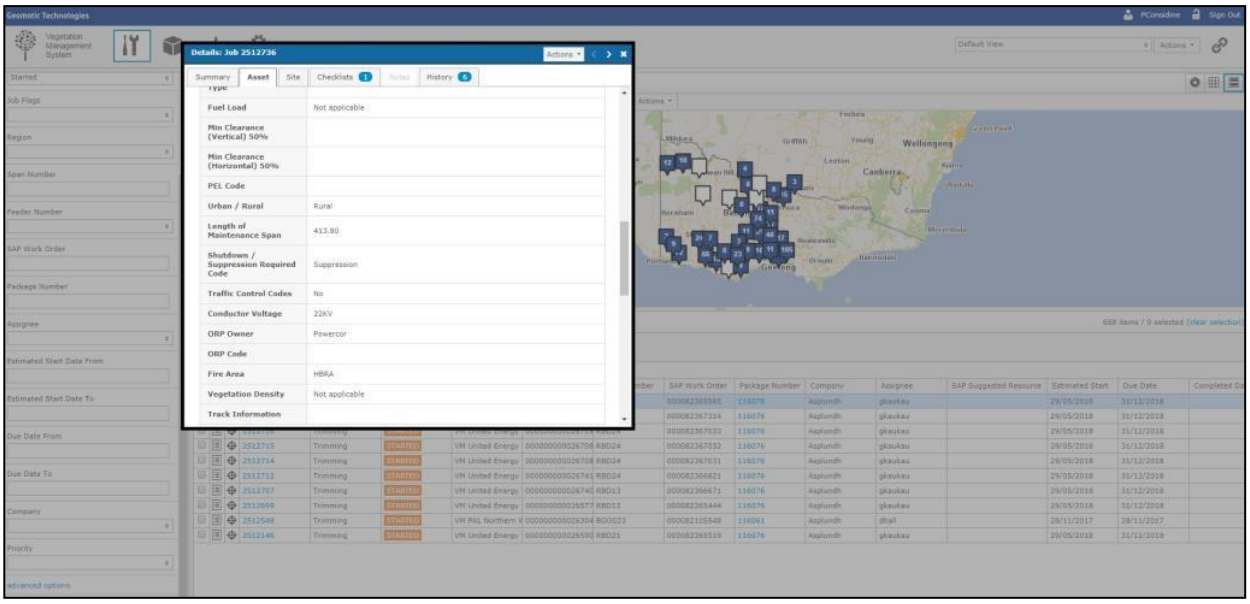


Figure 4-18 – Screenshot of VMS data

[105] Electric Line Clearance (Vegetation) Management Plan - JEQA4UJ443MT-150-27661

[107] Electric Line Clearance (Vegetation) Management Plan, Reference J - JEQA4UJ443MT-150-27661

We are responsible for vegetation management around overhead lines and other electricity assets in our network. In a Declared Area the municipal council is responsible for compliance with Electricity Safety (Electric Line Clearance) Regulations for trees situated on public land managed by that Council.

We liaise with municipal councils to provide assistance and advice to ensure they understand their responsibilities and obligations, as defined in the relevant legislation. Vegetation identified as a safety or reliability risk to our networks is reported to the responsible authority for action.

Vegetation Inspection Program

CP-PAL undertakes a vegetation inspection program, which is detailed within the ELCMP.

All spans, both HBRA and LBRA are automatically included for inspection in each year's inspection program.

Vegetation Management Performance Monitoring, and Auditing

ELCMP performance is assessed using leading indicators to provide advance visibility of the vegetation exposure level and lagging indicators to provide visibility of vegetation caused impacts. The vegetation management procedure[111] and vegetation reporting[112] provide additional detail.

Vegetation Management Program Governance

Vegetation management program governance has been established to assure compliance with legislation:

- Monthly Fire Prevention Committee meetings and quarterly Integrated Network Management System governance committee meetings provide governance over the efficacy of the approved Electric Line Clearance Management Plan. Regular committee reports/minutes are prepared for senior management, and the board.
- CEO and governance committee briefings regarding vegetation management activities, fortnightly at a minimum,
- Monthly reporting to Senior Management on the progress of the inspection and cutting programs and the implementation of the approved Electric Line Clearance Management Plan
- Weekly monitoring and reporting to the General Manager Service Delivery and weekly reporting to ESV (during the fire danger period) on the progress of the inspection and cutting programs
- Exception reporting through SAP for HBRA and LBRA to generate alerts of spans coming due and as a review of the data quality
- Weekly field audits, and reports to confirm quality of inspection and cutting and the degree of compliance
- Operational unit pre-summer vegetation inspections.

[111] 2019-2020 Electric Line Clearance (Vegetation) Management Procedure, Chapter 4 Vegetation Contractor Compliance and Quality Assurance

[112] Chapter 7 Vegetation Reporting

- Annual ESV, and third party audits to ensure our processes are achieving the desired results in the field
- Contractor safety and work practice audits of as part of the accepted Electricity Safety Management Schemes.

To ensure systemic compliance is maintained during the declaration period the following additional measures are undertaken:

- Pre-summer audits of the HBRA networks will be carried out before the declaration date using staff, sub-contractors or as part of the line condition observation program to confirm asset and vegetation readiness
- Inspection of at least 1% of the HBRA spans will be completed by internal Engagement and Quality Team staff
- Reporting and investigation into key vegetation incidents and faults, especially significant fires, to determine the root cause

4.2.3.9 Bushfire Mitigation

The climatic conditions in some parts of our network are highly favourable for fire ignitions and bushfire, especially during the hot and windy bushfire season (from November to March). On average, our networks experience 13 Total Fire Ban days each year. Bushfire is a big risk to the community and to our PAL network and so we take our responsibilities very seriously to minimise these hazards and risk AFAP.

We operate a Bushfire Mitigation Strategy Plan 2019-2024[116] to comply with the statutory requirements of Electricity Safety (Bushfire Mitigation) Regulations 2013.

The *Bushfire Mitigation Strategy Plan 2014-2019* specifies how Powercor complies with the amended Electricity Safety (Bushfire Mitigation) Regulations 2013, of 1 May 2016, specifically the obligations regarding:

- Rapid Earth Fault Current Limiters (REFCLs)
- Single Wire Earth Return (SWER) Automatic Circuit Reclosers (ACRs) including deployment of fuse savers
- Electric line construction areas

Our approach to bushfire mitigation is multifacited and across the entire business. Figure 4-19 below summarises the key parts and controls of our bushfire mitigation framework.

[116] Bushfire Mitigation Plan – Powercor 05-M810, Revision 5: CitiPower 05-M800, Revision 5

Figure 4-19 – Bushfire Mitigation Framework summary

The objectives of the Bushfire Mitigation Plans are to:

- Minimise the risk of fire starts from electrical assets.
- Achieve compliance with the relevant legislative and regulatory requirements while providing flexibility within the business to encourage innovation, continuous improvement and the effective use of resources.
- Define the companies approach to the management of the risk of bushfires caused by electricity assets.
- Reference the policies and procedures relating to bushfire mitigation activities into one document.
- Demonstrate a high level of commitment to meeting bushfire mitigation responsibilities.

Refer to the CP-PAL Bushfire Mitigation Plans for details of processes and procedures regarding the management of bushfire mitigation.

4.2.4 Other Management Systems

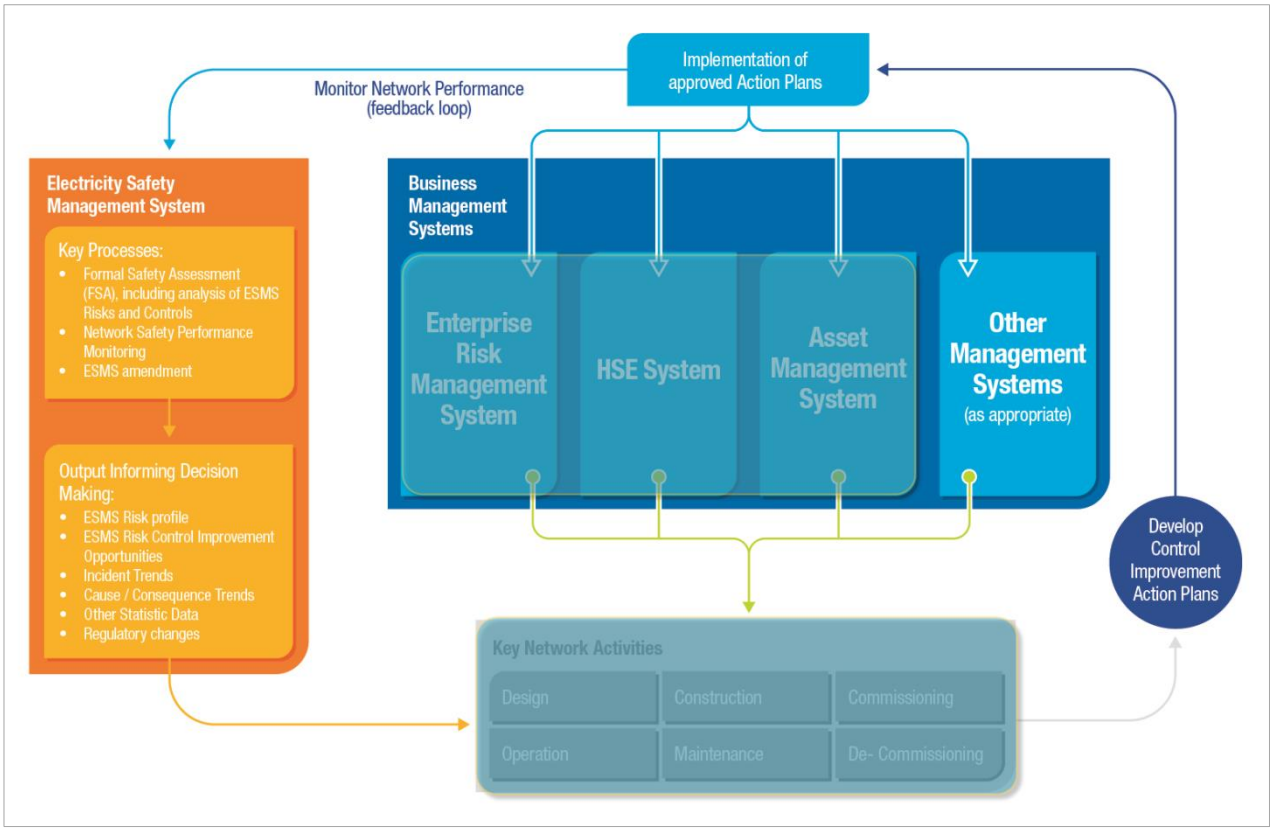


Figure 4-20 – ESMS Integration with Other Management Systems

Outputs of the ESMS are integrated with other business management systems to identify improvement actions to ensure all network safety objectives are fulfilled. These management systems are further discussed in the following sections.

4.2.4.1 Responsibilities, Accountabilities and Authorities

Governance over network safety is achieved through monitoring and reporting of compliance and performance to senior management on an annual basis, and to the Board via the Risk Management and Compliance committee. Exceptions to the performance of assets are governed through the Asset Failure Committee and escalated through the business organisational structure as relevant to each portfolio.

Table 4-1 demonstrates the responsibilities and accountabilities regarding asset management practices, relevant to each business unit.

Management Structure

The management structure for the implementation and control of ESMS related activities is shown in Figure 4-21:

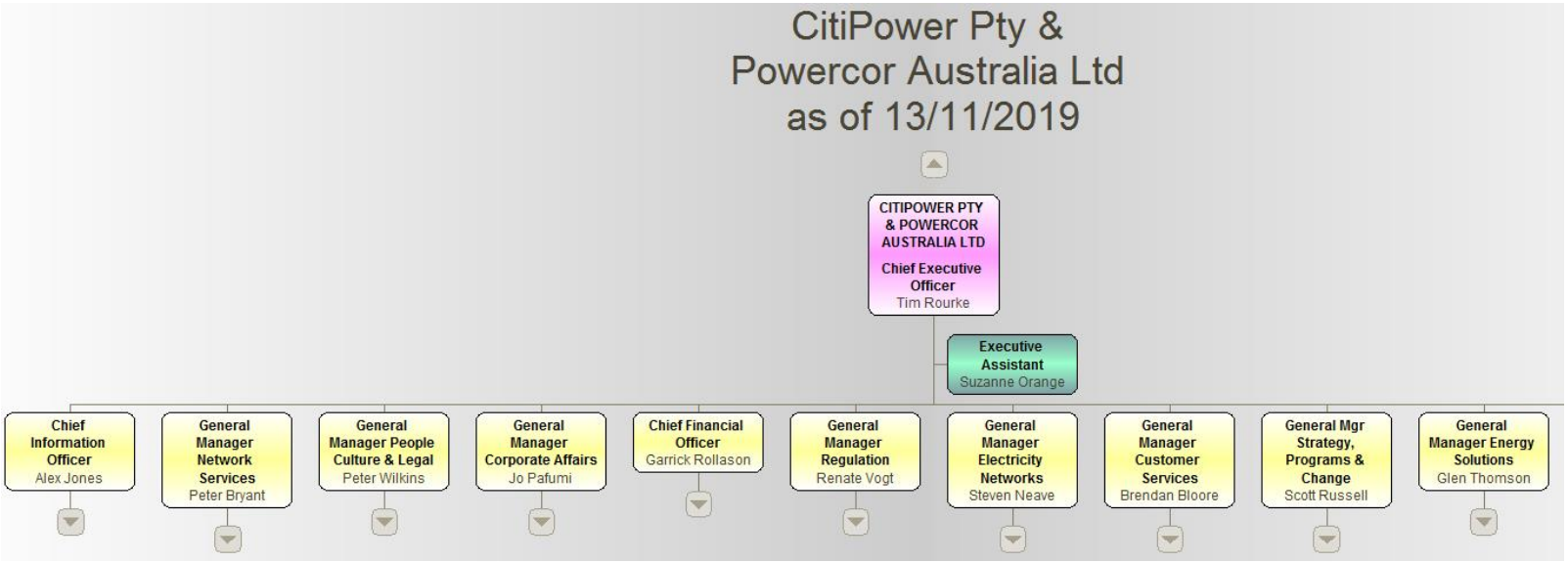


Figure 4-21 – CP-PAL's Management Structure

Business Unit	Responsibility & Accountability associated with ESMS
Electricity Networks	The General Manager, Electricity Networks has the responsibility for the activities associated with planning, design, construction, operation, and maintenance and decommissioning of the network assets. This responsibility includes the development, and management of the policies, processes, standards and instructions applicable to the operation and management of the Network. The Head of Network Compliance has the delegated responsibility for the activities associated with the preparation and submission of the Safety Case, Electricity Safety Management Scheme, Bushfire Mitigation Plans and Electric Line Clearance Plans and the outworking of these through the business. The Electricity Networks Business Unit (BU) is also responsible for the: ► development, implementation, monitoring and review of the ESMS activities including the Formal Safety Assessment outcomes ► control identification and assessment to mitigate the risks as per the business requirements ► technical standards ► operations and maintenance ► access authority ► safety management system policy and procedures for the network
Powercor Network Services	The principal activities of Powercor Network Services Business Unit are: ► design, construction, and maintenance on behalf of Electricity Networks ► 24/7 network fault response and repairs ► overhead and underground power and communications line design, construction and maintenance ► terminal station, zone substation and distribution substation design, construction and maintenance ► project and program Management ► field operating activities, and ► warehouse logistics
Information Technology	The IT Business Unit is responsible for the entire IT platform of hardware, software and telecommunications on which are critical to network operations.
Finance	Finance business unit is led by the Chief Financial Officer and is responsible for: ► corporate risk management ► real estate management ► procurement of plant, equipment and material for the network ► financial control ► business performance management
People & Culture & Legal	This business unit is responsible for providing a range of support services which includes: ► organisational legal services ► organisational change, industrial relations ► HR systems, remuneration and benefits ► staff and contractor health and safety

Business Unit	Responsibility & Accountability associated with ESMS
	➢ learning & development
Strategy & Program Delivery	This business unit is responsible for: ➢ monitoring quality assurance ➢ lean and efficient operations ➢ commercial sourcing ➢ program delivery ➢ automated & integrated works management ➢ customer initiated augmentation works ➢ metering contestability
Regulation	This business unit is responsible for: ➢ monitoring regulatory compliance obligations ➢ regulatory strategy & pricing ➢ preparation and submission of the Electricity Distribution Price Review (EDPR),undertaken in consultation with a wide range of internal stakeholders, which is conducted at five year intervals by the Australian Energy Regulator (AER).
Corporate Affairs	Corporate Affairs business unit is responsible for media communications and messaging to the community, which may include information related to widespread outages, impacts due to severe weather events or marketing and community partnership events.
Customer Services	This business unit is responsible for: ➢ management and operation of the 24 hr contact centre, allowing for the necessary interaction with customers and community ➢ customer connection services ➢ revenue management ➢ customer relations and requests

Table 4-1 - Business Units ESMS Responsibilities Description

The authority levels are specified within job descriptions for personnel within each of the management streams.

For the purpose of ESMS Risk Management, a Risk Owner has been assigned to each of the identified ESMS risk scenarios / events. ESMS Risk Owners are generally senior managers directly reporting to the General Manager – Electricity Network.

Similarly, a person with the responsibility of identifying ESMS risk mitigation controls is assigned as ESMS Control Owner who reviews, assesses and implements control improvement actions as required.

When control improvement actions are identified, the relevant ESMS Control Owners are responsible for determining resource requirements (e.g. financial, labour, material and equipment) and establishing work schedules for the associated implementation activities. The

Control Owner is also required to monitor and report work progress to the relevant ESMS Risk Owners and Network Safety, for updating the ESMS Risk Register.

Resource Management

The role of Resource Management is to ensure that there are appropriate levels and capabilities of resources used in the design, construction, operation, maintenance and decommissioning of the network, to achieve a safe and fit for purpose outcome.

Labour Resources

Competency management is done through the implementation of policies such as the Human Resources Policy Manual[117]. This policy stipulates that the person appointed to a vacant position be the most competent and suitable applicant when assessed against defined job-specific requirements, including qualifications, experience and competency.

To ensure that CP-PAL are optimising all labour resources (internal and external), long term planning is undertaken to ensure that a sufficient quantity of labour, with the skills and knowledge required, is available to deliver the required level of network and corporate services[118]. CP-PAL possess a database on employee skills to ensure each project is appropriately resourced and advises contractors of future projects to ensure sufficient supplementary and complementary labour will be available. Long term resource planning mitigates the risk of short-term labour shortages, an important aspect in safe work practices, reducing worker fatigue[119] and ensuring effective project delivery.

The number of internal and external labour resources required is determined by workload volumes, timing and locations, skill and competency requirements, resource availability, peak period workloads and labour rate diversification. For example, during the peak of the safety program in response to the Victorian Bushfires Royal Commission (VBRC), a resource partner was engaged to assist with the rollout of armour rods and vibration dampers in Hazardous Bushfire Risk Areas (HBRA), providing approximately 80 full time personnel. This example demonstrates that the use of resource partners enables CP-PAL to supplement its workforce to implement specific programs of work, without needing to engage more staff on a permanent basis.

Procurement of Equipment and Materials

To ensure safe and sufficient procurement of equipment and material resourcing, the CP-PAL Purchasing and Procurement Policy Manual[120] is followed. This policy assists employees in understanding their responsibility for all purchasing and procurement activities. The policy requires that procurement of new equipment and material is performed in consultation with the Health and Safety and Technical Standards teams, so that appropriate safety and technical

[117] Human Resources Policy Manual - Section 7 – 11-05-M0005

[118] Powercor Australia 2016-2020 Price Reset – Appendix B Labour cost efficiency – April 2015

[119] Fatigue Management Procedure - JEQA4UJ443MT-161-544

[120] Purchasing and Procurement Policy Manual – JEQA4UJ443MT-156-43

standards are included when selecting new suppliers and awarding contracts. The policy also enables required equipment and resourcing to be purchased by individual business units through delegation of a Procurement Authority.

The Procurement group is responsible for compliance to policy and continually improving procurement practices. The group is also responsible for the procurement of 'direct' and 'indirect' goods and services for CP-PAL. Direct goods and services relate to network operations and core business activity such as the purchase of transformers, poles and cross-arms. Indirect goods include IT, stationary and engagement of consultants.

The Procurement group is also responsible for managing issues with materials or equipment defects that have been supplied to CP-PAL. The process of recalling and quarantining materials or equipment defects upon detection is indicated in the Supply Chain Solutions Quality Control Standard Work Instruction[121].

Consultation and Communication

CP-PAL have responsibility to address the safety concerns of many stakeholder groups, including the community, landowners, employees, contractors, other utilities, service providers, emergency services, regulatory authorities and government agencies.

CP-PAL work to ensure effective two-way communication with all stakeholder groups through discussion forums, formal agreements, subject matter expert workshops, regulatory reporting or published policies and procedures.

Employee Consultation and Communication

CP-PAL consult with a wide range of staff across the business, to ensure that appropriately qualified and experienced persons are involved in reviewing network risks and that a diversity of views are considered. The Formal Safety Assessment process serves as an example, where employees (via the appropriate representation) are formally consulted on safety aspects and risk trends concerning the design, construction, commissioning, operation, maintenance and decommissioning of the network. The FSA process is discussed in sections 3.3 and 4.1.

Further ESMS consultation is achieved through committee representations, including the 'Strategic Asset Management Committees ', 'Incident Review Committee' and 'Operations Committee.' These committees provide a forum where incident causes and trends are analysed through consultation with subject matter experts, with any solutions or improvements communicated throughout the group.

The ESMS document provides information as to how CP-PAL meets their network safety regulatory obligations. Employees and contractors have access to the necessary documents and information systems relevant to their network role and activity.

[121] Supply Chain Solutions - Quality Control - Standard Work Instruction – 08-20-W0019

Authorised company-wide communications are utilised to ensure safe performance of the network and compliance with the ESMS. For example, CP-PAL Technical Standards issue update e-mail notifications to communicate changes to technical standards. These notifications provide a listing of updated Technical Standards, an overview of changes made and impacted key stakeholder groups (such as construction, maintenance or design teams). An example is shown in Figure 4-22.

A message from **Steven Neave**
General Manager, Electricity Networks

4 April 2017

The following message is from the Technical Standards Manager….

CitiPower / Powercor Technical Standards Update

Please ensure that this information is passed on to all field employees and contractors without electronic access.

The following Technical Standards updates are relevant to all technical and construction employees and contractors undertaking design and/or construction activities on the CitiPower and Powercor networks.

A list of the **CitiPower/Powercor Technical Standards March 2017 releases** is available below, including links to summaries and are available to view in full on the Source.

*All new design and construction proposals commenced after the **1 June 2017** are required to comply with these Technical Standards updates.*

If you have further questions, please contact the relevant Technical Standards Engineer associated with the published Standards/Specifications.

Regards

Steven Neave
General Manager, Electricity Networks

Never Compromise Safety Rules

1. Electrical permits
2. Live work
3. Polarity and NST testing
4. Working at heights
5. Plant and equipment
6. Personal protective equipment (PPE) and clothing
7. Drive safe
8. Risk assessment

NEVER COMPROMISE health & safety

Standard Category	Technical Standard	Standard Description	Overview	Impacted Key Stakeholder/s
D - General	DE011	Distribution Construction Standard - Connectors – Application	Standard updated to remove auto splice information and add 3 new full tension compression sleeves as the standard connection for copper and cad copper conductor. **Contact Darren Martini (03) 9683 4738**	CONSTRUCTION DESIGN
	DE131	Distribution Construction Standard - Connectors – Full-Tension Splices	Standard updated to remove all information regarding auto splices. **Contact Darren Martini (03) 9683 4738**	
	DE136	Distribution Construction Standard - Connectors – Full-Tension Sleeves	Standards updated to include 3 new full tension compression sleeves for existing imperial Cad Cu conductors (7/0.073, 7/0.093, 7/0.113) to table 2 & 4. **Contact Darren Martini (03) 9683 4738**	
	DE411-705	Distribution Construction Standard - Splices, Sleeves, Links, Lugs & Misc. Connector Materials	Standard updated to remove DE411 and add 3 new full tension compression sleeves for existing imperial Cad Cu conductors (7/0.073, 7/0.093, 7/0.113) to DE431. **Contact Darren Martini (03) 9683 4738**	
Click here for a SUMMARY of the above standards				
				LEGEND HIGH IMPACT MEDIUM IMPACT LOW IMPACT

Figure 4-22 – CP-PAL's Technical Standards Update

Community Consultation & Communication

CP-PAL manage community consultation as per the Community Consultation Policy[122]. The policy ensures that CP-PAL supports and establishes open, fair and constructive consultation with the community, when proposed works may affect community amenity. CP-PAL also ensures that the community is aware of all works proposed that may affect their amenity as early as is practicable, to provide opportunities to comment, seek additional information and to raise concerns.

CP-PAL utilise our corporate website for practical and effective communication to the community of safety related messages and projects. The website provides information ranging from safety around network assets, to descriptions of current safety projects, such as the powerline replacement program in bushfire prone areas, where the public is informed of impacts, benefits and project timelines.

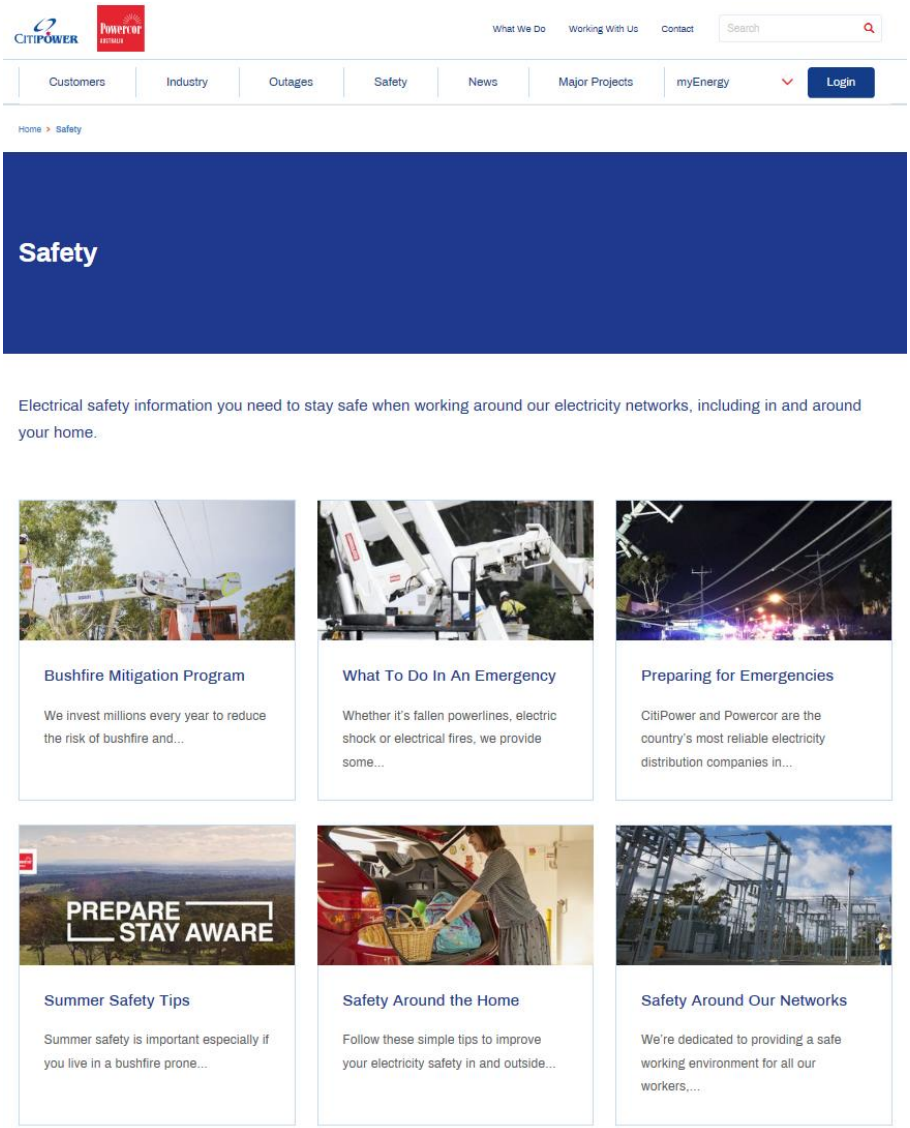


Figure 4-23 – CP-PAL webpage 'Safety screenshot

[122] CP-PAL, Community Consultation Policy – 04-05-CP0001

CP-PAL also utilises its website as a dedicated stakeholder engagement and consultation channel for keeping customers updated, informed and aware of opportunities in engagement activities. The website provides an opportunity to understand customers' views and desired outcomes, which assist in the critical business planning process and the development of regulatory submissions.

CP-PAL also communicates directly with customers regarding outages. This is particularly important for our life support customers who require greater notice and consultation regarding planned outages. All unplanned outages are also updated on the website, whilst the contact centre provides additional information directly to impacted customers.

4.2.4.2 Financial Planning & Approval

CP-PAL's regulated capital investment and operating expenditure relates to the following activities:

- Asset replacement
- Reliability improvement
- Bushfire and safety improvement
- Load demand
- Customer initiated works

An Electricity Distribution Price Review (EDPR) is required to be submitted to the Australian Economic Regulator (AER) every 5 years for investment in the network over the forthcoming EDPR period. This process determines the revenue requirements, which is funded through customer network supply charges, for the operation and maintenance of the network.

Each year an internal annual budget and a 10-year financial plan are determined. Budget approval and forecasting are undertaken annually through internal review and revision of AMPs and policies to ensure alignment with asset management objectives.

Historical volumes of asset replacement, which have been undertaken through maintenance activities, are taken into consideration when establishing the annual budget, EDPR submissions and 10-year plan. CP-PAL is committed to taking a targeted and cost effective approach to the replacement of its assets, with replacement relevant to asset condition. This condition assessment includes reviewing the overall performance of an asset class to ensure that expected end of life volumes are managed to avoid any 'bow wave' of age related asset replacement. For example, there are approximately 635,543 poles in the CP-PAL network. The pole age profiles for CP-PAL poles are discussed in section 3.1.1.1 of the Safety Case. Each pole is inspected on a cyclic basis in accordance with an asset management plan to determine pole condition. This condition assessment data is collated to form an overall view of pole condition, which identifies how many poles are in a serviceable and unserviceable condition. This is then considered when establishing EDPR submissions and forecast budget replacements to ensure poles remain in a serviceable condition and that replacement volumes are managed within budget forecast.

Projects go through a series of approval levels depending on their cost. These levels include:

- Staff Delegation of Authority (DOA) – Individual responsible for approving projects within their delegation (e.g. senior manager level).
- Network Investment Committee (NIC) – The NIC is primarily responsible for approving projects related to the network or customer projects exceeding individual staff DOA levels.
- Victorian Power Networks Investment Committee (VPNIC) – The VPNIC evaluates and approves major expenditure at each stage of development to ensure that both an appropriate level of diligence has been undertaken and that the investment is in line with CP-PAL's strategic direction.
- Board approval – Major projects and contracts require approval by the Board.

Overview of the NIC and VPNIC is outlined in Figure 4-24 below:

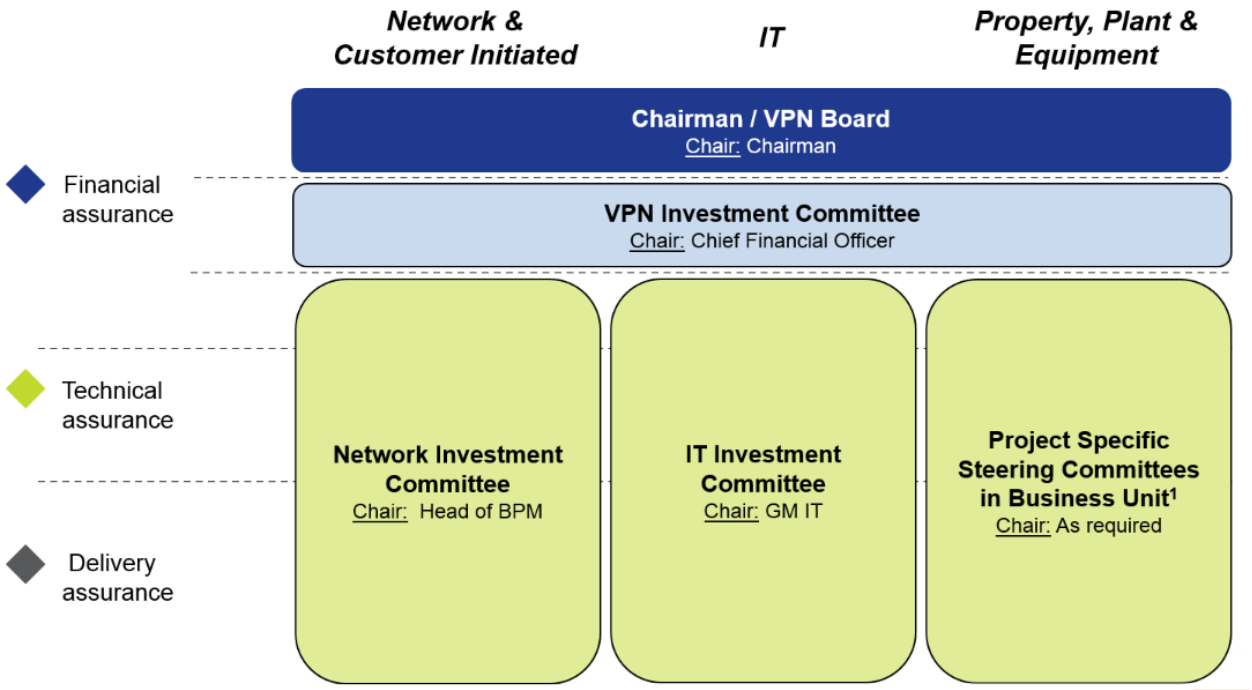


Figure 4-24 – Overview of VPN IC, NIC and ITIC

Initiatives in the financial plan are prioritised by considering regulatory obligations, safety risks, bushfire risk, demand expectations, asset availability, reliability, functionality and reputation. The priority ranking is achieved via the use of priority ranking using Copperleaf C55. The overview of capital expenditure budget process is provided in Figure 4-25 below.

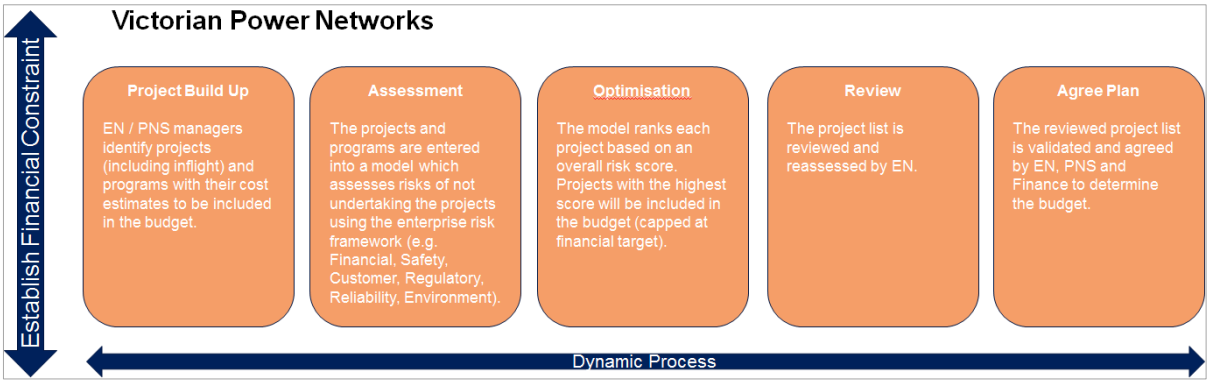


Figure 4-25 – CP-PAL EN Capital Expenditure Budget Process

4.3 Network Asset Life Cycle Activities

The network asset lifecycle activities include design, construction, commissioning, operation, maintenance, and decommissioning enable the business to operate the network safely and reliably.

These key network activities are ESMS risk mitigation controls, which are further discussed below.

4.3.1 Design and Delivery

Design is one of the controls in managing network safety risks. CP-PAL design network assets to perform safely and reliably. If assets are not designed using robust engineering analysis, they pose a risk of failure. Inappropriate design can lead to incorrect construction, commissioning, operations and maintenance of network assets, which lead to safety and reliability consequences.

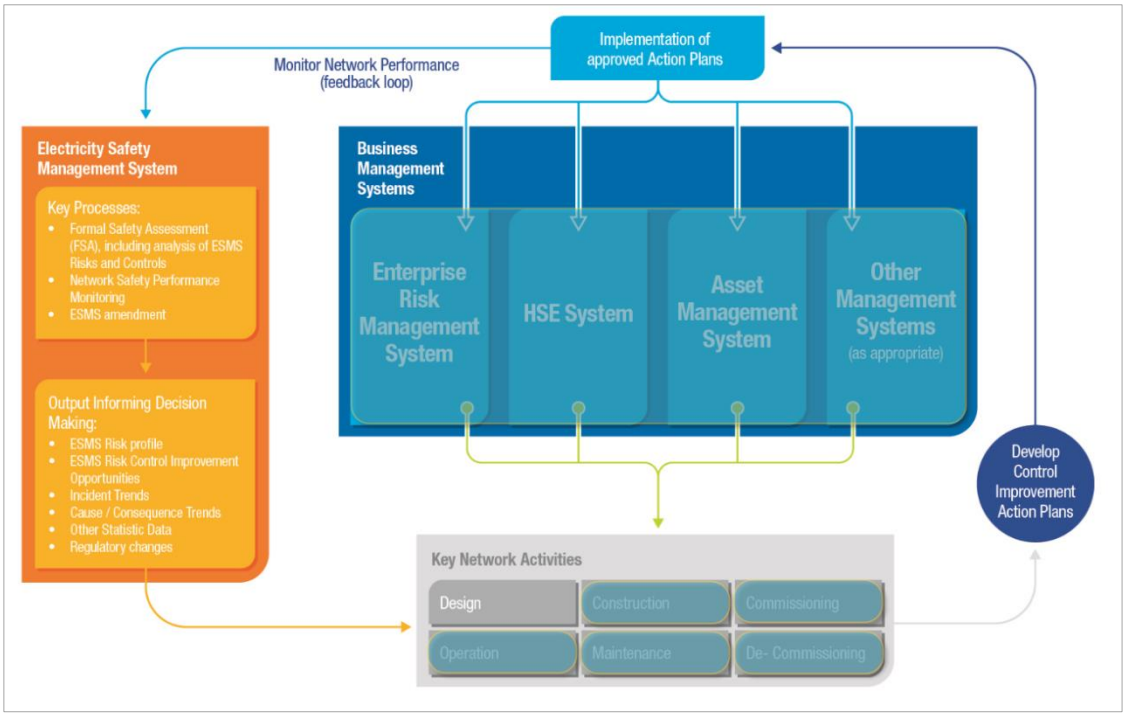


Figure 4-26 – ESMS Integration with Design

The Program Design and Delivery section of CP-PAL encompasses a large number of functions, specifically the management of technical design generation, project management, design performance and delivery. Detailed designs are created in accordance with both CP-PAL and Australian Technical Standard requirements. The Program Design and Delivery group also complete a Safety In Design assessment[123] for all projects, identifying project specific risks, their likelihood of occurrence/severity and any mitigation and control measures to be applied.

The procedure for any non-standard designs, which may mandate deviation from CP-PAL Technical Standards, is detailed in section 3.6.8. The Non Standard Structure Approvals Procedure[124] aims to ensure that non standard structures are appropriately developed or reviewed before construction.

4.3.1.1 Design Commitments

The commitment policies as discussed in *Section 2 Policy and Commitment* enable CP-PAL to establish the following network design key commitments:

- CP-PAL shall design its distribution network in accordance with both CP-PAL and Australian Technical Standards.
- CP-PAL shall undertake Safety In Design assessments for all design projects.
- CP-PAL shall undertake the Constructability, Operability and Maintainability (COM) reviews for all major projects.

[123] Safety in Design Risk Assessment - JEQA4UJ443MT-160-229

[124] Non Standard Structure Approvals Procedure" Document # JEQA4UJ443MT-160-43

These commitments are further detailed in sections 4.3.1.2 – 4.3.1.3 demonstrating how each is met.

4.3.1.2 Design Process Overview

Figure 4-27 illustrates each stage of the design process, from Project Management, Design Allocation and Management through to Construction. The 'Safety In Design' assessment spans the entire design process, from project initiation to closeout, ensuring all risks are identified and managed effectively. The 'Safety in Design' forms the basis of risk mitigation throughout the design process and is discussed further in section 4.3.1.3.

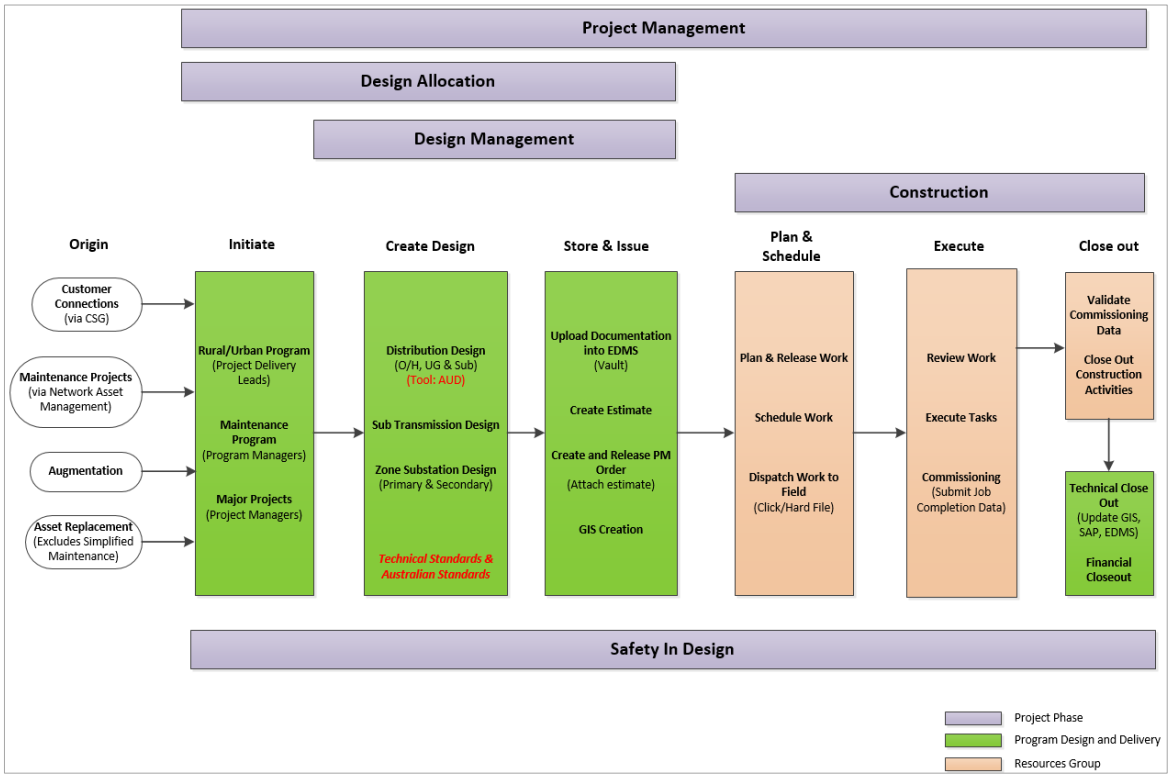


Figure 4-27 – Simplified Design and Delivery Process

The 'Design and Delivery' process presented above consists of the following stages:

1. ***Origin*** – Design requests originate from:
   - Customer connections requests (via the Customer Services Group or 'CSG'),
   - Maintenance projects
   - Network augmentation activities
   - Asset replacement projects

2. ***Initiate*** – Depending on the details of the project requested, the *design allocation phase* is initiated by one of the three project management groups: Rural/Urban Programs, Maintenance

Programs and/or Major Projects. A Design Request[125] process is in place to ensure that Project Managers are able to create, modify and submit design requests.

- The Rural and Urban Program groups are responsible for managing projects involving the design, maintenance or and construction of new and existing distribution network assets, including distribution substations and overhead and underground assets in urban and rural areas. The rural and urban groups differ in structure and size due to different volumes and complexity of work. Design requests within the two groups are managed by Project Delivery Leads, who are responsible for managing the delivery of projects to ensure design targets are achieved on time and budgets are met in accordance with quality and HS&E obligations. They are also responsible for customer and stakeholder management throughout the life of the design project.
- The Maintenance Program group is responsible for the efficient and timely delivery of Electricity Networks maintenance programs, including those related to electrical plant, government initiated programs resulting from the Victorian Bushfire Royal Commission (e.g.: installation of vibration dampers) and overhead line maintenance management. Program Managers are responsible for managing projects within the group.
- The Major Projects group is responsible for management of projects involving design, maintenance or construction of major distribution infrastructure, such as zone substations, sub-transmission lines or major customer projects. These projects require the supervision and management of dedicated Project Managers.

3. ***Create Design***[126] – The first phase, *design management*, is where technical designs are drafted by Design Engineers and Technical Officers, which adhere to applicable CP-PAL and Australian Technical Standards, for projects initiated in the previous stage. Designs activities are categorised into three groups reflecting technical requirements or scope of the project:

- Distribution Design (overhead/underground distribution assets and distribution substations)
- Sub-transmission Design
- Zone Substation Design (including Primary and Secondary design activities)

The AutoCAD Utility Design (AUD) engineering software package is used when completing detailed designs for overhead, underground and substation projects. This software also completes engineering analysis, validation and rectification of distribution designs. AUD is configured to adhere to the latest CP/PAL Technical Standards and design rules, and is maintained by the Design Performance and Technical Standards groups.

During this stage of the design process, the Design Manager will facilitate a Constructability, Operability and Maintainability (COM)[127] review for all major projects, ensuring design process is in accordance with the scope of works. All comments regarding

[125] Design Request – JEQA4UJ443MT-203-194

[126] Create Design Procedure – JEQA4UJ443MT-160-224

[127] COM Review Guideline Document – DM-PRO-0004

the design are raised and discussed during the COM review meeting, and (if required) a list of modifications and amendments is collated and incorporated into the designs. In every COM review meeting, one representative from each design discipline is present.

- ***Store & Issue*** – During this stage, the drafted design documents are uploaded into an Enterprise Document Management System (EDMS) called 'Vault'. 'Vault' is used for organising, managing and tracking the drawing and design files used by teams across the business. 'SAP' estimating software is then used to create 'cost-to-build' estimates for the designs. Plant Maintenance Orders (PMOs) are then created, which releases the design to the Resources Group for construction.
- ***Plan & Schedule*** – The beginning of *Construction phase*, where planning, scheduling and dispatching of work to field (through the use of 'Click' system or hard file) occurs. The construction phase is managed by the Resources Group which provides field services for CP&PAL.
- ***Execute*** – Construction work is reviewed and carried out. Assets are commissioned upon completion.
- ***Close Out*** – This stage is triggered when work has been executed and all completion data has been submitted from the Execute phase, either via hard file submission or using the mobile device ('CLICKMobile').

4.3.1.3 Safety In Design

The design process is undertaken in accordance with the *Energy Design Policy*[128]. It ensures that all design work is to be done in a safe, standardised and consistent manner.

The most effective means of implementing safety in a product, workplace or system of work is at the design phase. It is at the design phase that the potential for future hazards and incidents can be discussed, anticipated and avoided. A safe design means integrating control measures early in the design process to eliminate or, if this is not reasonably practicable, minimise risks to AFAP, for health and safety throughout the life of the final product.

Safety in Design[129] is a process completed for all projects, to ensure that the CP-PAL electricity network has an efficient, safe and functional design throughout the entire asset lifecycle (i.e. Construction, Commissioning, Operations, Maintenance, Upgrade, Decommissioning and Dismantling).

[128] Energy Design Policy – 15-05-CP0001

[129] Manage Safety in Design Procedure – JEQA4UJ443MT-150-162

#	Life Cycle Phase	
1	Construction / Installation	Hazard Identification, Risk Assessment & Control
2	Commissioning	
3	Operations	
4	Maintenance / Repair	
5	Upgrade / Retrofit	
6	Decommissioning	
7	Demolition / Dismantling	

Figure 4-28 – Safety In Design Considerations

Upon completion of this process, the following has been achieved:

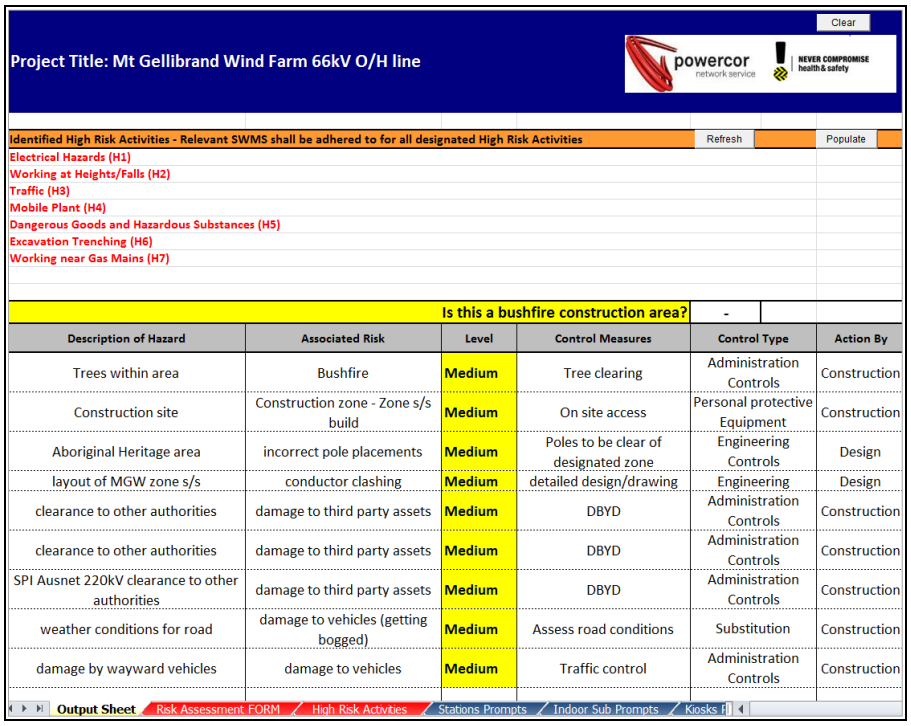
- All risks are acknowledged in the design process.
- Control measures are to be applied that enable the risks to be managed throughout the product lifecycle.
- Risks shall be managed to a level of As Low As Practicable (AFAP).
- Residual risks associated with the design are communicated to end users and other interested parties.

During the hazard identification phase of the 'Safety in Design' process, designers consult with relevant stakeholders who will interact with the product in as many stages of its life cycle as possible. The designers then record and communicate all identified hazards and applied control measures with stakeholders as part of the risk assessment process. Design documentation and any residual risks are then communicated to all persons who will interact with the product throughout its lifecycle.

The *Safety in Design Risk Assessment Work Instruction*[130] details the steps taken by a designer in recording and communicating all identified hazards and the applied control measures in a structured template. The template is used throughout the project lifecycle, especially during the initial risk assessment undertaken during the project bid phase. Further risk assessments are undertaken during project team kick-off meeting and subsequent periodic reviews by the project team.

The below screenshot of the *Safety in Design Assessment template* shows how the process was applied to identify hazards, risk and control measures associated with the Mt. Gellibrand Wind Farm 66kV overhead line construction project.

[130] Safety in Design Risk Assessment – JEQA4UJ443MT-160-229



Project Title: Mt Gellibrand Wind Farm 66kV O/H line

Clear

powercor network service

NEVER COMPROMISE health & safety

Identified High Risk Activities - Relevant SWMS shall be adhered to for all designated High Risk Activities

Refresh Populate

Electrical Hazards (H1)
Working at Heights/Falls (H2)
Traffic (H3)
Mobile Plant (H4)
Dangerous Goods and Hazardous Substances (H5)
Excavation Trenching (H6)
Working near Gas Mains (H7)

Is this a bushfire construction area? -

Description of Hazard	Associated Risk	Level	Control Measures	Control Type	Action By
Trees within area	Bushfire	Medium	Tree clearing	Administration Controls	Construction
Construction site	Construction zone - Zone s/s build	Medium	On site access	Personal protective Equipment	Construction
Aboriginal Heritage area	incorrect pole placements	Medium	Poles to be clear of designated zone	Engineering Controls	Design
layout of MGW zone s/s	conductor clashing	Medium	detailed design/drawing	Engineering	Design
clearance to other authorities	damage to third party assets	Medium	DBYD	Administration Controls	Construction
clearance to other authorities	damage to third party assets	Medium	DBYD	Administration Controls	Construction
SPI Ausnet 220kV clearance to other authorities	damage to third party assets	Medium	DBYD	Administration Controls	Construction
weather conditions for road	damage to vehicles (getting bogged)	Medium	Assess road conditions	Substitution	Construction
damage by wayward vehicles	damage to vehicles	Medium	Traffic control	Administration Controls	Construction

Output Sheet | Risk Assessment FORM | High Risk Activities | Stations Prompts | Indoor Sub Prompts | Kiosks

Figure 4-29 – Safety in Design Assessment Template

As shown in the figure above, the risk assessment template contains several interdependent tabs:

- Output Sheet – Used primarily for communication of hazards between design group and field construction crews.
- Risk Assessment FORM – Used for identifying safety hazards and risks based on individual projects; mandatory for all projects.
- High Risk Activities – Lists the relevant High Risk Activities that are present in the Electrical Distribution Business, as prescribed by section 5.1.5 of the OH&S Regulations 2007.

Various Prompt Tabs – These are used as hazard prompts to assist the user in identifying and recording hazards. These consist of hazard listings for indoor substations, kiosks, underground assets, major and minor projects.

Technical Standards

Network design is performed in accordance with our internal technical standards that are derived from published Australian Standards, International Standards (i.e. IEC) and industry guidelines.

Technical standards are a key tool in defining safe standards for design, construction and operation of our network assets. For details of their operation and function, refer section 3.6.

Design Performance and Governance

The Design Performance group undertakes progressive performance reviews of design activities as part of a continuous improvement cycle. As part of this review, the following functions are considered:

- Design and approval in accordance with Design Management Procedure[131]
- Technical compliance
- Safety In Design
- Governance of Design and Delivery functions
- Innovation portfolio
- Ownership and management of End-to-End
- Ownership and management of engineering systems and tools: AutoDesk, Vault, GIS creation and close out. Business owner for GIS to provide specialist services to the business, including:
  - 3D modelling for OH & UG line Design, indoor substation design, civil and primary design
  - GIS Analytics, data capture, load forecasting and asset modelling
  - LiDAR data is used for surveying and modelling and for determining Vegetation clearances.

4.3.2 Construction and Commissioning

Network augmentation, asset replacements and customer connection projects require construction and commissioning works to be undertaken. If these are not done safely, to quality standards and competing timeframes poses potential risk for safety and reliability of supply.

[131] Design Management – JEQA4UJ443MT-160-230

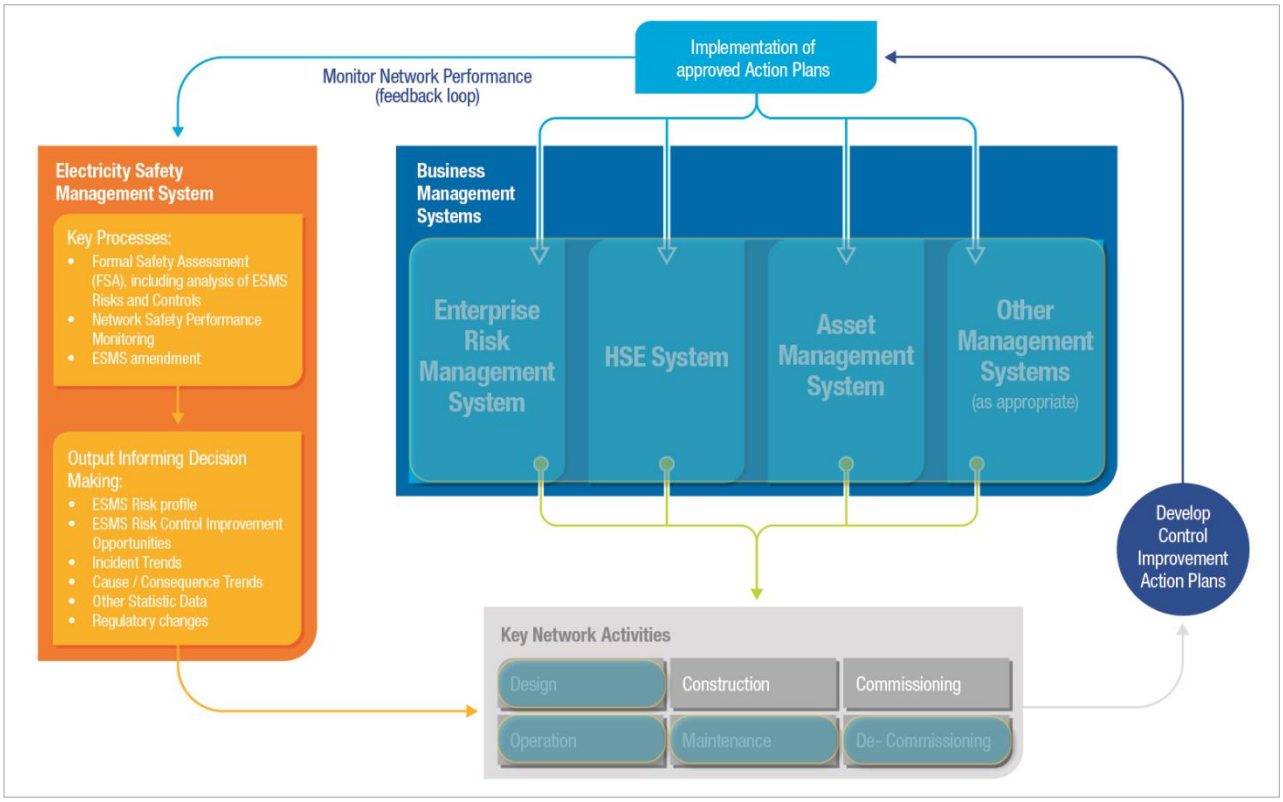


Figure 4-30 – ESMS Integration with Construction and Commissioning

4.3.2.1 Construction and Commissioning Commitments

The commitment policies as discussed in *Section 2 Policy and Commitment* enable CP-PAL to establish network construction key commitments as listed below.

- CP-PAL shall plan and optimise the works program
- CP-PAL shall adopt a consistent and standardised approach for all works scheduling and dispatch functions using standard processes, systems and tools
- CP-PAL shall meet Health, Safety and Environmental outcomes
- CP-PAL shall respond to faults to ensure rapid continuity of supply to the customer

The abovementioned commitments are discussed in sections 4.3.2.2 – 4.3.2.6 below to demonstrate **how** these commitments are met.

4.3.2.2 Construction and Commissioning Process Overview

The management of network assets construction activities is undertaken and managed by Powercor Network Services (PNS), responsible for project management, design and construction, in consultation with the Electricity Networks.

All construction activities applicable to network assets are undertaken in accordance with design requirements and CP/PAL technical standards.

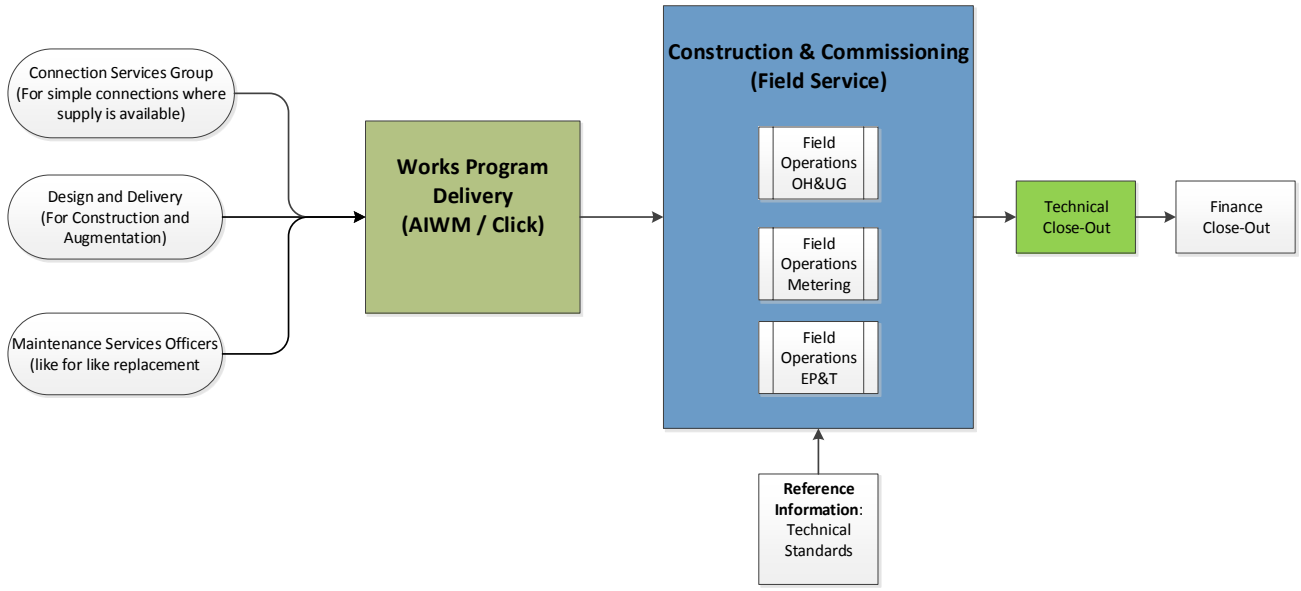


Figure 4-31 – ESMS Integration with Construction and Commissioning

Network construction activities are undertaken in accordance with the 'Standard Works Practices' as specified by the 'Safety and Works Practices' group. Refer section 4.2.2.2 of this ESMS.

Construction and commissioning relevant areas of PNS are further discussed below.

Works Program Delivery Team (WPDT)

WPDT provides a consistent and standardised approach for all works scheduling and dispatch functions using standard processes, systems and tools. The WPDT aims to deliver works to meet Health & Safety outcomes, maximise utilisation, productivity and target delivery achievement.

The WPDT is responsible for resource assignment against work orders[132].

The WPDT group lead and manage the work scheduling and have accountability for:

- Planning and optimisation of the works program
- Providing a consistent and standardised approach for all works scheduling and dispatch functions using standard processes, systems and tools
- Optimising the schedule such that work meets Health, Safety and Environmental outcomes
- Maximising utilisation, productivity and target delivery achievement
- Leading and managing supply versus demand (forecast versus capacity)

Works Management

All construction and commissioning works are delivered using the Automated Integrated Works Management (AIWM) IPSDEC framework. IPSDEC framework is illustrated in Figure 4-32 below.

[132] Scheduling Resources Group Work Guideline – 20-15-G0001

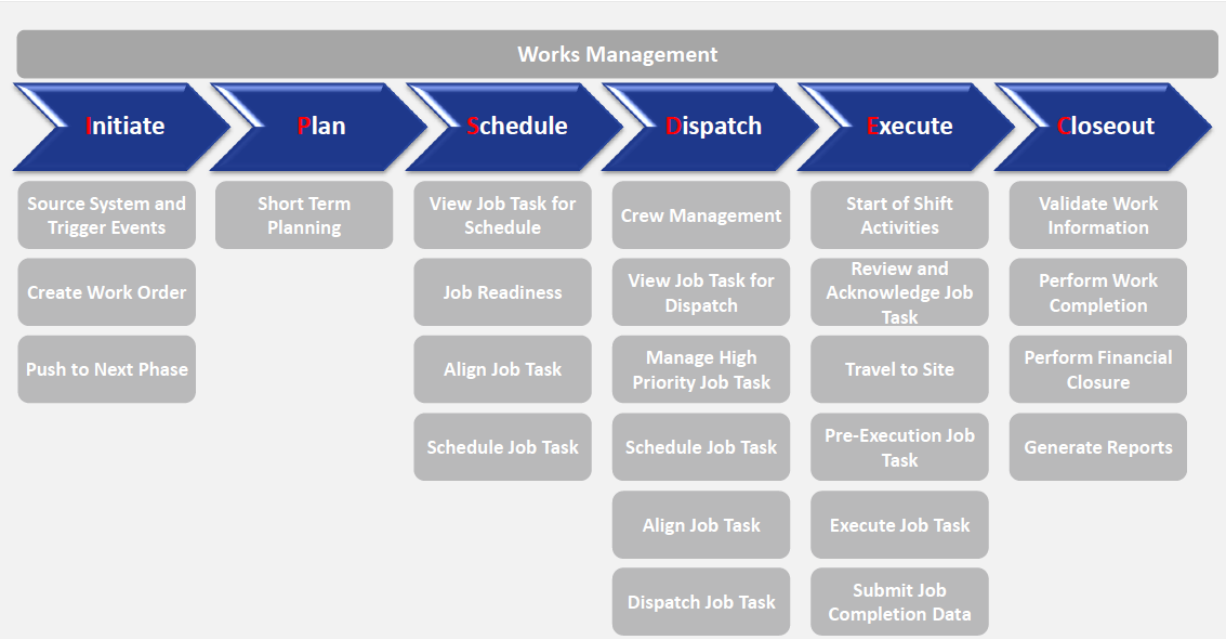


Figure 4-32 – IPSDEC Framework

IPSDEC framework is further elaborated in Figure 4-33 below to reflect how the end-to-end business process and function.

Faults are managed via the abovementioned AIWM IPSDEC framework principles. But the levels of details vary depending on the situation.

End to end business process and functions

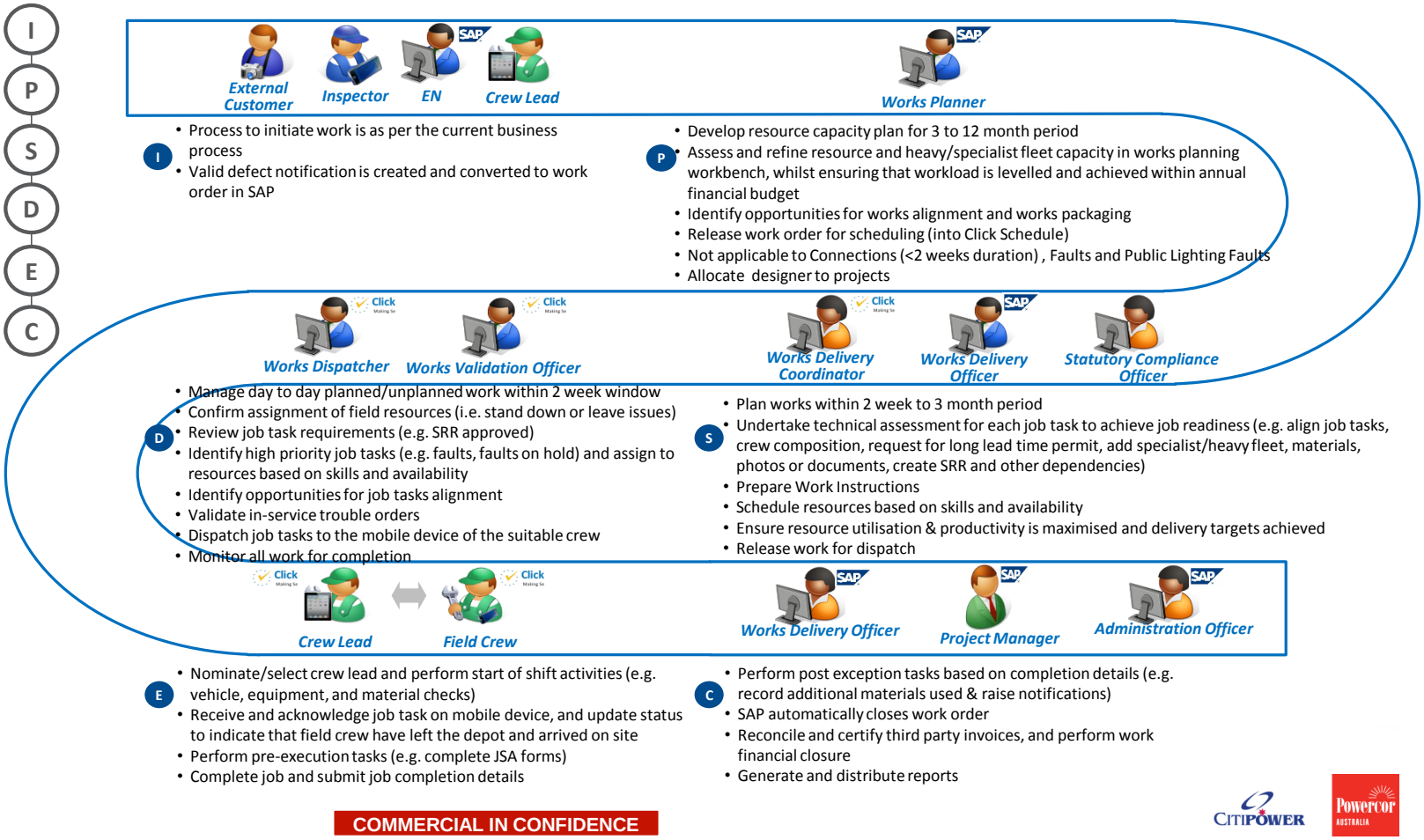


Figure 4-33 – A more detailed view of overall Works Program Delivery and Construction & Commissioning processes

When the Works Initiator (typically a Project Manager) releases activities to be completed within SAP (status updated from Created to Released) this information is available for the Works Planners (within Portfolio Governance) to manage future resource requirements (from 3-12 and even up to 18 months) to ensure maximum foresight of resource peaks and troughs. The Works Planner dependent on resource forecasts and capacities will release the Work Orders into the WPDT for scheduling and dispatch. Field Services will execute the work orders and provides field closeout. (This could be automatically through actions on the field mobile device or manually dependent on the work stream.) The Work Initiator is then responsible for business and financial closeout.

Similar level of detailed process may not apply against all work types (e.g. Faults and Connections).

Figure 4-33 above illustrates how end-to-end business processes work to deliver the field works including construction and commissioning works.

Works Planning and Scheduling

Works planning and scheduling processes are triggered by planned augmentation and construction works of the distribution network. Planning and scheduling of work is carried out safely and in line with ESMS requirements, the following embedded policies, guidelines and procedures:

- Scheduling Resources Group Work Guideline[133]
  The guideline provides parameters for employees to effectively complete the scheduling of planned work. It provides employees with a consistent reference and understanding of the scheduling process and serves as a guide to the items that must be considered when scheduling works. The guideline also provides information to assist employees in meeting compliance obligations, which require the control of any particular risk. This is achieved by providing each employee who may be exposed to the risk with sufficient information, instruction and training to perform his or her work in a manner that is safe and without risks to health.
- Manage and Schedule Work Procedure[134]
  The procedure describes in detail the processes associated with scheduling and dispatching work which utilises information technology organisational tools to issue and receive work tasks and monitor the works program.
- Live LV Work
  CP-PAL preferred approach is to conduct all LV works live where safe and practicable to do so. Whilst field scoping is conducted, the consideration is given to whether works should be done live or dead based on the following criteria:
- Safety

[133] Scheduling Resources Group Work Guideline – 20-15-G0001

[134] Manage and schedule work - JEQA4UJ443MT-68996575-121

- Complexity
- Safe Work Method Statements (SWMS) and Safe Works Practices
- Access requirements
- Other variables

Field staff will always conduct site risk assessment prior to executing works and will only proceed if the live LV works can be completed safely.

Part of the works planning and scheduling requires initiating a DBYD request for relevant UG excavation works. A PTW is organised where identified by the DBYD process. This process helps CP-PAL meet the regulatory requirements of Gas Industry and Pipelines Acts relevant to excavation works.

4.3.2.3 Field Services

Field services key responsibilities include effective utilisation of field resources, driving consistency, productivity and continuous improvement in field operations. Local ***Field Leader*** (Field Services) has day-to-day oversight and management of field resources.

The Field Services group leads and manages the field resources and has accountability for:

- The ongoing Health and Safety and Environmental compliance matters;
- Maintaining, Constructing and Augmenting the Distribution Networks (Overhead and Underground assets);
- Responding to faults to ensure rapid continuity of supply to the customer;
- Assessment for completed work to standard. For e.g. Verification /Statements of works
- The professional development and performance management of field resources.

Construction Project Leaders and Work Site Leaders are in-field based positions to supervise and lead on the job delivery of construction activities to ensure conformance to stakeholder requirements as measured by time, quality and cost. ***Construction Project Leaders*** *may also be requested by the* ***Works Delivery Coordination*** *team to input into and assist with field planning activities and applications for Network Access.*

As part of field mobile works, consultation was facilitated with employees and applicable unions. Post implementation of the technological and process changes employee representatives have had opportunities to workshop and be involved in future system and process development.

4.3.2.4 Site Hazards and Risks Identification

Hazards are identified during the process via:

- Office based planning and assessment aiming to engineer risks and hazards out of the process wherever practicable. For example, the Works Delivery Coordinator (WDC) reviews the Work Order task and scope and this helps promotes this.
- Field Onsite assessment (Field Plan) completed by our Project Leaders for tasks that require planning of resources other than short term unplanned works or Priority 1 and

fault response requiring immediate action. The field plan is provided to the Works Delivery Coordinator prior to the job being scheduled and will give enough lead time to book nominated resources. A Field Plan does not take the place of a SWMS or JSEA but may reference, or be part of either document.

- Site Risk Management processes by Field Crew further identify any local hazards due to terrain or local conditions. These are mitigated and managed by the use of JSEA, SWMS, and Daily Take 5's.
- Mandatory use of Personal Protective Equipment (PPE Mandatory use of Personal Protective Equipment (PPE).

Also from the Executive level to all level of management, a structured program of safety observations and conversations are built into our KPI's.

Hazards and risks identified during the works can also be reported with the use of the following applications, which are readily available to the field crew:

Never Compromise Safety

Never Compromise Safety application provides ready access to report incidents, hazards and working alone events. It also provides access to safety notices that have been published or circulated by the business.

The introduction of the Never Compromise Safety application has driven a significant increase in the reporting of hazards, which assists in undertaking preventative actions to mitigate the hazard.

An example of an application that is available on iPhones and iPads to field personnel is shown below in Figure 4-34 being the Never Compromise Safety App.

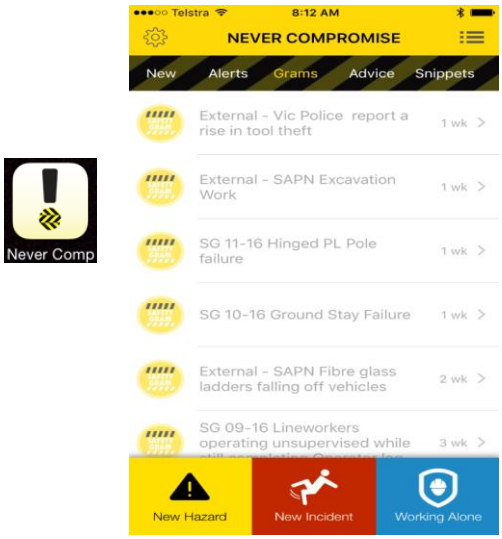


Figure 4-34 – CP-PAL Never Compromise App – iPhone

Report It

Report It application captures details of, and reports asset and vegetation defects and GIS inconsistencies.

Simpler steps in submitting the report including defects with the assets are outlined below:

1. Take a photo and mark up.
2. Select the equipment to be reported.
3. Select the type of report.
4. Provide any additional info and comments then submit.

A WDC will document or identify any known hazards or risks through the Long text against the Work Order operation, or through the Additional Information section within ClickSchedule. This information is supported by the fieldwork practice requirements to complete the JSEA and SWMS processes on site at the time of work.

4.3.2.5 Site Hazards and Risks Management

Hazard identification

- A Work Delivery Co-ordinator (WDC) as part of their planning process will identify any known hazards or risks through the Long text against the Work Order operation or through the Additional Information section within ClickSchedule.
- Hazard information is also available via *HSE Hub* and *Cintellate*.

Site hazard management

- Hazards are assessed and managed against a risk matrix as part of Site Risk Management processes, Training, Qualifications and Authorisations and Work Practices; and
- Through the provision of tools and supporting information to assist in meeting compliance obligations (e.g. Work Order Scope, task lists and other supporting documents on Secure content locker).

Site safety risks management

- Safety risks are eliminated or reduced to as low as reasonably practicable during normal and abnormal Operations principally by engineering them out of the process up front at the design and preplanning phases; and
- The Field Worker follows a work practice requirement that augments this risk mitigation by undertaking an on-site assessment to create a relevant JSEA complementing our structured SWMS.

The Training, Qualifications, Authorisations and Work Practices documents provided to employees also support their ability to identify hazards on site. We also provide Field Services with tools and supporting information to assist in meeting our compliance obligations (e.g.: Work Order Scope, task lists and other supporting documents on *Secure* content locker and *HSE Hub*).

4.3.2.6 Construction and Commissioning Records

Most of the records handled by the ***WPDT*** are electronic works orders in SAP. All key documentation is uploaded and stored against the relevant PM Works Order or Work Order Operation.

As an example SAP PM Oder 1349398 has the following documents attached:

- Safety in Design
- DMS SAR sheet (proposed and existing assets)
- Construction Plan
- Project Environmental Control Checklist
- Roads Exemption.

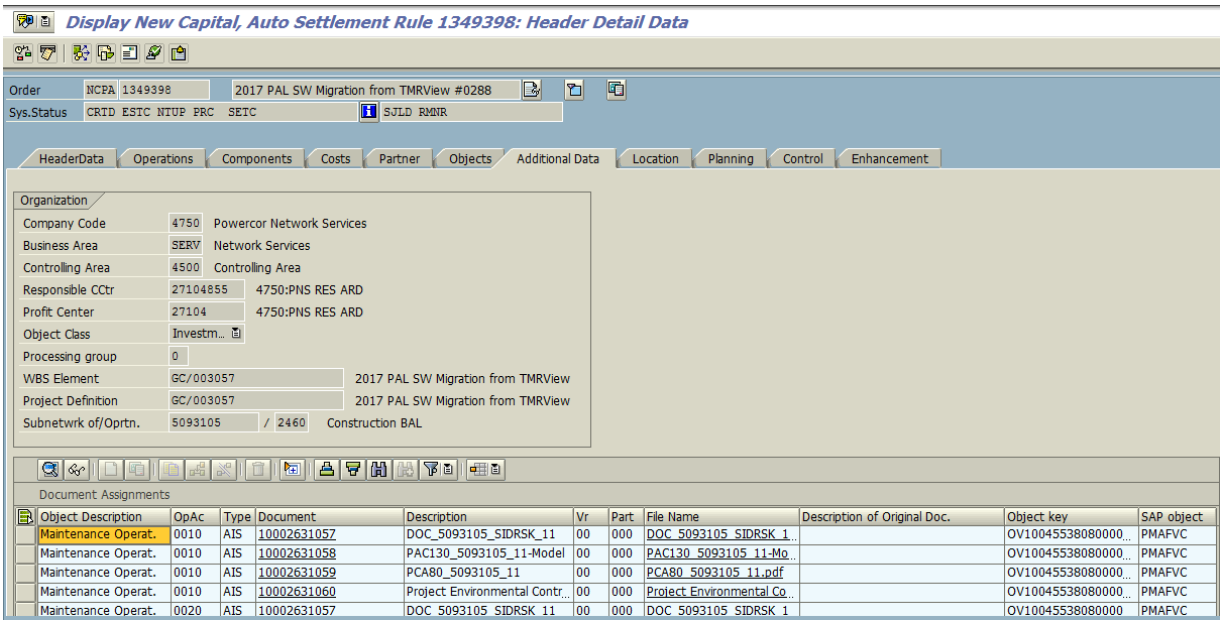


Figure 4-35 – SAP PM Order Example

If there is a need to make changes and updates to ***Field Services*** & ***Works Delivery*** records then a reinitiate process has been established where the ***WPDT*** re-initiate in SAP ('REINT') if the change significantly impacts the delivery of work and/or timeline, **and then only upon agreement with the project initiator**:

- Field planning identified significant change to project scope
- Change in budgeted hours
- Unable to meet delivery timeline / deliver by the 'notification date' (for lines maintenance, early escalation to the program manager required)

4.3.2.7 Governance of Construction and Commissioning

Within the WPDT the Works Program Delivery Manager is responsible for approving policy and procedure documentation.

All Job Description documents within the WPDT have an innovation and continuous improvement section that typically requires all team members (at all levels) to:

- Create and instil a workplace culture that is focused on work place continuous improvement.
- Actively support and gain employee engagement in new or modified processes and systems.
- Identify, analyse and improve Works Program Delivery by understanding and addressing the root causes of projects not meeting agreed performance measures
- Review, maintains and manages update of key systems (e.g.: RealEst, Skills, SAP HR) to ensure the accuracy, currency and effectiveness of the key information used for schedule optimisation.
- Commit to maintaining and updating technical skills and knowledge (as required).

4.3.3 Operations

Network operations are essential for the safe operation of the network and reliable supply of electricity to our customers.

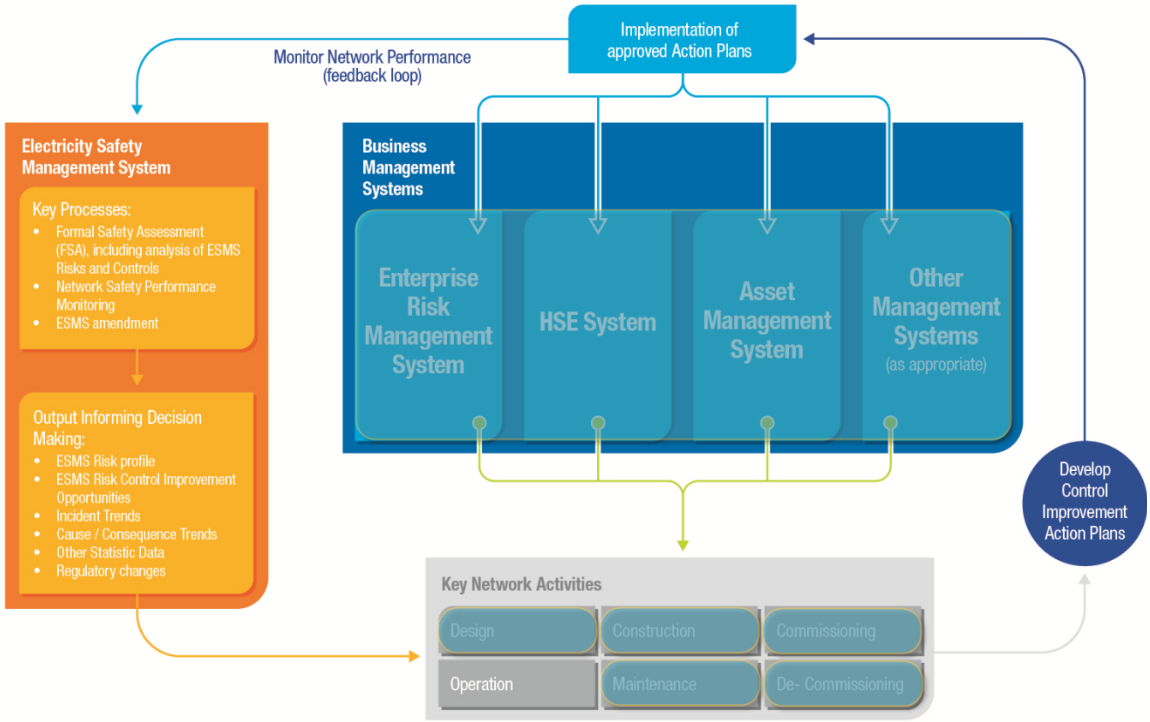


Figure 4-36 – ESMS Integration with Operation

Network control and operations act as central interface across various areas of business and external stakeholders for managing planned and unplanned outages, facilitating fault response and emergency response.

Incorrect network operations can lead to safety and reliability consequences.

4.3.3.1 Operations Commitments

The commitment policies as discussed in *Section 2 Policy and Commitment* enable CP-PAL to establish network operations key commitments as listed below.

- CP-PAL shall have 24x7 manned control room, field operators on duty and customer contact centre
- CP-PAL shall attend to all the known faults, unsafe situations and make safe
- CP-PAL shall maintain compliance with the Victorian Distribution Code which requires that in the case of an unplanned interruption or an emergency, a distributor must use best endeavours to restore the customer's supply as soon as possible making allowance for reasonable priorities

These commitments are further detailed in sections 4.3.3.2– 4.3.3.5 demonstrating **how** each of these is achieved.

4.3.3.2 Operations Process Overview

The Network Control and Operations division manage the System Control Centre and Operational functions for Electricity Networks. The functions of Network Control and Operations span across both planned and unplanned works.

Network Control and Operations are responsible for the following:

- Safe operation and switching of network including 24x7 real-time monitoring of the network
- Field coordination including issuing and management of Access Authorities
- Coordination with external stakeholders such as SES, CFA, Police, AEMO etc. including escalation events
- Network performance monitoring, reporting and reliability improvement initiatives
- Operations
- Contingency Planning management
- Quality of Supply
- Fault Response
- Outage Management
- Faults Incident Investigation
- HV / LV switching incident investigations
- Authorisation of employees and contractors

Network Control and Operations consist of the following key sections:

- Control (System Control Centre)
- Network Access

- Network Performance

Overview of Network Control and Operations is presented in Figure 4-37 below:

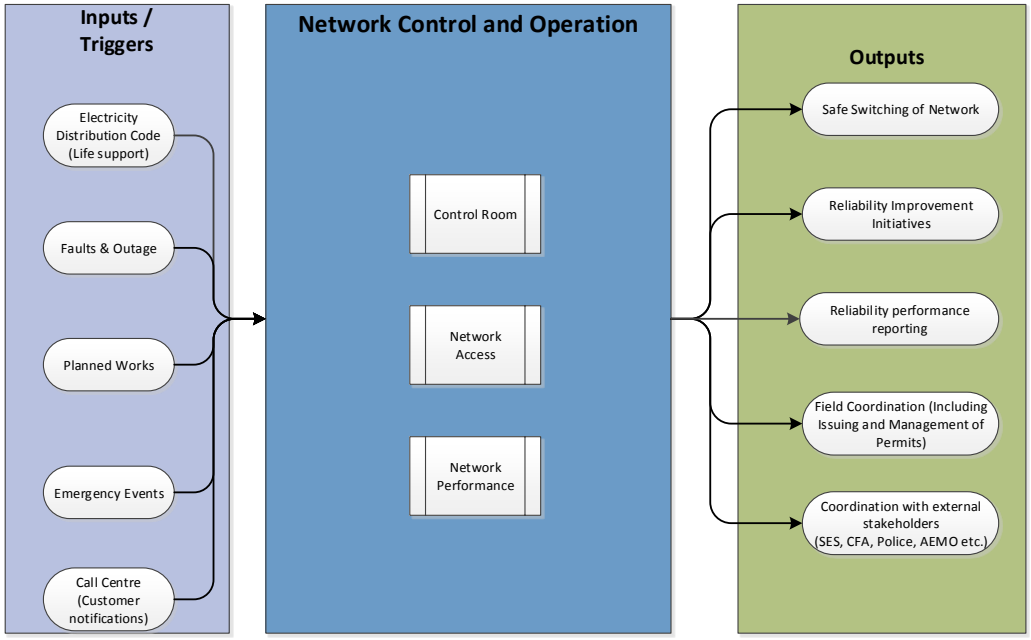


Figure 4-37 – Network Control and Operations Process Overview

Network control and operations sections are described below.

4.3.3.3 Control (System Control Centre)

System Control Centre (SCC) maintains a 24-hour service and also manages the escalation of response to emergency events.

SCC has many key external interfaces, notably the Australian Energy Market Operator, DELWP, transmission and other distribution companies and Emergency Management Victoria, including the State Control Centre.

The status of electricity network is continuously monitored at the CP-PAL System Control Centre at the sub-transmission, zone substation and some distribution feeder elements using a SCADA system, telemetry systems and remote monitoring / control devices.

SCC is responsible for the day-to-day performance and security of the Electrical Network. This includes ensuring the maintenance of accurate operational records on the system events involving planned and unplanned outages and business wide strategic development of control and operating functional work practices and procedures.

SCC is also responsible for developing and maintaining appropriate contingency plans and whole of business escalation processes and rosters for the Electrical Network.

Network Operations ensures the creation and maintenance of accurate operational records on system events involving planned and unplanned outages and accuracy of the Distribution Management System (DMS) network model.

Network Control is also responsible for the response to network emergencies, consistent with the Event Command Organisation Manual[135]. The business will scale resource levels to manage significant events. Refer section 4.2.1.1 Emergency Preparedness and Response of this ESMS for further information.

DMS

The Distribution Management System is a single state of the art software system to efficiently and safely manage the day to day operation of the Electrical Network, today and into the future, which:

- Consolidates disparate systems and provide a single real time network model for management of operations on the Sub Trans and distribution networks across CP-PAL
- Integrates real time SCADA data onto the network model to provide clear feedback and situational awareness
- Integrates SCADA control of devices into network model to ensure clear representation and minimize risk of error
- Allows for information recording to be overlayed onto the network model, and safety logic to be integrated into switching operations to minimise the associated risk
- Provide tools to manage the creation, review and execution of switching instructions
- Interfaces with the corporate Outage Management System to ensure recording of system outages
- Provide a platform to leverage off future smart grid initiatives, including utilization of smart meter data and analytics

The strategy for the application and future application of the DMS will be described within the Network Operations and Utilizations strategy. Refer Appendix 16.

The Operations Procedures manual contains procedures for utilization of the DMS as part of network switching where applicable.

CP-PAL has recently deployed Fault Detection, Isolation and Restoration (FDIR). FDIR is a software module to automate switching of the electricity network in response to the identification (from a SCADA event) of a network outage.

The system will perform all the same checks and conduct switching just like a human operator but will action switching automatically resulting in the number of customers off supply reducing sooner. In many cases sustained outages are transferred into momentary (<60 sec) outages. FDIR can only be deployed where network assets provide the functionality to facilitate

[135] Event Command Organisation Manual – 13-40-M0002

automated switching. This means that FDIR has only been deployed onto a minority of distribution feeders with the aim of growing the population in the future.

Industry acknowledges FDIR as a foundational step to becoming a "Self-Healing Network".

CP-PAL introduced FDIR after undertaking the Formal Safety Assessment to ensure that the risk levels are not elevated as a result of introducing the FDIR.

Unplanned Outage & Fault Response

Network faults are identified via various inputs including from customers, alarms or from telemetered devices. The System Control Centre then prioritises and responds to the faults via the use of remote control devices and/or the dispatch of fault crews. The priority of fault attendance is to make safe and subsequently restore supply to customers. Repairs to the network are carried out prior to supply being restored to the faulted section. To minimise the number of customers affected by supply outage during HV faults, the network may be switched to isolate the faulted section and supply safely restored via alternative means.

The collection of the following documents covered by the scope of the Unplanned Outage Management Policy[136] satisfies this requirement:

- Manage Network Faults Procedure[137]
- Fault Dispatch Guideline[138]
- Manage Fault Follow-up and Repair Guideline
- Livewire procedures for unplanned outages
- Operations Procedures Manual[139]

The Fault Management Governance Group, which has representatives from the senior management of Electrical Networks, PNS, Customer Services and Information Technology, is responsible for the application of this policy, along with any employee or contractor involved in the rectification of Network Faults.

Fault Response

Network faults are monitored, accepted, dispatched and repaired according the Manage Network Faults Procedure. The outcome of this procedure is to proactively manage risk the public and employees and to minimise customer minutes off supply.

The Faults Dispatch Guideline describes how faults and other miscellaneous jobs are to be managed to meet the following objectives:

- Safety of the public and our workforce
- Customer satisfaction

[136] Unplanned Outage Management Policy – JEQA4UJ443MT-148-37

[137] Manage Network Faults Procedure – JEQA4UJ443MT-149-83

[138] Fault Dispatch Guideline – JEQA4UJ443MT-149-543

[139] Operation Procedures Manual - JEQA4UJ443MT-185-11385

- Supply reliability and quality
- Financial constraints

The Dispatcher is accountable for managing the trouble order dispatch priority for both Networks, and assigning appropriate response crews to meet the above objectives.

A defect notice approach is used to advise customers of installation defects. The customer outage impact is recorded and reported upon. Where an event requires escalation, (such as a major storm) the business moves into a heightened mode of awareness, resourcing and operation.

Planning and preparation for abnormal operation

The control centre is manned 24/7 and is the first contact point for any abnormal operation of the network. The voice communications systems available to the control centre include:

- Fixed line telephony
- Mobile telephony
- TMR radio

Emergency services have direct lines into the 24/7-dispatch room that bypasses the customer contact centre. The System Control Centre has a full system backup, which allows for the establishment of a separate System Control Centre, in the event of complete system failures. In the event of loss of electrical supply, system control centres have UPS and diesel generator back up supplies. UPS and diesel generator undergo routine maintenance and testing. The control centre telephony system is fully redundant to allow for continual operation in the event of system failures.

In the event of system communications failure, network relays will continue to protect assets and ensure the safety of the network autonomously.

Contingency Plans

Where normal network configuration does not allow sufficient redundancy to supply customer for a single unplanned event, contingency plans are developed and maintained in line with the requirements of the Essential Services Commission's Electricity Distribution Code Section 3.1. Currently there is the following number of specific plans to manage these risks:

Risk item	Powercor	CitiPower
Zone substation transformer	33	11
Sub-transmission line	9	6
Terminal station transformer	5	1

Table 4-2 – Operational Contingency Plans

Load shedding is initiated to protect assets or network health. This is required due to local constraints or due to a request from the market operator or transmission company (AEMO / TNSP). This is described in the Load Shedding Guideline[141].

Escalation availability rosters are maintained for where unplanned events reach a higher than BAU state. The escalation team overviews the event and responds to requests from various internal and external parties including Government and oversight bodies.

The escalation process is described in the Event Command Organisation Manual [142]and section 4.2.1.1 Emergency Preparedness and Response of this ESMS.

Emergencies

Our Crisis Management Plan[143] is the framework document describing the Business's policy, guiding principles, resourcing and sustaining the processes of emergency preparedness, response and recovery.

This Manual also provides a guide to, and brief descriptions of, the integrated hierarchy of other manuals and plans, which together form the written elements of the Business's Crisis Management Plan.

These guide the effective and timely response of the organisation and its personnel to emergencies, which affect or have the potential to impact on the operation of the network, the health and safety of its personnel, the public or major asset groups.

Comprehensive operational instructions are detailed in the CP-PAL Operations Procedures Manual[144]. Whilst other field staffs undertake most manual switching, the network operations group relies on a number of full time operators and part time operator planners.

4.3.3.4 Network Access

Controls are in place to manage safe access to work on, near or in the vicinity of the CP-PAL Distribution and Sub Transmission Networks.

The Authorisations and Access Authority processes relevant to Network Access are shown in Figure 4-38 below.

[141] Load Shedding Guideline – JEQA4UJ443MT-149-213

[142] Event Command Organisation Manual – JEQA4UJ443MT-154-111

[143] Crisis Management Plan – JEQA4UJ443MT-154-386

[144] Operations Procedures Manual – JEQA4UJ443MT-185-11385

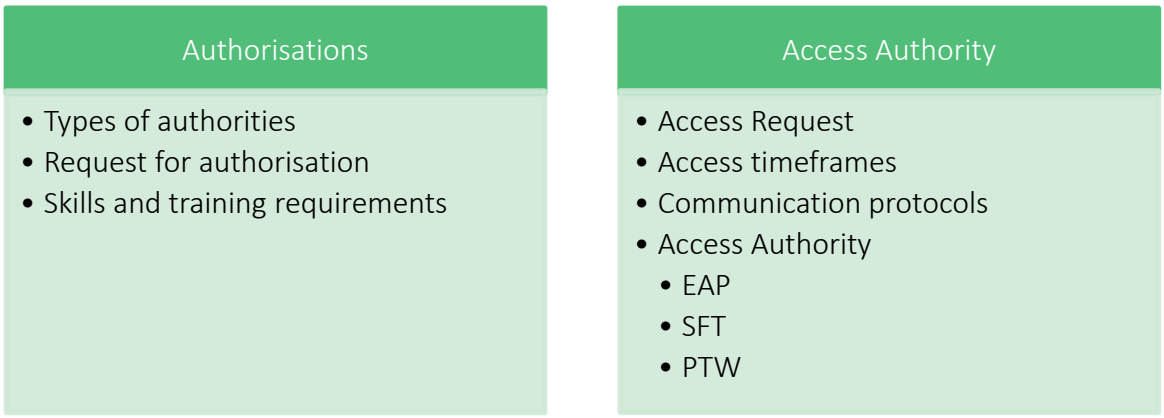


Figure 4-38 – Network Access – Authorisations and Access Authorities

Authorisations

Only suitably authorised persons can apply for access to the CP-PAL Networks.

Persons are authorised via the manage network authority request[145].

The VESI Skills and Training matrix[146] lists the roles for the VESI (including CP-PAL) and their applicable qualifications, training and authorities.

The authorities, which apply to CP-PAL, include VESI and CP-PAL specific authorities (refer to Operations Procedures Manual[147]):

- VESI - Make Application For (MAF)
  The attainment of the VESI Make Application For allows the holder to make application for specific works to be performed on the CP-PAL Networks and ensure that adequate planning for electrical and other safety requirements are met.
- VESI - Enter Enclosures
  The attainment of the VESI Authority to Enter Enclosures allows the holder to enter Distribution and Zone substations.
- VESI - Receive Access Permits
  The attainment of the VESI Authority to Receive Access Permits allows the holder to receive Electrical Access Permits on either Distribution and/or Sub Transmission apparatus. The Authority holder shall ensure that an Electrical Access Permit contains an accurate description of the apparatus covered and the precise description of the isolations, earthing, special notes/precautions and warnings to allow work to be safely carried out.
- VESI - Sanction for Test
  The attainment of the VESI Receive Sanction for testing allows the holder to access high voltage electrical apparatus for the purpose of carrying out electrical tests which will raise

[145] Manage Network Authority Request – JEQA4UJ443MT-148-35
[146] VESI Skills and Training Matrix – http://www.vesi.com.au/index.php/skills-training?acc-1=1
[147] Operations Procedures Manual – JEQA4UJ443MT-185-11385

the primary conductor to a voltage that has the potential to produce currents hazardous to the human body. A VESI Receive Sanction for testing Authority will allow the holder to make electrical apparatus alive via test equipment or by other means.

VESI - High Voltage (HV) switching authorities:

- RSO

  Authorised to carry out high voltage switching, earthing & issue electrical access authorities under the direction of System Control Centre on distribution overhead and ground type substations, spur and SWER lines and associated apparatus. Excluding metal clad switchgear and underground network.

- DSO

  Shall hold a current VESI – RSO authority and has been the holder of a VESI – RSO for a period of 12 Months prior to being presented as a candidate or have documented approval from the operating authorities authorisations Team Leader or Delegate. Authorised to carry out high voltage switching, earthing & issue electrical access authorities under the direction of System Control Centre on All Distribution O/H field apparatus and Sub Transmission Earthing

- DS

  Shall hold a current VESI - DSO authority or has held a RSO authority with a geographical restriction of CitiPower and have been the holder of the authorities for a period of 6 Months prior to being presented as a candidate or have written approval from the operating authorities Authorisations Team Leader or Delegate

- ZSS

  Authorised to carry out high voltage switching, earthing & issue electrical access authorities under the direction of System Control Centre on all Sub Transmission & Distribution apparatus within Zone substation. Including 66kv Line Regulators where specifically inducted

- TSF

  Authorised to carry out high voltage switching, earthing & issue electrical access authorities under the direction of System Control Centre on all CP-PAL controlled apparatus in Terminal Stations

CP-PAL specific Authorities are listed below (refer to Operations Procedures Manual[148]):

[148] Operations Procedures Manual – JEQA4UJ443MT-185-11385

LV Switching

- Install Mobile Generator Set Synchronised LV Genset
- Install Mobile Generator Set Synchronised HV Genset
- PAL - Suppression of ACR
- Switching Control Operations (SCC) Controller
- RSO - Restricted Switching Overhead (EP&T)
- DSU - Distribution Switching Underground

Network Access

A Network Access Requests (NAR) is required to obtain safe access to carry out work on either the CitiPower or Powercor Electrical Distribution Networks.

A Network Access Request (NAR) is required for all jobs where access is required to High Voltage (HV) apparatus and/or Low Voltage (LV) apparatus or for work to be performed in the vicinity of HV apparatus.

For work where a NAR is required, the Authorised Applicant shall have a clear and complete understanding of the work to be done, the means of doing it, together with knowledge of the physical arrangement of the electrical apparatus and any existing or potential hazards.

Only suitably authorised persons can apply for access to the CP-PAL Networks.

There are required lead time periods for NAR which are listed below:

- Quick Access - same day
  Any job that does not require a switching instructions
- Simple Access - 2 Clear Working Days
  Any jobs that does not require a switching instruction but will have a Vicinity Access (VA) on issue or working on in-service equipment
- Planned Access - 10 Clear Working Days
  Jobs requiring preparation of switching instructions and or customer notifications

Network Access Requests can be submitted 24 hours a day/7 days a week via either phone, Non Verbal Communication (NVC) or Switching Request Register (SRR) as required.

Refer Network Access Request (NAR) Requirements guidelines[149].

[149] Network Access Request (NAR) Requirements – JEQA4UJ443MT-149-563

The following Access Authorities procedures appropriate to various section requirements for access to electrical apparatus are as follows:

Authority		Purpose
EAP	Electrical Access Permit	To allow work, in a dead condition, on electrical apparatus that is capable of being energised.
LV EAP	LV Electrical Access Permit	Issued by a suitably trained person when isolation & bonding of LV supply is carried out.
PTW	Permit to Work	Issued to a person who does not work for or is contracted by the asset owner and is required to perform work near or in the Vicinity of the networks electrical apparatus. Note! May be issued in conjunction with an EAP.
SCAP	Statement of Condition of Apparatus - Plant	Are required on apparatus controlled by HV customers or other operating authorities
VSCAP	Verbal Statement of Condition of Apparatus - Plant	Verbal Statement of Condition of Apparatus and Plant used between operating authorities.
VA	Authority to Work or use Mobile Plant in the Vicinity of Electrical Apparatus.	Issued to CitiPower Powercor personnel, (including contractors under the control of CitiPower Powercor personnel), for work in the Vicinity of electrical assets on the Distribution system and in Zone and Terminal stations.
SFT	Sanction for testing	Issued when electrical testing of electrical apparatus is required.
SILV	Statement of Isolation of Customer Low Voltage Supply	Issued to a customer or REC when isolation of a customer's LV supply is reliant on a Distribution Network assets.

Table 4-3 – Access Authorities procedures

The type of access authority appropriate to a particular requirement for access to electrical apparatus is decided by Operations Planning after assessing the works required, described in the application.

Authorised Network Access allows for work on the Network. System Configuration Changes, including additions, and Standard Operating Instructions are captured within Network Access requirements.

Operations Procedures Manual[150]

The Operations Procedures Manual recognises that CP-PAL employees and contractors are required to work on, near or in the vicinity of the CP-PAL Distribution and Sub Transmission Networks.

The purpose of this document is to provide a common understanding for operational activities across the organisation.

[150] Operations Procedures Manual – JEQA4UJ443MT-185-11385

The Operations Procedures Manual[151] covers the following:

- Authorisation – required authority categories and functional restrictions required by CP-PAL employees and contractors
- Network Access – types of access authorities appropriate for access to high voltage and low voltage electrical apparatus under different operational considerations
- Access Precautions – the precautions that are needed to allow safe access to assets
- Co-Ordination of Operations – the method of co-ordinating and recording switching operations on the CP-PAL networks for planned and unplanned outages
- Switching – safe switching requirements of electrical equipment with co-ordination by the System Control Centre
- Earthing – safe earthing of electrical apparatus
- Reporting – reporting of defective electrical apparatus and alarms

4.3.3.5 Reliability and Network Performance

A team of Asset Performance Officers have identified targeted reliability improvements. These are then scoped and a business case is created to determine the projects viability and priority.

Reliability initiated projects are targeted to address specific issues that generally have a high likelihood of occurrence and utilise historical outage data to quantify the reliability improvement. Some examples of targeted reliability projects are:

- Installation of automated protection and switching to minimise the extents of an outage
- Installation of animal mitigation devices to reduce the number flashovers caused by animals
- Installation of covered conductor /underground to mitigate the impact of tree related faults
- Installation of fault indicators to locate the faulted feeder segment more rapidly, and the
- Replacement of targeted wooden HV cross-arms to minimise pole fire related outages

Risk based projects are usually targeted to address issues that generally have a low likelihood of occurrence whose consequences are generally very high. Some examples of targeted risk projects are:

- Catastrophic Zone substation failure
- Significant loss of supply to the CBD
- Major Bushfires
- Enforced load shedding (demand management)
- Sub Transmission failures, particularly radial systems

Reliability improvement projects are developed using the assessment and evaluation of reliability enhancement projects framework guide[152]

[151] Operations Procedures Manual – JEQA4UJ443MT-185-11385

4.3.3.6 Governance of Network Operations

Control and operations use the comprehensive suite of Operations Procedures Manual[153] to manage activities that minimises risk. These procedures have been developed and maintained from the knowledge obtained through experienced people, strict application of industry codes and specific assessment through incident investigations and learnings.

Risks and hazards may also be identified during strategic and operational process with a specific item or practice. This is reported to the System Control Centre who attaches 'warning tags' to the equipment shown on their network diagrams. The physical item of equipment will also be tagged.

Where a hazard applicable to a class of device is found, all devices of that type are identified and tagged in the System Control Centre distribution management system. This equipment may not always have a physical tag fitted. Where a class of devices is affected, a safety alert is issued to ensure the wider business is alerted to the hazard.

When a hazard is reported, the System Control Centre will typically assess the risk based upon known failure modes (i.e. switches which have not latched correctly) and shall record the defect accordingly. Tagging the individual piece of equipment, both onsite and in the System Control Centre is undertaken to make relevant persons aware of a hazard. Refer to PSCC Reporting of defective equipment[154].

All operations on the network are directed by the System Control Centre to maintain visibility of these hazards. Refer to Recording System Information[155].

Prior to the introduction of new equipment, it is reviewed by the Operations Committee to mitigate any associated hazards and must adhere to the process outlined in the procedure for Introducing New Plant and Materials[156].

Where a hazardous practice (rather than equipment) is found it is referred to the Operational HSE Improvement team.

CP-PAL has functional operations committee[157]. This committee advise the business on the following issues:

- Review switching incidents

  A switching incident is any unintended physical occurrence arising while carrying out or intending to carry out a switching program.

  Examples include:

[152] Reliability enhancement projects framework guide – JEQA4UJ443MT-150-367

[153] Operations Procedures Manual – JEQA4UJ443MT-185-11385

[154] PSCC Reporting of defective equipment – JEQA4UJ443MT-150-206

[155] Recording System Information – JEQA4UJ443MT-149-147

[156] New Plant and Materials – JEQA4UJ443MT-160-222

[157] Operations Committee Charter

- Network outage or reclose operation;
- Over/under voltage;
- Injury to staff or public;
- Equipment damage; or
- Incorrect primary switching equipment being operated even if none of the above outcomes result

  Once a switching incident has occurred, an investigation is initiated. The potential severity of the incident will determine the level of investigation. The investigation report will typically include a number of action items that are monitored in Cintillate the CP-PAL HSE incident reporting systems.

- Review faults and reliability targets including feeder performance
- Field operator audits
- Network reliability programs effectiveness review
- Review permits
- Review the introduction of new Distribution Apparatus or Designs
- Review of Operations Procedures
- Develop a consistent approach to operating standards & practices across CP-PAL Networks
- Review of non-standard or innovative network designs

CP-PAL has operations committee[158] in place where the findings of the field operating audits, identified hazards and operating incidents are reviewed. Post these reviews corrective actions are developed and implemented.

4.3.4 Asset Maintenance

Asset maintenance is one of the controls in managing network safety risks. CP-PAL maintain assets to perform safely and reliably. If assets are not maintained effectively, they pose a risk of failure, which leads to safety and reliability consequences.

[158] Operations Excellence Committee Charter

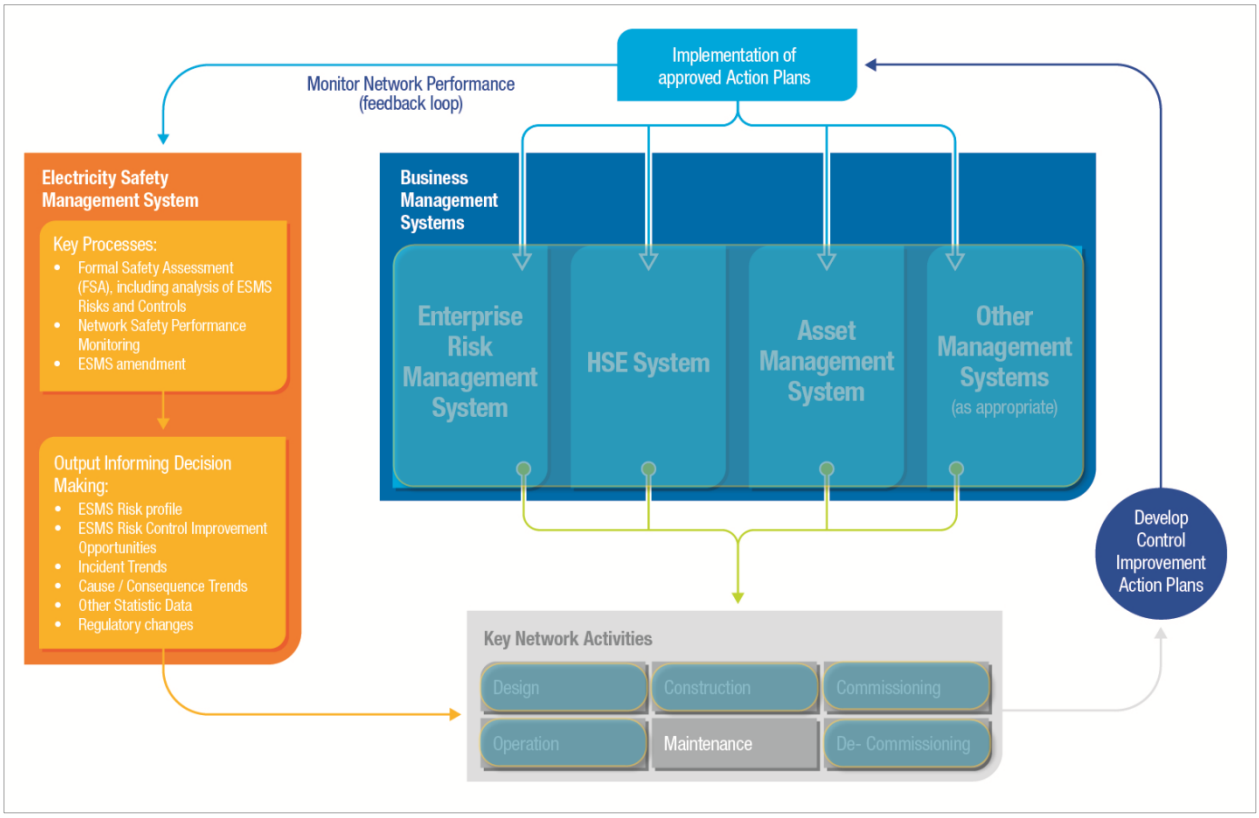


Figure 4-39 – ESMS Integration with Maintenance

Asset failures are triggered due to a number of factors, which include:

- condition
- inherent manufacturing defects
- deterioration
- 3rd party impacts
- severe weather events etc.

CP-PAL utilises a suite of Asset Class Strategies, Asset Maintenance Policies and Work Instructions to effectively maintain its assets in safe and reliable manner.

Our asset maintenance commitments and summary of how these commitments are achieved are further discussed below:

4.3.4.1 Asset Maintenance Commitments

To further complement our Asset Management commitments as discussed in section 4.2.3.1 of this ESMS, CP-PAL has planned to undertake the following targeted programs:

- CP-PAL will maintain its assets in accordance with document asset maintenance policies.
- CP-PAL will inspect all the Dog Bone termination LV services. Refer Appendix 16.
- CP-PAL will maintain the ground clearances of the LV services using a risk-based approach in accordance with our Services Asset Maintenance Policies.

- CP-PAL will action defects identified through asset inspections in accordance with asset maintenance priority policy[159].

These commitments are further detailed in sections 4.3.4.2– 4.3.4.11 demonstrating **how** each are met.

4.3.4.2 Asset Maintenance Process Overview

The CP-PAL asset management framework requires that all network physical assets making up the electricity distribution network are maintained, refurbished or replaced in accordance with the documented Asset Management Plans.

CP-PAL assets are managed and maintained by the Asset Management division. Asset Management division utilises various inputs such as Asset Management Framework, CBRM, ESMS, performance monitoring, budget and industry forum considerations to undertake detailed analysis to develop / update its:

i. Asset Management Plans
ii. Asset Management Policies
iii. Work Instructions
iv. Maintenance Works (Poles & Wires Assets, Plant and Stations Assets)

Figure 4-40 below illustrates the asset maintenance process overview.

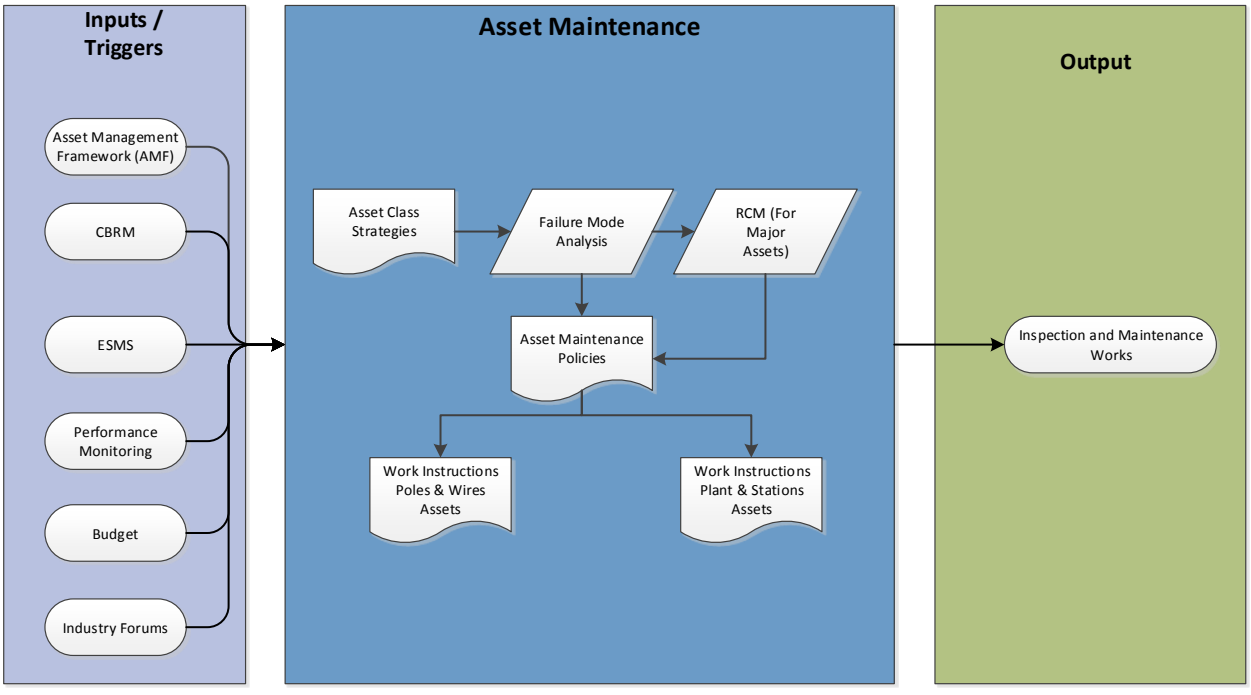


Figure 4-40 – Asset Maintenance Process Overview

[159] Network Asset Maintenance Priority Policy – 05-C001.A-025

Each of the items of the Figure 4-40 is further discussed below:

4.3.4.3 Inputs

All the below mentioned inputs are considered as part of development and review of asset management strategies.

Asset Management System Framework

The Asset Management System Framework[161] is designed to manage our network assets to ensure we deliver a reliable and safe supply of electricity in accordance with the business needs.

The Asset Management System Framework governs the CP-PAL Asset Management system.

ESMS

The outputs of the Electricity Safety Management Scheme (ESMS) in the form of asset class risk levels, consequences, likelihood, control improvement and action plans are used as an input for the development and reviews of asset management policies.

ESMS outcomes inform asset management plans by identifying opportunities to achieve desired network safety outcomes.

For example, the output of ESMS assessment leads to the improvement of service pit lids controls to reduce the risk associated with trips and falls being experienced by the members of the public. Refer section 4.2.2.1 for details.

CBRM

Condition Based Risk Management (CBRM) is an approach adopted by CP-PAL for evaluating the decision making of maintaining and replacement of the most critical primary electrical plant and equipment e.g. zone substation transformers and circuit breakers.

As illustrated in Figure 4-41 below, CBRM provides information that assists in the decision-making process for maintaining and replacement of assets.

Figure 4-41 – Condition-Based Risk Management

[161] Asset Management System Framework – JEQA4UJ443MT-150-27597

CBRM is a method, which enables CP-PAL to quantitatively define:

- Asset condition – Health index
- Asset Performance – Probability of Failure (POF)
- Risk – Combination of POF and Consequences of failure (COF) including safety consequence

Different investment strategies that include maintenance, intervention for life extension (for e.g. refurbishment, reinforcement) are techniques used to achieve an optimum outcome.

Risk profiles of the extended life assets are monitored and actions are implemented accordingly.

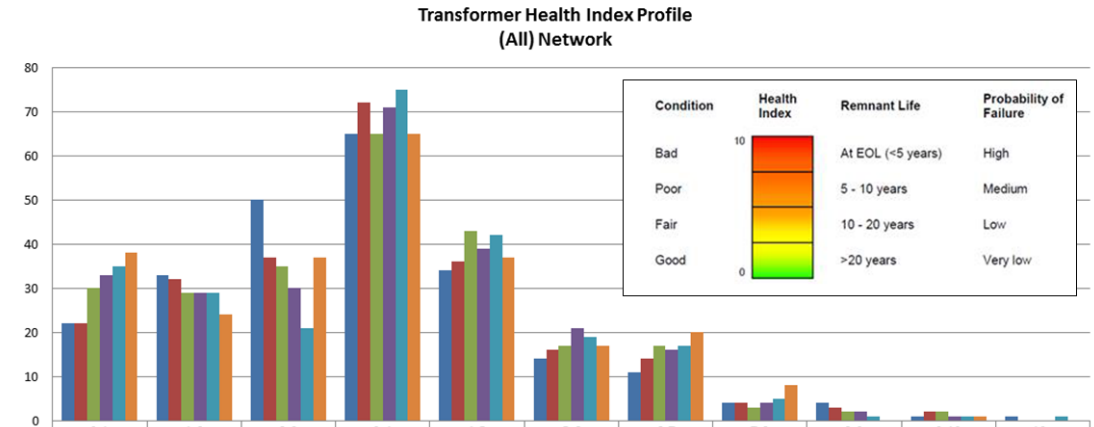
A *Network Health Index* using Condition Based Risk Management (CBRM) methodology for zone substation transformers and circuit breakers is used to monitor the status and condition of these key items of plant over time. These health indices are shown below.

The Health Index (HI) represents the extent of degradation as follows:

- Low values of HI (in the range 0 to 4) represent some observable or detectable deterioration at an early stage. This may be considered as normal ageing i.e. the difference between a new asset and one that has been in service for some time but is still in good condition. In such a condition, the *Probability of Failure* (PoF) remains very low and the condition and PoF would not be expected to change significantly for some time.
- Medium values of HI, in the range 4 to 7, represent significant deterioration, degradation processes starting to move from normal ageing to processes that potentially threaten failure. In this condition, the PoF, although still low, is just starting to rise and the rate of further degradation is increasing.
- High values of HI (>7) represent serious deterioration, advanced degradation processes now reaching the point that they actually threaten failure. In this condition, the PoF is significantly raised and the rate of further degradation will be relatively rapid.

Network Health Index – ZSS Transformers

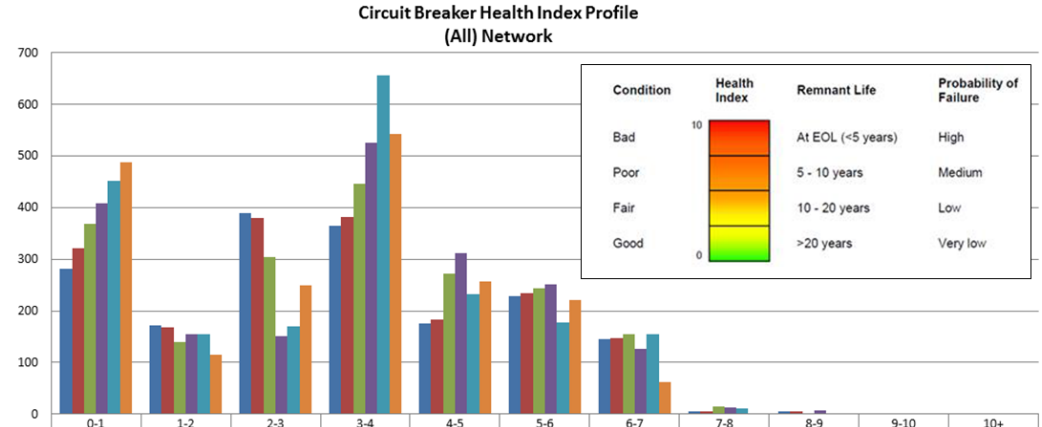
CitiPower and Powercor combined



	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	10+
2011	22	33	50	65	34	14	11	4	4	1	1
2012	22	32	37	72	36	16	14	4	3	2	
2013	30	29	35	65	43	17	17	3	2	2	
2014	33	29	30	71	39	21	16	4	2	1	
2015	35	29	21	75	42	19	17	5	1	1	1
2016	38	24	37	65	37	17	20	8		1	

Network Health Index – ZSS Circuit Breakers

CitiPower and Powercor combined



	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	10+
2011	282	171	389	364	175	229	146	5	6		
2012	322	167	380	382	184	235	147	6	6		
2013	368	140	304	446	272	243	154	14			
2014	409	154	150	526	311	252	126	13	7	1	2
2015	451	155	169	657	232	177	155	10			
2016	488	115	250	542	257	220	62				

The two graphs show that the majority of our transformer and circuit breaker assets are in the low probability of failure category.

CBRM is currently used for the following assets

- ZSS Transformers (CP-PAL)
- ZSS Switchgear (CP-PAL)
- HV Cables (PAL)

The models are updated annually and assist in determining key timing for asset replacement using health index and delta risk

With Copperleaf we are expanding the models LV Circuit Breakers, HV Switchboards and Ring Main Units (RMU).

Budget

- OPEX and CAPEX budgets available via the annual budgeting processes are considered for introducing new technology or changing any of the existing maintenance practices. Refer section 4.2.4.2 of this ESMS for additional financial planning & approval information.

Performance Monitoring

Performance monitoring is achieved via asset failure investigations[162]

The primary purpose of an asset failure investigation is to:

i. identify the root cause of an asset failure and the contributing causal factors
ii. identify the controls that are being applied to manage associated asset performance
iii. identify opportunities to improve on the controls

Asset failure investigations are undertaken in accordance with the principles described in Australian Standard AS62710: 2016 Root cause analysis (RCA).

Asset failure investigations follow the type 1 objectives for RCA, as per AS62710:2016, which focus on analysing an event (an asset failure), using only verifiable information.

Root cause analysis techniques (e.g. why method or cause trees) are applied and selected as appropriate to drill down to where identified causal factors enable the appropriate asset management policy and/or standard to be identified. Identifying the relevant asset management policy and/or standard enables a review of the control(s).

Where opportunities to improve are identified the investigation will detail these recommendations.

- Performance data via asset failure incident trends analysis, defect trending analysis, and network safety incident trends analysis.

[162] Asset failure investigations framework – JEQA4UJ443MT-150-27384

Asset failure investigations are triggered via the trigger levels of the following as noted in Figure 4-39:

- Fire Ignition
- Electric Shock / Injury
- Property Damage
- Interruption of Supply

- Incident Consequence – Figure 4-42 illustrates the incident consequence levels, Overview & Objective and Trigger Levels.

1	Fire ignition	ElectricShock/ Injury	Property Damage	Interruption of supply
Overview & objective	Incidents involving ground fire ignition *[Meet the requirements of critical control 0338 in the risk management of catastrophic bushfires]*	Incidents involving shock or injury to employees and the public *[Meet the requirements of critical control 0338 in the risk management of third party interactions with our assets]*	Incidents involving damage to company and third party property *[Meet the requirements of critical control 0338 in the risk management of failure of network assets]*	Incidents involving significant reliability of supply disruption *[Meet the requirements of critical control 0338 in the risk management of failure of network assets]*
Trigger level	1. A potential class 3 incident (and above) involving ground fire, or 2. Any ground fire in BCA , or 3. Any ground fire in HBRA caused by overhead conductors or FOLCB's (top 2 fire starting assets)	1. Any potential class 3 incident (and above) involving shock or injury, or 2. A regulatory reportable incident threshold reached	1. Any potential class 3 incident (and above) involving property damage, or 2. The Network Major Event Report threshold reached (attributed to major plant failure)	1. A potential class 3 incident (and above) involving supply reliability, or 2. The Network Major Event Report threshold reached
Requested by	1. Incident Manager (IM) / Lead Incident Investigator (LII) 2. Network Safety	1. Incident Manager (IM) / Lead Incident Investigator (LII) 2. Network Safety	1. Incident Manager (IM) / Lead Incident Investigator (LII) 2. Network Operations	1. Incident Manager (IM) / Lead Incident Investigator (LII) 2. Network Operations
Estimate per annum	12	6	6	6

Figure 4-42 – Asset Failure Investigation Incident Consequence Triggers

- Asset Performance - Figure 4-43 illustrates the asset performance overview & objective and Trigger Levels.

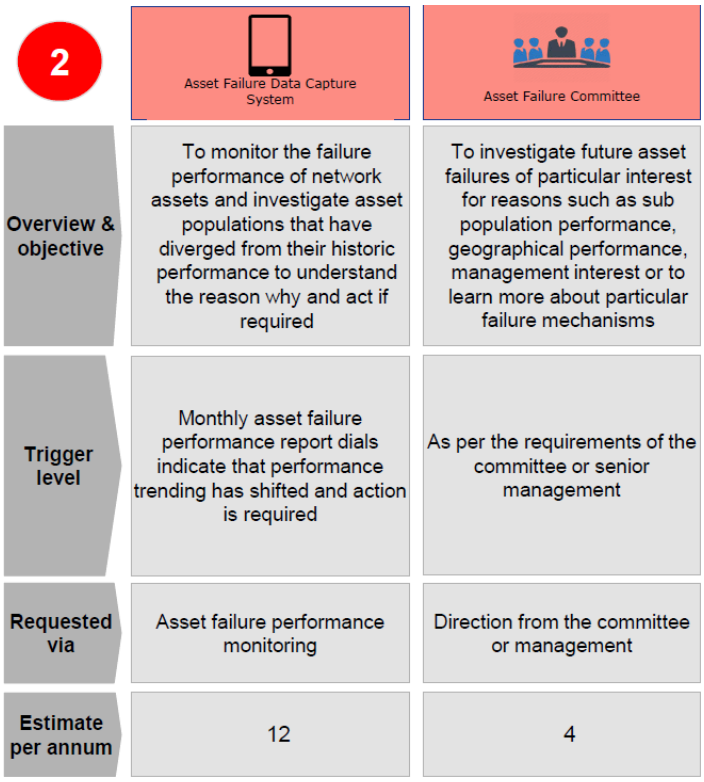


Figure 4-43 – Asset Failure Investigation Incident Consequence Triggers

Industry Forums

Advice from relevant industry forums is considered during the development of the Asset Management Plans

4.3.4.4 Asset Class Strategies

All the above mentioned inputs under section 4.3.4.3 are considered during the development of Asset Class Strategies to effectively manage the assets to achieve asset management objectives.

Asset Class Strategies (ACS) document the management strategies for the major asset classes being:

- Poles and towers
- Pole top structures, HV fuses and surge arresters
- Overhead conductors
- Underground cables
- Zone transformers
- Distribution substation plant miscellaneous
- Public lighting
- Zone substation plant miscellaneous

- Distribution transformers
- SCADA and communications
- Zone switchgear
- Protection and control
- Property and facilities
- Metering
- Distribution switchgear
- Service lines

Each ACS is formed on the review and analysis of the required performance, including reliability and quality of supply, risk profile including the outcomes of the formal safety assessment, functionality, availability and safety.

The ACS drive maintenance policies, inspection plans, condition monitoring and work instructions. AMPs are reviewed every five years, unless otherwise specified.

Example ACS and their contribution to the mitigation of the risks associated with bushfire, electric shock and physical injury, property damage and supply interruption are described in Table 4-4 below:

Asset Management Plan	Description	Risks Mitigated
Overhead Lines Asset Class Strategy	Drives the inspection and maintenance of overhead lines in a safe and reliable manner.	
Secondary Systems Equipment Asset Class Strategy	Drives the inspection and maintenance of secondary systems.	
Distribution Substations & Switchgear Asset Class Strategy	Drives the inspection and maintenance of distribution substation transformers and switchgear.	
Zone Substations Asset Class Strategy	Drives the inspection and maintenance of zone substations assets.	
Underground Cables Asset Class Strategy	Drives the maintenance of underground HV cables.	

Table 4-4 – Asset Management Plans Sample

Each Asset Class Strategy is supported by a corresponding Asset Management Plan, which details how the asset management objectives and strategies will be prioritised and delivered.

4.3.4.5 Failure Mode Analysis

Failure Mode Analysis identifies all the known and potential failure modes. This generally includes identification of the following:

- Function of the asset
- Failure types
- Potential impacts of failure
- Potential causes of failure

Outcomes of Failure Mode Analysis feed into RCM Analysis for major distribution assets and into Asset Maintenance Policies for all other assets.

4.3.4.6 RCM Analysis

RCM analysis is an internationally recognised and widely used methodology used to determine a maintenance strategy for a particular class of asset that is optimised to deliver performance requirements.

CP-PAL applies a tailored RCM methodology to high value, high risk and/or high impact (reliability, community) asset classes.

Tailored RCM methodology determines the parameters of time and condition-based maintenance activities for selected major asset groups.

A team of subject matter experts is assembled comprising CP-PAL personnel and industry personnel (including suppliers, other authorities, research bodies) to undertake the analysis.

The RCM process is used to determine the following:

- What are the functions of the equipment?
- In what ways can it fail?
- What causes it to fail?
- What happens when it fails?
- Does it matter if it fails?
- Can anything be done to prevent the failure?
- What do we do if we cannot predict or prevent the failure?

In summary RCM analysis enables CP-PAL to determine what must be done to ensure that our physical network assets continue to operate at their intended performance levels.

The example below demonstrates how CP-PAL applied RCM analysis to outdoor HV air break switchgear.

The RCM analysis for outdoor HV air break switchgear identified the failures modes and consequences for each type of switch and variant of installation. The consequences were analysed under the operating context of a pre-operational check being performed prior to operation, which impacted the analysis by allowing potential safety consequences becoming

operational consequences where a defect was deemed to be reliably and consistently identified by a HV Operator.

Most of the failure modes were identified as being of a random pattern with no sign of age related patterns. Failure modes could be categorised by consequence as follows:

- Failure modes that lead to an outage without the switch being operated (unassisted failure), often with the associated possibility of a fire (due to arcing/sparking).
- Failure modes that lead to a switch being completely inoperable without safety risks.
- Failure modes with safety risks during operation that will be identified during the pre-operational check, leaving only operational consequences.
- Failure modes with safety consequences during operation that cannot always be identified during the pre-operational check.

A large number of the failure modes that fall under the first category were identified to be managed through other inspection programs, such as the Thermographic Inspection program or the Asset Inspection Program (Pole Inspection).

Most operational consequences as a result of a failure mode falling under the second or third category generally did not have a significant enough impact to justify targeted maintenance activities scheduled at the estimated useful life of the components.

The majority of the maintenance program was aimed at managing the fourth category.

The following Table 4-5 and Table 4-6 provide with the summary of the activities determined by the RCM program for outdoor switchgear; the first table, by program and the second table by switch type.

Task	Applies To	Cycle	RCM Task Type	Tasks
Outdoor				
Inspection & maintenance program	All outdoor switches	20 years	Scheduled restoration task / On-condition task	► Close visual inspection from bucket for damage or deterioration ► Open/close operation ► Clean and grease main contacts ► Check and tighten mechanical linkages ► Check for drive shaft or operating shaft flex ► Re-align switch (contact penetration, flicker blade, arc chute, etc.) ► Tighten all mechanical hardware and lubricate if required
			Scheduled discard task	► Replace EziBreak/DuoGap expulsion interrupters
			Scheduled discard task	► Replace wooden operating shafts
Earth test program	Outdoor switches with earthed handles	4 years	On-condition task	► Test earth impedance and repair as required
Thermographic inspection	All CitiPower switches, Powercor switches where current is >50A.	1 year	On-condition task	► Identify and repair hot connections as required
Asset inspection program	All outdoor switches	2.5/5 years	On-condition task	► Visual inspection of all pole mounted assets from ground for damage ► Ground clearance check of switch handle
Replacement program	Vertically mounted outdoor switches with DuoGap or EziBreak interrupters	-	Redesign task	► Replace with horizontal switch or retrofit arc chute ► CRO tag, defect report as found

Task	Applies To	Cycle	RCM Task Type	Tasks
New maintenance package	New replacement program		Existing maintenance items under different policy	➢ Operating context change

Table 4-5 – Failure Mode Analysis for Outdoor Switchgear

The following table shows which activities will be applied to each type of switch:

Outdoor Switch Type	Applicable Maintenance Activities
Gevea GDS (stick operated)	➢ Inspection & maintenance program (20 years) ➢ Thermographic inspection program (1 year, not all switches) ➢ Asset inspection program (2.5/5 years) ➢ Pre-operational inspection
Stanger PR2/PR3, Taplin D201/D221/D209 – Arc Chutes	➢ Inspection & maintenance program (20 years) ➢ Earth testing program (4 years) ➢ Thermographic inspection program (1 year, not all switches) ➢ Asset inspection program (2.5/5 years) ➢ Pre-operational inspection
Stanger PR2/PR3/USB, Taplin D201/D221 – EziBreak/DuoGap interrupters – Horizontally mounted (USB on normally closed switches only)	➢ Inspection & maintenance program (20 years) ➢ Earth testing program (4 years) ➢ Thermographic inspection program (1 year, not all switches) ➢ Asset inspection program (2.5/5 years) ➢ Pre-operational inspection
Stanger PR2/PR3, Taplin D201/D221 – EziBreak/DuoGap interrupters – Vertically mounted	➢ Obsolete, replacement program
Stanger/Taplin – Flicker Blade	➢ Inspection & maintenance program (20 years) ➢ Earth testing program (4 years) ➢ Thermographic inspection program (1 year, not all switches) ➢ Asset inspection program (2.5/5 years) ➢ Pre-operational inspection
Stanger Unitized Side Break Switches	➢ Obsolete, replacement at inspection (existing policy – bird flashover risk)
66kV Distribution Air Break Switchgear	➢ Excluded from policy scope

Table 4-6 – RCM Activities for Outdoor Switchgear

Outcomes of RCM feed into Asset Management Policies.

4.3.4.7 Asset Maintenance Policies

Outcomes of Failure Mode Analysis, RCM and Asset Class Strategy (ACS) form the basis of developing and updating Asset Management Policies.

Policies outwork the strategic direction provided by ACS. ACSs provide this direction through detailing the management strategies required to meet future asset performance requirements.

All the above mentioned inputs are considered in the development of policies to effectively maintain the assets to achieve asset management objectives. Policies are implemented through procedures and work instructions such as the Asset Inspection Manual that details our asset inspection requirements for poles and wires related assets.

Maintenance Policy Development

Appropriate maintenance actions are determined for failure modes to meet the required performance. This performance is generally expressed as an availability rate for the asset. The maintenance policy for poles includes inspection frequencies, pole treatment frequencies (fungal decay), pole reinstatement, redesign, pole replacement and termite treatment requirements.

Maintenance Policy Implementation

Maintenance plans, policies, tasks and work instructions are captured and managed in the SAP Maintenance Management system. The RCM timing and task outcomes are configured in SAP, which automatically generates time based work orders for inspection and maintenance planning.

Notifications are also created to undertake any required maintenance actions triggered during the inspection process.

Monitoring

Performance of maintenance policies are monitored such as defect and failure rates to ensure effective implementation and verification of expected outcomes.

Maintenance and associated condition monitoring policies are reviewed every five years. A further review may be undertaken should performance not meet expectation.

When new assets are introduced into the network, existing maintenance and condition monitoring plans are reviewed to ensure coverage of the change or new plans are created as appropriate.

4.3.4.8 Asset Maintenance Work Instructions

CP-PAL undertakes the maintenance of assets in accordance with asset maintenance policies requirements that are configured in SAP. Records are managed in the SAP maintenance management system, which is customised to include all maintainable items. SAP automatically generates time based and defect rectification work orders for maintenance activities.

CP-PAL maintains its assets per the following main groups work instructions:

i. Asset Maintenance – Poles & Wires

CP-PAL poles and wires assets include overhead lines, metering & services and public lighting asset groups.

These assets are inspected and maintained based on Work Instructions driven by relevant Asset Management Policies.

Asset inspection plays a critical role in asset verification and asset condition assessment to ensure network assets are maintained in a safe and reliable manner.

The key role of asset inspection is to identify hazards and defects and have them reported in accordance with asset management policies.

Requirements for inspection of assets and the condition assessment criteria are described in the CP-PAL Asset Inspection Manual[163]. The manual ensures consistent inspection methods are applied and is regularly updated with learnings from the asset inspection process, asset failure investigations and operational experience in managing the assets.

Hazards and defects are reported in accordance with CP-PAL Maintenance Priority Policy[164], which defines reporting, and rectification timeframes.

Defects are also identified through network monitoring via the Network Control Centre, SCADA, AMI and customer calls.

Defect items identified go through a rectification process to ensure items are addressed within the prescribed policy timeframes. This rectification process includes:

- Review – to ensure that items are defective in accordance with policy
- Scope – the most appropriate maintenance outcome for the defect
- Plan – to complete the work in the most efficient way before the due dates
- Complete – the undertaking of the scoped work
- Closeout – to update defect and asset records to reflect the status of the completed works

Wood poles inspection

An example of how we undertake asset inspection of poles is described below.

Wood poles are inspected in accordance with the Table 4-7 below. The inspection intervals are determined by regulatory requirements and supported by RCM analysis.

[163] Asset Inspection Manual – 05-M450

[164] Network Asset Maintenance Priority Policy – 05-C001.A-025

Poles	Type of inspection	Cycle
Serviceable poles in HBRA	Above ground inspection	2.5 years +/- one month
All serviceable poles	Full Inspection	5 years +/- one month
AC serviceable poles	Above ground inspection	1 year +/- six months
AC serviceable poles	Full Inspection	2 years +/- six months

Table 4-7 – Pole Maintenance Inspection Intervals

Note: AC in Table 4-7 means '*with Additional Controls in place*'

The aim of the inspection is to determine the remaining strength of the pole and this is dependent on the following:

- Type of timber
- External diameter
- Height
- Internal condition

Once the remaining strength is determined, the pole is classified as serviceable, AC serviceable or unserviceable.

WoodScan is one of the new technologies implemented in 2017 after undergoing a rigorous evaluation process. WoodScan determines the pole condition by providing a cross-sectional assessment of the pole and calculating the remaining strength of the pole. This then determines what maintenance action, if any, is required.

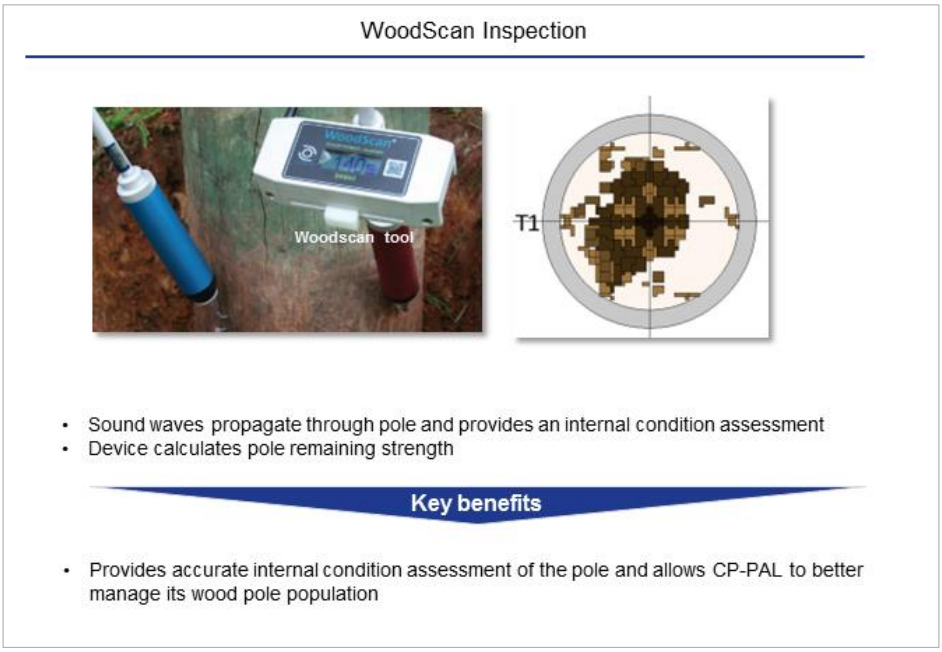


Figure 4-44 – WoodScan Pole Inspection Tool

ii. Asset Maintenance – Plant and Stations

CP-PAL plant and stations assets include zone substations, distribution substations, secondary systems equipment and underground cables.

Plant and stations assets are maintained via Work Instructions driven by relevant Asset Management Policies.

Some examples of plant and stations maintenance activities are listed below:

- Power transformers Routine overhaul
- Power transformers Oil sampling
- Power transformers tests for e.g., bushings, windings, insulation, surge arrestors
- Power transformers OLTC Class 1 and Class 2 maintenance
- Circuit breakers Class 1 maintenance
- Circuit breakers Class 4 Overhaul
- Protection schemes post commissioning and routine overhaul
- Isolators and earthing switches Class 1 and Class 2 Overhaul
- Instrument transformers general maintenance
- Earth grid inspect test & measurement
- Outdoor buses routine maintenance
- Infrared / Ultrasonic switchyard surveys

All maintenance activities are supported by relevant standard work practices to safely and effectively undertake the required maintenance activities. Refer section 4.2.2.2 Operational Delivery - Works Practices of this ESMS.

CP-PAL undertakes risk assessment to risk assess zone substation plant and station items that have or will go past their maintenance window to ensure Powercor Australia meets its regulatory requirements. These risk assessments are managed in accordance with the Zone Substation Plant & Stations Risk Assessment (RA) Procedure[165] and Over-Due Maintenance Risk Assessment Guidelines[166].

iii. Asset Maintenance – Protection and Control

Protection and Control is responsible for setting the protection philosophy for all protection relay, device software settings related to sub-transmission, zone substation, distribution substations, secondary and primary equipment or plant. The delivery of protection schemes installed throughout the electrical network to detect faults and/or abnormal plant operating conditions and isolate them selectively and quickly from the network so that the adverse consequences of the fault or condition is limited AFAP.

[165] Zone Substation Plant & Stations Risk Assessment (RA) Procedure - JEQA4UJ443MT-150-27490

[166] Over-Due Maintenance Risk Assessment Guidelines - JEQA4UJ443MT-150-27488

The design and setting process takes into consideration the above requirement and need to provide primary and back-up protection to cater for the failure of any one item of protection or plant.

Manage Protection Settings Procedure[167] is utilised when developing settings and applying them to devices installed on the electrical system. Application of the procedure helps CP-PAL to apply standard and consistent protection settings across its network.

Underpinning this process is the following:

- Protection and Control Standard[168] philosophy.
- High Voltage Protection Sub - Code
- Standard relay application manuals, configuration files, calculation and setting summary documents specific to each application listed in
- Appendix 15 – Relays Standard Application Guidelines
- Standard setting calculation documents
- Standard relay setting summary documents

Protection and Control Performance Monitoring

A tracking and monitoring process is currently being established which will result protection and control investigations being listed within the monthly Electricity Networks business report, issued by the General Manager Electricity Networks. Refer Appendix 16.

iv. Asset Maintenance – Communication Assets

CP-PAL has a communication network, which is used for network management, operations and maintenance.

Figure 4-45 below provides with diagrammatic view of the distribution network, including links for AMI, Protection and SCADA communication network. The red line represents the criticality of the link with regards to protection, with the more critical links having more sensitivity to latency. SCADA links are not related to protection, although often SCADA utilises the same communications media as protection (although not the same channel), especially where a fibre or supervisory link are utilised.

[167] Manage Protection Settings Procedure – 06-P770

[168] Protection and Control Standards – NA001

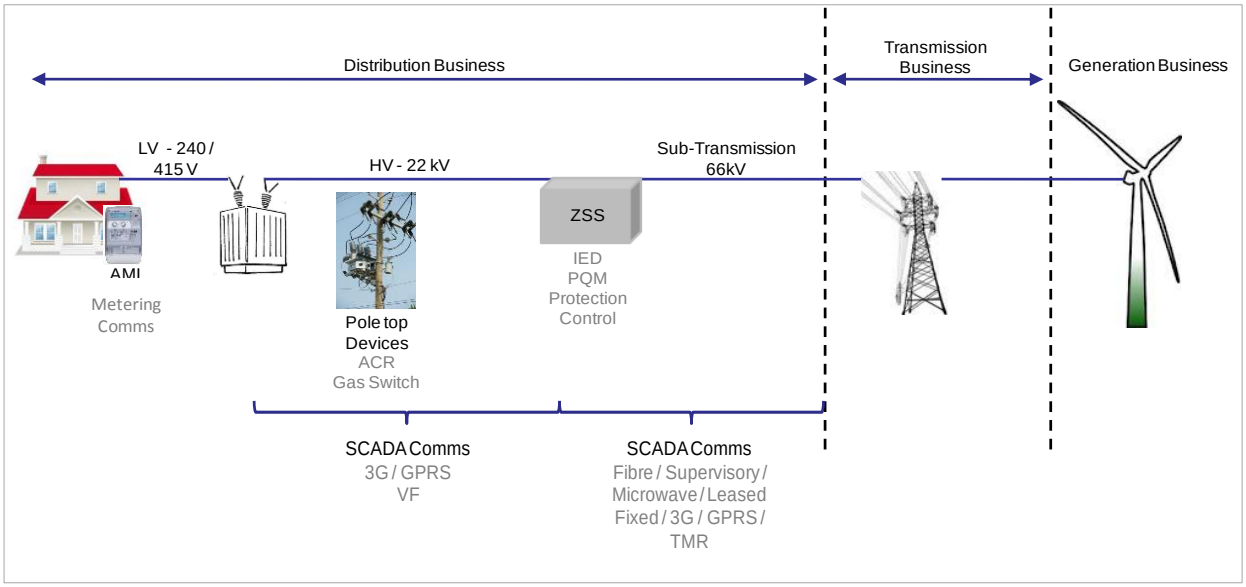


Figure 4-45 – CP-PAL Network Communications Infrastructure

Maintenance of communication network, is reliant upon the electronic diagnostic of the equipment. CP-PAL has service level contractual arrangements in place with its communication network service providers who maintain the communication infrastructure of CP-PAL network.

4.3.4.9 Inspection and Maintenance Works

Maintenance activities are scheduled to meet the timeframes specified within asset maintenance policies.

Works planning and scheduling processes are triggered by network faults, asset maintenance activities (SAP notifications), and defects found during inspection programs of the distribution network (SAP notifications). Planning and scheduling of work is carried out safely and in line with ESMS requirements.

Faults and maintenance defects on the distribution network are managed according to the Network Asset Maintenance Priority Policy. The policy specifies rectification time frames applicable for each priority rating which directly influences scheduling and planning of works. Furthermore, the policy manages the risks associated with faults and defects within acceptable levels by setting out rectification time frames consistent with the risk management component of the CP-PAL Asset Management Framework.

CP-PAL asset data management systems (SAP/GIS) are updated with results from the inspection and maintenance activities (which includes digital photography of asset defects identified at the time of inspection). Maintenance notifications are subsequently created to address any maintenance defects identified.

All defect items are assigned a rectification timeframe, in accordance with maintenance policy. The identified defect and planned rectification dates are recorded in SAP. System generated reports are used to ensure maintenace actions are completed within the policy timeframes.

There are occasions where it is not possible to complete an item prior to its policy target date. Typical reasons for this are:

- Localised flooding
- Assets being located in an active fire ground
- Customer or other authority access issues

If an item cannot be completed before the policy due date, a risk assessment is undertaken to determine the best approach to manage the asset until the work can be performed. This can include:

- Installing temporary supports
- Installing barriers to prevent public access
- De-energising assets

4.3.4.10 Asset Data Management

There are a number of processes, plans and policies that support the management of network assets, referred to collectively as 'asset data management systems'. Key elements of our asset data management are outlined below.

As described in section 1.6 of this ESMS, our CP-PAL networks consist of a large number of assets including poles, conductors, primary plant and secondary assets which span across an area of over 145,000 square kilometres. Asset information is recorded in various data management systems including SAP, Design Standards, GIS, OMS, FMC and Work Order (using Click software system).

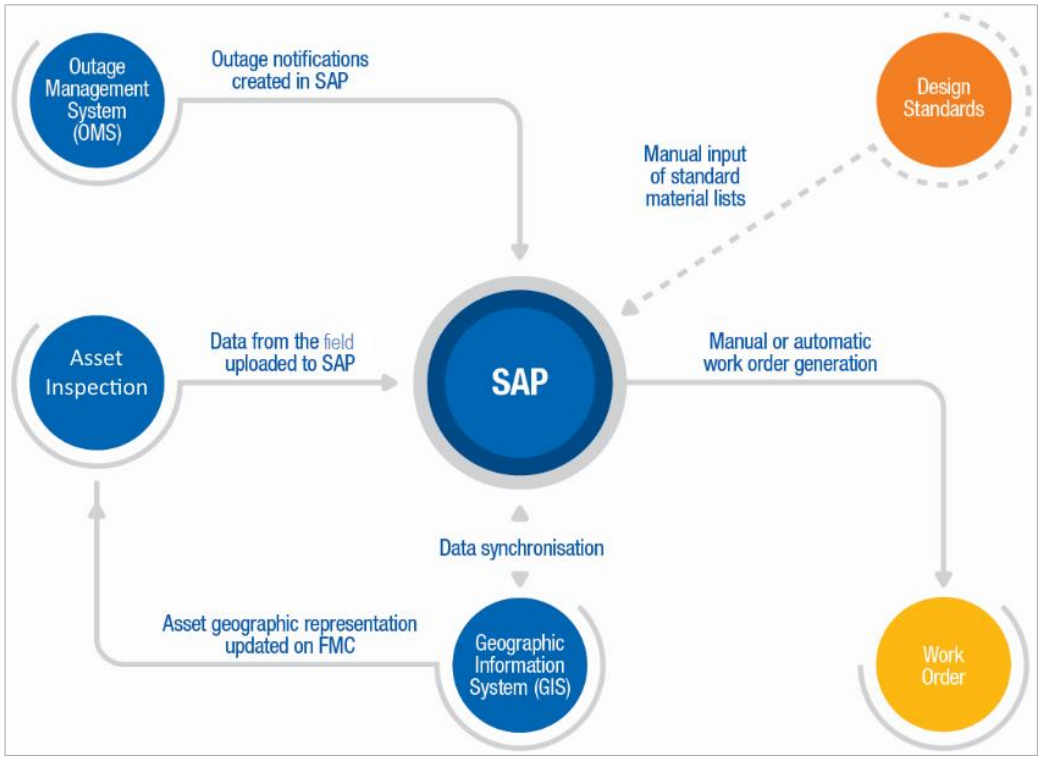


Figure 4-46 – CP-PAL Asset Data Management Systems Overview

The following sections briefly describe the functionality of asset data management systems.

SAP

SAP is used as the primary asset, material and maintenance data management system which is customised to include:

- all maintainable assets;
- management of inspection data and maintenance rules; and
- corrective maintenance as well as reporting of physical and financial performance of the asset.

The RCM rules for plant and equipment are configured in SAP, which automatically generate time based work orders for inspection and maintenance planning.

Design Standards (Materials)

Design standards are actively linked to SAP to enable materials to be created for a particular design. This ensures that the accuracy, completeness and currency of materials are maintained.

GIS

GIS is a map-based application that is used to spatially represent the CP-PAL network.

OMS

OMS is an application used to manage network faults and supply outages on the CP-PAL network. OMS data is used to undertake asset failure and fire start incident analysis.

Asset Inspection

Click is a mobile data entry program that enables asset inspectors to enter inspection data directly into SAP (via a hand held field device). The Click application also enables asset inspectors to retrieve data from SAP to review:

- equipment specifications
- previous condition
- historical faults
- maintenance data

Work Order (using Click software system)

Click is a software system used for scheduling and dispatching work orders to field based employees. Field staff enter and receive data[169] from their mobile devices (iPads) enabling CP-PAL records to be updated in real time. Click software system is currently being rolled out within CP-PAL.

DMS / SCADA

As network utilisation increases, the degree of complexity in managing the network also increases. Our networks are supported by a best practice approach where CP-PAL has implemented the first stage of a Distribution Management System (DMS). The benefits will include removal of disparate operating systems within the Network Control room and prediction of outcomes for restoration rather than relying on control staff manually determining switching arrangements. The DMS also includes operations planning improvements substantially reduce errors within switching instructions for planned network interruptions.

[169] Refer to section 'E' of Figure 4-33

4.3.4.11 Asset Maintenance Governance

Asset Management Plans and Procedures are developed and reviewed in accordance with the Asset Maintenance Policy and Asset Management Plan Review and Development procedure[170]. This procedure outlines the process/actions to be followed when a Policy or Asset Management Plan (AMP) related to electrical network assets is reviewed or a new Policy or AMP is developed.

This procedure references the Policy and AMP Review Checklist[171]. This checklist provides support information for the process of asset maintenance policy and asset management plan review and development.

Head of Network Asset Management approves asset management plans and procedures.

The Network Asset Management team monitors performance of the Asset Management Plans, Policies, Work Instructions and Guidelines. Key performance metrics monitored are:

- Asset Strategy:
  - Planned inspections
  - Number of defects found
  - Number of defects rectified
  - Planned maintenance items
- Failed Asset Investigations:
  - Recording of failed assets on our overhead and underground electricity networks
  - Investigation of key asset failures, along with recommendations of corrective actions.

Asset inspection compliance is monitored in accordance with the Maintenance Compliance Audit procedure[172] and the Asset Inspection Compliance Audit procedure[173].

The Maintenance Compliance Audit procedure is applied to auditing of maintenance work from the cyclic inspection program. This process is an annual audit program that is defined in the Field Audit Program plan and produces the following outputs:

- Monthly audit report with agreed corrective actions identified and allocated to the responsible officer.
- Audit results recorded in the SAP Audit Management system and the SAP audit report generated.

[170] Asset Maintenance Policy and Asset Management Plan Review and Development - 18-05-P0003

[171] Policy and AMP Review Checklist – 18-05-G0001

[172] Maintenance Compliance Audit procedure – 18-20-P0005

[173] Asset Inspection Compliance Audit procedure – 05-C001.A-090

The Asset Inspection Compliance Audit procedure is followed to conduct a compliance audit on network assets inspected during the cyclic asset inspection program. This audit process verifies that:

- the service provider (asset inspector) has actually visited the site;
- all required data has been captured; and
- the accuracy of reporting complies with the asset inspection work instruction (data recording and defect reporting).

4.3.5 Decommissioning

Part of CP-PAL network operations requires assets to be decommissioned either as a need of obsolesce or when it can no longer adequately perform the function it is intended to perform[174].

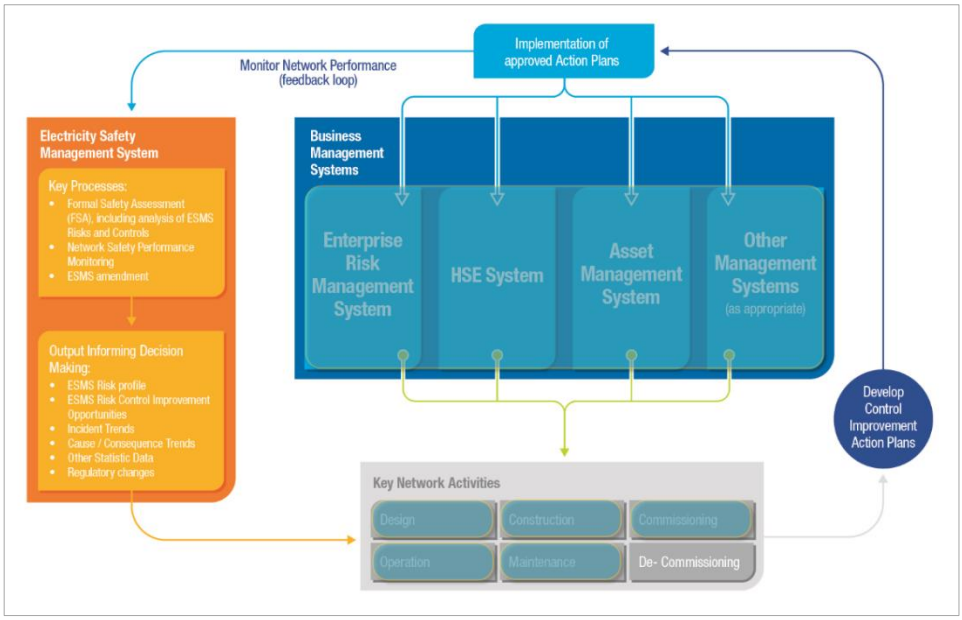


Figure 4-47 – ESMS Integration with De-Commissioning

De-commissioning of CP-PAL network assets is managed via the following key process steps.

4.3.5.1 Initiation of Decommissioning

Assets to be decommissioned are identified via:

- Performance monitoring – Assets which are no longer able to meet required functionality
- Supply abolishment – Where supply to the customer has been requested to be abolished
- Obsolete assets whose spares are no longer available

[174] Managing Obsolete Distribution Equipment Guideline – 18-05-G0005

Once assets are identified to be decommissioned, they are programmed to be retired as part of:

- Asset management plans
- Network planning and development
- Bushfire mitigation programs
- Reliability improvement programs
- Safety improvement programs

4.3.5.2 Decommissioning works

Prior to decommissioning of the asset, an Out Of Commission 'OOC' statement is required to be issued. One of the conditions of the receipt of 'OOC' is that System Control Centre is to confirm and be satisfied with the isolations created and required earthing is applied.

Once apparatus is declared 'OOC' it can be removed from the network using Standard Works Practices. For additional information refer section 2.4 of CP-PAL Operations Procedures Manual[175].

4.3.5.3 Disposal of Decommissioned assets

All the assets, which are retired as a need of replacement or augmentation or obsolescence, are disposed safely using the Retirement and Disposal of Fixed Assets policy[176].

CP-PAL maintains a register of accredited suppliers to manage the recycle, disposal and scrapping of materials associated with CP-PAL electrical assets.

CP-PAL has in place an Environmental Manual that defines policies for disposing of hazardous/dangerous materials.

Where obsolete plant is to be disposed of, the responsible officer must ensure that the project definition details include an appropriate plant disposal process. Disposal is to be facilitated through CP-PAL's Procurement section. As waste oil and some waste electrical equipment are defined as "Prescribed Industrial Waste" by the Victorian Environment Protection Authority, advice is sought from the Network Environmental Officer to determine the suitable waste stream and method of disposal.

[175] Operations Procedure Manual – JEQA4UJ443MT-185-11385

[176] Retirement and disposal of fixed assets – JEQA4UJ443MT-162-119

Section 5. ESMS MEASUREMENT AND EVALUATION

This section addresses the clause 4.5 requirements of AS 5577:

4.5 Measurement and Evaluation

4.5.1 Monitoring and measurement

4.5.1.1 General

The ENSMS shall incorporate procedures for the appropriate measurement and evaluation of the performance of the ENSMS elements. The results of audit, review and monitoring processes shall be utilized for the purpose of management review of the ENSMS.

4.5.1.2 Data acquisition and analysis

The Network Operator shall establish procedures for identifying, recording and analysing network operational, maintenance and reliability data to identify trends in the network's operation and performance that may affect the safe operation of the electricity network.

Analysis of this data should support operation of the network to continue as planned. It should also identify any negative trend that may result in an event adversely impacting the safe operation of the network.

4.5.2 Incident investigation and corrective and preventive action

4.5.2.1 Accident/incident investigation and reporting

The Network Operator shall establish procedures for identifying, notifying, recording, investigating and reporting accidents and incidents. This shall cover any event associated with the network that either causes or has the potential to cause any one or combination of the following:

(a) Death or significant injury to network personnel or the public.

(b) Significant damage to property.

(c) Significant impact on the safe operation of the network.

NOTES:

1 Significant needs to be defined by the Network Operator.

2 Reporting includes notification of relevant regulatory authorities as required by legislation.

4.5.2.2 Corrective and preventive action

The Network Operator shall develop and implement procedures for determining, approving and implementing corrective and preventive actions.

NOTE: Corrective actions are taken to deal with an existing issue while preventive actions address potential issues.

The agreed actions shall, as far as reasonably practicable, eliminate or mitigate the identified hazard and shall be appropriate and commensurate to the risk identified. The agreed actions shall be documented and their implementation monitored and confirmed.

The basis for any action shall be documented. The outcomes of corrective or preventative actions taken, along with their effectiveness, shall be subjected to independent internal review.

4.5.3 Records

The Network Operator shall implement relevant records management arrangements for the following:

(a) Control of documents, legislation, standards, codes, guidelines and procedures required for the safe design, construction, commissioning, operation, maintenance and decommissioning of the network.

(b) Maintenance of asset records including, but not limited to, maps, databases, designs and as-built drawings.

(c) Maintenance of commissioning, operation, maintenance and audit records.

(d) Maintenance of records relating to the ENSMS and revisions to it.

(e) Systems for storage and retrieval of records.

(f) Accident/incident records.

4.5.4 System audits

The Network Operator shall establish procedures for planning and implementing audits to determine the Network Operator's compliance with, and the effectiveness of, the ENSMS's plans and procedures. System audits should also assess compliance with regulatory requirements and ensure the ENSMS adequately addresses these issues.

The Network Operator shall consider the hazards identified and risks evaluated in the Formal Safety Assessment to ensure that audits evaluate—

(a) the effectiveness of the ENSMS in controlling the risks identified; and

(b) the effectiveness of the monitoring procedures in place to identify new or changed hazards and risks.

Audits shall be performed by competent personnel who are independent of the section of the ENSMS being audited. The audit procedures shall cover the timing of audits, including the conduct of external independent audits where chosen or where required by regulatory authorities.

Audit procedures shall cover arrangements for verifying the implementation and effectiveness of corrective and preventive actions designed to address any non-conformances identified during the audit.

The outcomes of audits shall be subject to management review.

NOTE: Guidance regarding auditing is given in ISO 19011.

5.1 ESMS Monitoring

CP-PAL have range of business processes in place to monitor the performance of the network. Table 5-1 lists the relevant monitoring processes along with their frequency.

Committee/Process	Frequency
EN reporting	Monthly
Network Monitoring via Control Room	24 x 7
Network Voltage	24 x 7
Bushfire summer reporting (during fire season)	Weekly
Line Maintenance (P1, P2 & P28)	Monthly
Strategic Asset Management - Network Safety Committee	Bi-Annual
Strategic Asset Management - Asset Maintenance Committee	Quarterly
Incident Review Committee	Quarterly
Bushfire pre-season and post-season review	Annual
Operating Performance Excellence Committee - The purpose for the Operating Performance Excellence Committee is to initially review operational industry standards, codes and processes, learnings from incidents, observations and investigations. The committee then develops and oversees the implementation of relevant strategies.	Bi-Monthly
Corporate Risk Profiling	Bi-Annual
Strategic Asset Management - Bushfire Mitigation Committee	Bi-Annual
Strategic Asset Management - Network Safety Committee	Bi-Annual
Electric Line Clearance Management Plan Review	Annual
ESMS/Safety Case Review – Network Safety Performance Review	Annual
Asset Management Plan Review	5-yearly

Table 5-1 – Systems Reviews and Continuous Improvement

These monitoring processes assist CP-PAL to implement preventative and corrective actions to manage the network safety risks to AFAP.

5.2 Incident Management and Reporting

The role of incident management and investigation within the ESMS is to ensure that all incidents (including electrical safety related incidents) are appropriately investigated to determine cause and to ensure suitable actions are put in place to reduce the likelihood of the incident re-occurring. Learnings from incident investigation assists in identifying controls that are required to be enhanced or put into place to manage the associated risk. All incidents shall be recorded and managed in 'Cintellate'. Cintellate is the CP-PAL online HSE information system which includes the following activities:

- Raising incidents, hazards and near misses
- Conducting audits, inspections and Take 5s
- Recording HSE conversations and interactions
- Managing HSE risks
- Managing and closing-out agreed HSE actions
- Monitoring environmental data
- Reporting on HSE trends.

The Incident Management Procedure[177] provides the process to report and investigate network safety related incidents, including incidents associated with:

- Death or serious injury
- Shock to person
- Damage to property
- Serious risk to public safety
- An imminent risk of electrocution
- Significant disruption to community and
- Significant media interest

CP-PAL reports electrical safety incidents to Energy Safe Victoria (ESV) in accordance with ESV's Distribution Business Electrical Safety Reporting Guideline.

The CP-PAL Incident Management Review Committee reviews incident reports on a regular basis and initiates or directs corrective action where required. The committee also develop, maintain and provide interpretation of the incident reporting system, Incident Management Procedure and other relevant documentation. Any changes or suggested improvements are forwarded to the document administrator who co-ordinates a review of the proposal by all relevant stakeholders. The Incident Management Review Committee meets regularly to review incidents and associated actions.

CP-PAL utilises the Incident Cause Analysis Method (ICAM) to investigate incidents of higher actual or potential consequence. Appropriately trained and experienced persons undertake incident investigations who may seek assistance of technical expertise during the investigation.

[177] Incident Management Procedure – JEQA4UJ443MT-185-28490

Where an incident has occurred, Protection and Control may provide data to responsible individuals/investigating officer.

Where an incident is directly attributable to protection equipment, undertake an investigation and provide recommendations/corrective actions.

Any actions involving the reported hazards / incidents, Audits, Inspections, Safety Interactions and Conversations and Take 5s are logged within the central database Cintellate. Once the actions are logged within Cintellate, the actions are managed to closure with timely notifications and escalation to the management structure.

5.3 Management Review Data Variables

CP-PAL Electricity Networks Monthly reporting with the following data:

- Network Faults
- Switching Incidents
- Safety Management System Performance Index
- F-Factor and Compliance
- VBRC Programs
- Vegetation Management
- Reliability
- Policy and Performance (including Asset Failure Performance)
- Line Maintenance
- Plant and Stations
- Technical Standards

5.4 System Audits and Corrective Actions

The role of system audits in the ESMS is to ensure that systems and processes are being undertaken in accordance with company policy and that compliance is achieved. Non-compliances may prevent the safe operation of the networks and hence are required to be investigated to determine the cause. Appropriate corrective actions are identified and put in place to rectify and minimise re-occurrence.

CP-PAL undertakes audit programs to confirm policies and procedures are used by both its internal resources and external contracting companies, to manage business risks and identify improvement opportunities in the areas of Quality, Health & Safety, Asset and Environmental Management.

Audits are based on the Institute of Internal Audit Australia Standards including International Standards for the Professional Practice of Internal Auditing.

CP-PAL have a centralised, standardised and documented system for the requirements of Audit and Inspection programs. The Audit and Inspection Program Requirements Policy[178] ensures that the requirements of the management systems are satisfied to the following standards and reflects ESMS audit management requirements:

- ISO 9001:2008 – Quality Management System (QMS)
- ISO 14001:2004 – Environmental Management System (EMS)
- AS 4801:2001 – Occupational Health and Safety System (OH&S System)

Planning and Implementation of Audits

Annual audit plans are established by Project Management Officer (Quality) and approved by the CP-PAL executive management team by taking into account business changes, industry focus, the risk profile, maturity of controls and results of previous audits.

CP-PAL develops audit programs (including frequency of audits) in accordance to internal audit program guidelines. These guidelines outline audit requirements and provide support information for the process of preparing audit and inspection programs[179]. Considering the range of audit program conducted across the organisation, each audit program is required to determine:

- Audit Scope – the scope of review or focus area.
- Auditor Selection – the auditors are nominated based on the training, competency and qualification requirements of the auditors executing the program.
- Audit Frequency – the frequency of review activities (i.e. number of audits per annum).
- Audit Sampling – audit sampling methods i.e. random sampling vs. targeted specific areas.

Audit program owners must ensure all above program requirements are satisfied before conducting an audit. Audit and inspection program activities are conducted in accordance to established procedures[180] and upon completion of the audit process the following results are achieved:

- Review of procedures to ensure currency and reflection of current practices.
- Review of systems to ensure adequacy and completeness.
- Communication and recording of issues raised during the audit process.

Frequency and Types of Audits Conducted

Table 5-2 below summarises the main types of audits and inspections conducted across the CP-PAL business[181]:

[178] Audit and Inspection Program Requirements Policy - JEQA4UJ443MT-175-29

[179] CP-PAL, Define Audit and Inspection Requirement MATRIX – JEQA4UJ443MT-175-58

[180] Conducting System, Site and Procedure Audit Procedure – JEQA4UJ443MT-175-35

[181] Define Audit and Inspection Requirement MATRIX – JEQA4UJ443MT-175-58

Audit Type	Audit Description	Frequency
Technical Training Compliance	Training currency compliance of contractors	Contractors are audited based on the Manage Technical Training Management Systems Audit – Contractors guidelines[182]. These guidelines require the scheduling of audits based on the contractor management system audit schedule. The audit schedules require that audits samples are based on auditing 10% of Trade roles and 5% of other roles listed in the VESI Skills and Training Matrix.
OHSMS System Audit	Auditors are engaged to ensure CP-PAL is certified to AS/NZS 4801:2000 Occupation Health and Safety Management System. In accordance with CP-PAL Health and Safety policy, a program of audits is coordinated as part of an annual audit plan. These Health and Safety audits are regularly conducted on worksites, depots, offices, plant and equipment.	Annual
Internal Audit	Internal audits determine whether the relevant department's QMS is being effectively implemented and maintained and conforms to the requirements of the standard. Audits selection includes consideration to highest risk areas. For example Bushfire Mitigation	A yearly schedule is prepared every January. Audits are conducted throughout the year.
Resource Partner Performance Management Audit	Management System audits of Field Resources are conducted to identify and verify that health, safety, quality customer services, environmental systems are in place and that they are sufficiently maintained to deliver contractual requirements to the business.	20 per annum.
Resource Partner Field Inspections	Field Inspections are conducted on Field Resources to measure and monitor contract company compliance with contractual obligations. They are conducted by competent personnel using Field Inspection Audit Checklist and associated documentation.	350 per annum.

[182] Manage Technical Training Management Systems Audit – Contractors – JEQA4UJ443MT-173-27

Audit Type	Audit Description	Frequency
Field Safety Compliance Inspections	Field Safety Compliance Audits are designed to check compliance to Management System requirements. They are designed to focus attention on safety – to promote awareness, discussion and ownership of safety issues.	A yearly schedule is prepared every January. Audits are conducted throughout the year.
Work Practice Observations	Field audits for assessing work practice compliance to published procedures are completed via Work Practice Observations (WPO). The purpose of which is to observe works practice and testing procedures to ensure they are understood and correctly followed.	10 days of auditing annually
Operations Safety Observation	The Audit is focused to ensure that the operating instructions are adhered to whilst undertaking operational activities.	Approximately 60 per annum
Asset Compliance Audit	Network construction and maintenance activities are subject to audit for compliance with policy, procedure and standard requirements and business policies and strategies.	Daily; audit volumes are dependent on the total work effort in each construction area and the audits are assigned proportionately. Audit volumes for internal construction and maintenance projects are selected based on a number of factors: 1. the size of each depot (small, medium, large) which is determined by the volume of work completed; 2. the previous performance/risk of each depot (as determined by the Weighted Quality Measure); and 3. available resource to undertake audits.

Audit Type	Audit Description	Frequency
Asset Inspection Compliance Audits[183]	This audit process verifies the following aspects: - whether the service provider (asset inspector) has actually visited the site; - all required data has been captured; and - the accuracy of reporting complies with the asset inspection work instruction (data recording and defect reporting). There are two stages to the audit process; a desktop audit (to select suitable samples) followed by a field audit (site visit).	Field audits shall be undertaken within six weeks of the inspection date. Minimum of 10% of poles of the selected work orders as well as minimum 5 poles per inspector are selected from the previous month's inspections. The benchmark sample size for field visits is a minimum of 10% of poles of the selected work orders as well as a minimum of 5 poles per inspector.

Table 5-2 – CP-PAL Audit types and frequency

Review of Design Processes and Procedures

CP-PAL conducts annual review of Project Design and Delivery (PDD)[184] processes and procedures.

The PDD Documentation Review Guideline[185] guides this review to ensure design processes and procedures are consistently reviewed to ensure that the information is appropriately documented and meets Enterprise Process Model (EPM) and organisational quality documentation requirements.

Evaluation and Management of Audit Findings

Once an audit has been completed, its findings are evaluated in accordance to the Evaluate Audit Evidence for Findings Guideline[186]. The guideline ensures that appropriate evidence is collected and should consist of records, statements, activities and other information relevant to the audit criteria.

Audit evidence is then compared with audit criteria to verify whether it satisfies requirements as set out by the audit scope and references the applicable standards or procedures. Any defects or

[183] Asset Inspection Compliance Audit Procedure Document Procedure No. 05-C001.A-090

[184] PDD Annual Documentation Review Procedure – JEQA4UJ443MT-160-323

[185] PDD Documentation Review Guideline – JEQA4UJ443MT-160-318

[186] Evaluate Audit Evidence for Findings – JEQA4UJ443MT-175-27

shortcomings found during audits are denoted as non-conformances, which is defined as a failure to conform to accepted standards or procedures.

Any non-conformances raised from audits are logged in the 'Customer Action and Response Notification' (CARE) system where they are tracked to closure. Any opportunities for improvement raised during audits are logged and tracked in a centralized 'Improvement Register'.

5.5 Records

An accurate record of our assets is critical to inform sound asset management strategies now and for the long term. The role of record management in the ESMS is to provide accurate and current information related to the network assets, which may be used to inform network strategies and further improve network safety outcomes.

CP-PAL records are managed in accordance with its ISO 9001 certified system, Records Management Policy[187]. This allows CP-PAL not only to comply with legislative requirements and the relevant Australian Standard (AS 5577 – Electricity Network Safety Management Systems) but also to support business operations and facilitate secure access to records.

The records and data include location, condition assessment and configuration assists in the safe operation and management of the networks.

Relay application manuals are maintained on the business drawing management system – Autodesk Vault. Setting records and associated documentation are maintained in the business Relay Setting Information System – 'RESIS'. Any changes or updates made to documentation are reviewed by a senior engineer and then approved by the Manager of Protection and Control.

[187] Record Management Policy – JEQA4UJ443MT-153-36

Section 6. ESMS MANAGEMENT REVIEW AND CHANGE MANAGEMENT

This section addresses the clause 4.6 requirements of AS 5577:

4.6 Management Review and Change Management

4.6.1 Management review

The Network Operator shall establish procedures for regular management review of the effectiveness and appropriateness of the ENSMS.

NOTE: This should include review by the Network Operator of those elements of the ENSMS considered high risk, and take into account the outcomes from the various procedures covering the measurement and evaluation of elements of the ENSMS.

The ENSMS shall be reviewed and, if necessary, updated at least every five years or in the event of any change to the ENSMS. This includes, for example, changes to legislative requirements, organizational structure and operational experience.

4.6.2 Change management

The Network Operator shall establish procedures for managing changes to the ENSMS, procedures, network design, construction, operation, maintenance and decommissioning so that they are made in a controlled manner, reviewed, recorded and approved by the Network Operator.

Any change to the network or its operating context shall be reviewed and approved by the Network Operator. Change shall be considered to have taken place if the engineering design has been upgraded or modified. Change shall be considered to have taken place if any event or newly identified hazard initiates an operational, technical or procedural change in the measures to (as a minimum)—

(a) protect the network and associated components;

(b) promote public safety awareness of the network;

(c) operate and maintain the network safely;

(d) implement emergency response arrangements;

(e) prevent or minimize loss of supply;

(f) carry out required inspections; and

(g) ensure that the plans and procedures continue to comply with the network's engineering and design standards.

The change management procedures shall address implementation of any resulting ENSMS changes, including notification and training of staff impacted by the change and the allocation of responsibilities for any identified actions. The change management procedures shall also include communication of changes to relevant stakeholders.

NOTE: Change triggers may also arise from external influences such as, but not limited to, legislative changes, coronial findings and Royal Commission recommendations.

6.1 Management Review

The role of management review within an ESMS is to ensure that policies and processes are reviewed, maintained and continually improved. Objectives are monitored and reported to management to ensure network safety is maintained, which includes:

- Performance against key safety performance indicators
- Items which present risk to the business
- Regulatory and legislative impacts
- Results of audits, both internal and external

Regular reviews of key electrical safety plans, Bushfire Mitigation Plan, Electric Line Clearance Plan and Asset Management Plans are undertaken to ensure alignment with business objectives and ESMS requirements.

ESMS management reviews are undertaken in the form of companywide half yearly risk profiling, which enable senior management to review and analyse the performance of the ESMS in respect to its performance in mitigating network safety risks. CP-PAL utilises the Risk Management Governance Framework to manage business risks. This framework involves all levels of the business including the Board, the Executive Management Team and the staff from all Business Units.

Management review of the ESMS also takes the form of regular performance reviews, where the effectiveness and performance of the ESMS is analysed and deficiencies within the ESMS are identified, particularly where changes have been made. Each review is recorded and stored in the ESMS Safety Performance Review records, which are communicated annually to the Electricity Network Management. Summary of reviews conducted and their frequencies are listed in Table 6-1

Review Description	Frequency of Review
Strategic Asset Management – Network Safety Committee[188]	Bi-Annually
Corporate risk profiling	Annually
Regulatory obligations reporting[189]	Annually
Review of asset management policies, plans and procedures	Timeframes specified within documents

Table 6-1 – Monitoring and Evaluation Review Table

The management review and governance process is further discussed in Element 9 of the Safety Case.

[188] ESMS FSA Monitoring and Review Procedure – JEQA4UJ443MT-173-48

[189] Quantate Regulatory reporting

6.2 ESMS Governance

ESMS is achieved via the following Committees:

- Network Investment Committee (NIC)
- Victorian Power Network Investment Committee (VPNIC)
- Strategic Asset Management (SAM) Committees
- Asset Policy Review
- Quality Forum
- Works Practices Governance Committee
- HSE, Incident Review Committee
- Operations Committee

6.3 Change Triggers

The following can trigger changes to CP-PAL's Safety Case, ESMS including the Asset Management Framework or HSE Framework:

- Changes in the operating environment
- Changes in the requirements of local jurisdictions including ESV
- Material changes to CP-PAL's electricity network
- Updates due to Control Improvement Plans

Changes to the ESMS

In accordance with section 107 of the Electricity Safety Act 1998, CP-PAL submits a revised ESMS to ESV where there has been a significant change to the risk of the network. For example, this may result from a significant change to the configuration of network assets or practices that would result in a material increase to network risks. Justification of the change would be supported by a risk assessment.

Control Improvement Actions will be determined as a result of the FSA Monitoring and Improvement process as discussed in sections 5.3 and 5.4.of this ESMS

A regulatory change or formal direction from ESV may also result in the requirement for a revised ESMS, as an example our ESMS was revised to include the requirements associated with the direction for installation of armour rods and vibration dampers.

Changes to Asset Management and HSE Frameworks

Changes to the Asset Management or HSE Frameworks are managed in accordance with the processes as described in section 4.2.1.1 and 4.2.2.1 respectively.

6.4 Document Control and Rationale for Change

Process documentation is classified, controlled and managed in accordance with the Process Documentation Policy[190], Manage Process Documentation Procedure[191] and the Enterprise Process Model (EPM)[192]. The EPM is supported by the Source - Process Portal (SharePoint platform) that ensures that documentation is readily accessible, standardised and aligned with the requirements of the Quality Management System (certified to ISO 9001). Process documentation includes:

- Policies
- Standards
- Procedures
- Work Instructions
- Standard Work Practices
- Guidelines and
- Support Information

CP-PAL's Process Documentation Policy and the incorporated business rules ensures that processes are:

- Created, maintained and archived throughout the stages of their lifecycle, to ensure that they are current, accurate, complete, useable and accessible by the organisation.

[190] Process Documentation Policy - JEQA4UJ443MT-175-86

[191] Manage Process Documentation - JEQA4UJ443MT-175-87

[192] EPM Process Model Understanding Source

- Owned by a person or role within an organisational function and
- Aligned with a function and process.

The policy defines the key roles of Business Process Owner (BPO) and Business Process Analyst (BPA) as follows:

- BPO must ensure the respective processes are current, duly followed and any improvements are proactively identified and managed.
- BPA must work with the BPOs to ensure all processes are documented to the agreed standards and any deficiencies are resolved in a timely manner.

The standard procedure for managing Process Documentation has the following steps:

- The relevant BPA is required to verify with relevant stakeholders:
  - for new documentation
    - the need/reason(s) for documentation; and
    - that no similar document exists.
  - for updates
    - that requirements are valid;
    - engage all key stakeholders and seek feedback on proposed changes; and
    - address any issues presented by the stakeholders.
- When a new process is developed or changes are required, the Business Process Owner (BPO) reviews and either approves or rejects the request for documentation creation or update.
- It is responsibility of the BPO to confirm that by approving the creation of a document or a change to a document, CP-PAL's network safety risk is assessed.
- All relevant stakeholders involved with and affected by the use of the documentation are engaged to ensure that:
  - Stakeholder feedback is sought;
  - Any issues presented by stakeholders are addressed; and
  - Key stakeholders formally support new documentation or changes to existing documentation.

ESMS documentation is developed and modified in accordance with the business policy and procedure described above. The responsibilities, accountabilities and authorities relevant to CP-PAL's ESMS are prescribed in section 4.2.4.1 Responsibilities, Accountabilities and Authorities.

6.5 Process Change Responsibilities and Accountabilities

The positions assigned the role of BPOs and BPAs for the four key areas of Design, Operations, Asset Management and Works Practices are listed in Table 6-2 below:

Business Process	Business Process Owner (BPO)	Business Process Analyst (BPA)
Design	Head of Design	Manager Substation & Underground Design Manager Overhead & Distribution Design
Operations	Manager Network Control & Operations	Control manager Investigation & Authorisation Manager Network Access Manager Faults & Reliability Manager
Asset Management	Head of Network Asset Management	Technical Standards Manager Plant & Station Manager Asset Strategy Manager Protection Solutions Manager Manager Communication Networks
Operational HSE Improvement	Manager Operational HSE Improvement	Development Services Officer
Vegetation Management	Head of Vegetation Management	Technical officer, Strategy Program and Change Lead
Safety Case and ESMS	Network Safety and Bushfire Mitigation Manager	Network Safety Engineer

Table 6-2 – BPO and BPA for key Business Processes

6.6 Change Management

Change Management is the discipline that guides how we prepare, equip and support individuals (e.g. employees, customers, suppliers, partners) to successfully adopt change in order to drive organisational success and positive business outcomes. It is a proactive approach that anticipates and addresses the potential resistance to and people impacts from change.

Change management also incorporates feedback and seeks optimal people, process and system outcomes.

The Strategy Programs & Change (SP&C) team within CP-PAL provides three core change management services dependent upon the complexity of the change. These core services are to Consult, Plan or Execute. The services delivered will not be mutually exclusive (e.g. Consult, Plan and Execute can be delivered for a single initiative / project). SP&C will also provide an additional service to identify and engage with additional external change management resources as and when required.

Changes to processes and practices are implemented in accordance with the 'Organisational Change Management Framework'. The framework covers the three phases of Preparation, Management and Reinforcement. Key activities to be undertaken in these phases are:

- Preparation Phase
  - assess the scale / scope of change
  - identify Stakeholders
  - identify and to assess risks (refer section 4.1)
  - assess other issues or business impacts
  - prepare Change Management strategy and plan
  - obtain approval from management.

  Note: Approval of the change is generally from line manger relevant to the change. Depending on resource requirements (e.g. risk levels, financial, etc.) of the change, approval process may be escalated to higher management levels through normal business process.
- Management Phase:

  The management phase comprises a range of activities to ensure employees are adequately trained to implement the change thereby managing the risk of non-compliance with new or modified practice/procedure.
- Reinforcement Phase:

  Activities included in this phase consists of monitoring, review and evaluation processes, including but not limited to the following:
  - User acceptance survey
  - Conducting change health checks
  - Post implementation reviews

- Operational handover documents are prepared for BAU transition (compiled with the process as described in Section 6.4).

The Organisational Change Management framework is provided in Appendix 10.

HSE Change Management

HSE Change Management procedure[193] explains what needs to happen when we change any aspect of how or where we work, so that we can identify, assess and manage any HSE risks that arise.

This procedure outlines the following key instructions:

- Assess changes
- Initiate the change
- Obtain approval
- Implement the change
- Conduct a post change review

[193] Change Management Procedure - JEQA4UJ443MT-185-28471

6.7 ESMS FSA Outcomes as Inputs to other Business Systems

Outcomes of the half-yearly risk profiling are provide to relevant business units as inputs for their on-going reviews as shown in Figure 6-1 below:

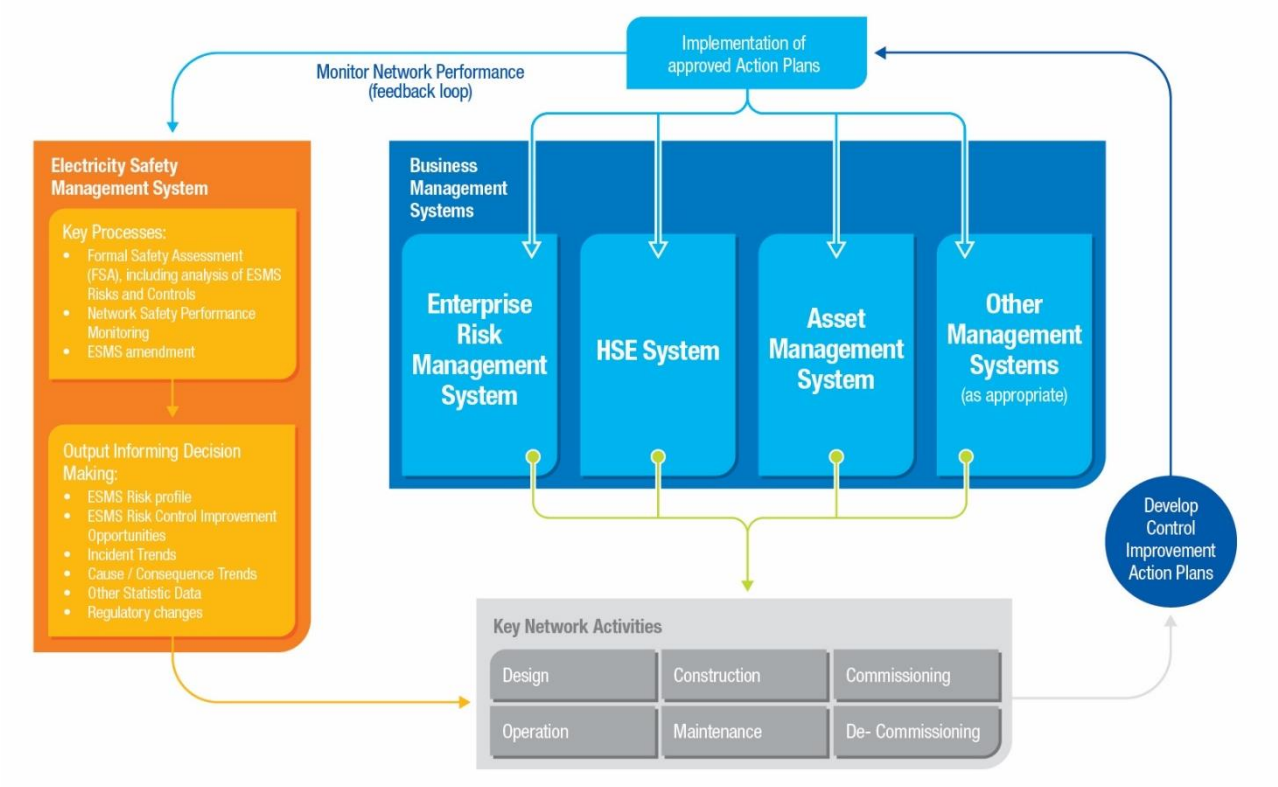


Figure 6-1 – ESMS-FSA Outcomes as Inputs to other CP+PAL Management Systems and Key Network Activities

For details of examples on how the outputs from ESMS-FSA are made visible to and communicated with senior management or other business units, refer section 4.1.3 of this ESMS.

6.8 Monitoring and Evaluation

Monitoring and evaluation

The effectiveness and appropriateness (performance) of the ESMS is regularly reviewed and deficiencies within the ESMS are identified, particularly where changes have been made. Reviews conducted and their frequencies are listed in Table 6-1.

These measures ensure that the continuous monitoring and review activities are achieving the desired effectiveness and appropriateness of the ESMS. Each review is recorded and stored in the ESMS Safety Performance Review records.

Executive Visibility of Actions Implementation

CP-PAL undertakes company-wide half yearly risk profiling. Executive management team is part of this process. The CP-PAL Board is informed via the VPN Risk Management Compliance Committee (RMCC) of all the risks via risk profiling exercise, which takes place twice a year.

Any risk that are added, removed or change in risk ratings is reviewed and discussed along with focus areas for e.g. top 10 risks during the RMCC meetings.

The main deliverable of this process is the consolidated risk profiling documentation capturing the inherent and residual risk profile, the controls, their effectiveness and corrective actions implementation timeframes. The actions are monitored for timely implementation. High risks and their associated control improvement actions are reported to the Board.

6.9 Continuous Improvement

CP-PAL develop strategic programs that align with the CP-PAL's key strategic focus areas and values as shown in Figure 6-2 below.

Figure 6-2 – CP-PAL Strategic Focus Areas and Values

Our strategic program of work comprises initiatives across the five strategic pillars being:

- Optimising Regulatory Outcomes, Driving Operational Excellence,
- Building a Network for the Future,
- Delivering Customer Outcomes and Improving Stakeholder Engagement
- Strategic Programs are governed by the Strategy
- Programs and Change Steering Committee comprising of CP-PAL executive management.

One of the CP-PAL key strategic focus areas is ***Driving Operational Excellence*** which means that we focus on delivering cost effective and efficient operation and maintenance of our network so we can continue to provide our customers with a safe, reliable and affordable supply of electricity. We are improving and strengthening our business for the long term by doing more with what we have (increasing productivity) and being smarter about how we do things (better utilising our capabilities). This strategic focus area drives continuous improvement within our organisation

including asset management systems and methods. CP-PAL utilise the *Lean Splash Methodology* to provide guidance in continuous improvement activities. [195]

'MyIdeas'[196] is a process that has been implemented in CP-PAL to ensure that a consistent, standardised and centralised approach is used for raising, assessing, treating and communicating on the status of ideas and improvement opportunities within the organisation. **This process provides a company-wide channel to raise ideas and improvement opportunities and covers the process to assess, decide and communicate decisions on the ideas raised.**

When proposed new materials or equipment is requested to be introduced onto the CP-PAL networks, the Field Trial Process[197] shall be followed to ensure that a structured and consistent approach for the approval and implementation of trials is followed.

CP-PAL has a dedicated team called Network Technologies to focus on identifying and proposing new and emerging technologies in order to be more effective and efficient for managing our assets. A wide group of stakeholders including SMEs from design, construction, operation, maintenance and safety are involved in reviewing Network Technologies proposals.

A recent initiative involved the mapping of the LV Network using AMI meter voltage signatures, matching them to local transformers and providing a visual representation as shown below at figure 6-5. This initiative has improved the accuracy of our LV map systems and has avoided 92 unplanned outages from incorrect data.

Figure 6-3 – Map of LV Network Visualisation

CP-PAL are presently working to validate Neutral Integrity Fault detection application.

The Neutral Integrity Fault detection application/algorithm identifies potential issues with LV customer connections.

The algorithm provides both an indication of the severity of the issue and a confidence rating (0-100%) that it is likely to be a real issue. Refer Figure 6-4 below.

[195] Applying Lean Splash Methodology Document # JEQA4UJ443MT-175-72

[196] Raise and manage ideas using myIdeas Document # JEQA4UJ443MT-206-141

[197] Field Trial Process Document # JEQA4UJ443MT-224-2

Early detection means that maintenance can be scheduled before the connection becomes a safety risk or an outage.

Figure 6-4 – Neutral Fault Detection Sample

CP-PAL are aiming to introduce this into regular use to proactively identify and address these issues once the validation works are completed. Refer Appendix 16.

6.10 ESMS Resubmission

As per the requirements of the Electricity Safety Act 1998, CP-PAL submits a revised ESMS to ESV where there is a material change to the risk profile of the network. This may result for example from significant changes to network assets or work practices that lead to a material increase to network hazards and risks. The revision will normally be accompanied by relevant risk assessments that consider these changes. CP-PAL will issue ESMS revisions to ESV and will consult ESV on significant changes, which may result in a formal revised ESMS submission.

Less material changes to the risk profile are managed by reviewing the relevant identified network safety risks and updating their risk assessments accordingly. This may lead to a review of and changes to individual asset management strategies and other nominated controls for the risks. Changes and the reasons are recorded in updates to the formal safety assessment.

LIST OF FIGURES & TABLES

Figures

Tables

APPENDICES

Appendix 1. CP-PAL'S HEALTH & SAFETY POLICY

Health and Safety Policy

CitiPower Pty and Powercor Australia Ltd
(including Powercor Network Services and CHED Services)

The health and safety of our employees, contractors, customers and the community is CitiPower and Powercor's highest priority.

We live safe. We never compromise health and safety.

To achieve our safety commitment, we must all strive to adopt a 'whole of life' approach to safe behaviour, while focusing at work on:

- Leading through strong and visible leadership.
- Promoting a health and safety culture of cooperation, commitment and responsibility where safe behaviours are recognised and promoted.
- Ensuring adherence to health and safety policies, systems, practices and expectations.
- Intervening when unsafe acts or conditions are observed.
- Proactively identifying hazards and minimising risk during all aspects of the design, planning and execution of our work.
- Ensuring everyone understands the hazards associated with their work, the relative risk associated with the hazard, and the controls required to minimise risk exposure.
- Ensuring our contractors understand and follow this policy and all relevant sub-policies.
- Effectively consulting with each other about health and safety.
- Meeting or exceeding all relevant laws and management system requirements.
- Preserving the safety of the public in all matters under our operational control.
- Setting and holding ourselves accountable for achieving challenging and transparent health and safety objectives and targets.
- Driving continuous improvement and innovation in health and safety behaviours and performance.

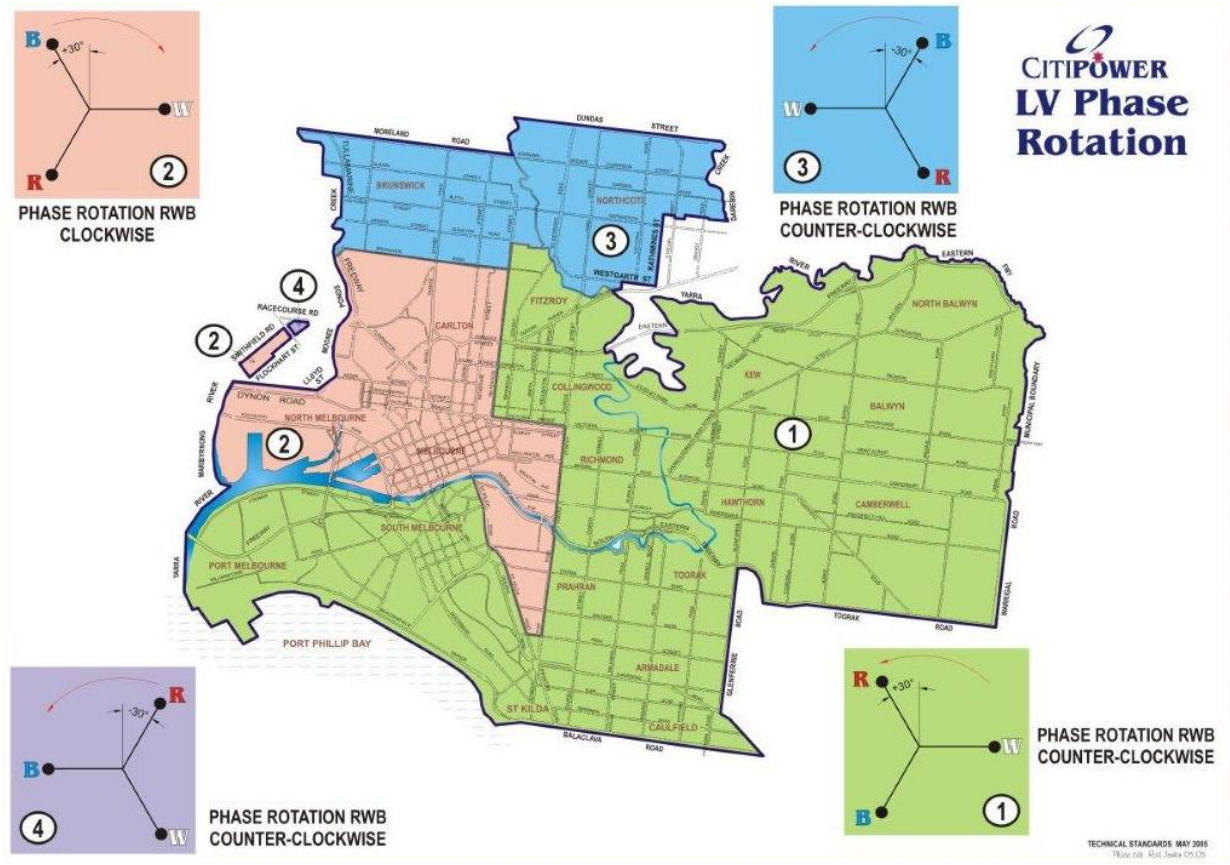
Timothy Rourke
Chief Executive Officer
January 2014

CITIPOWER

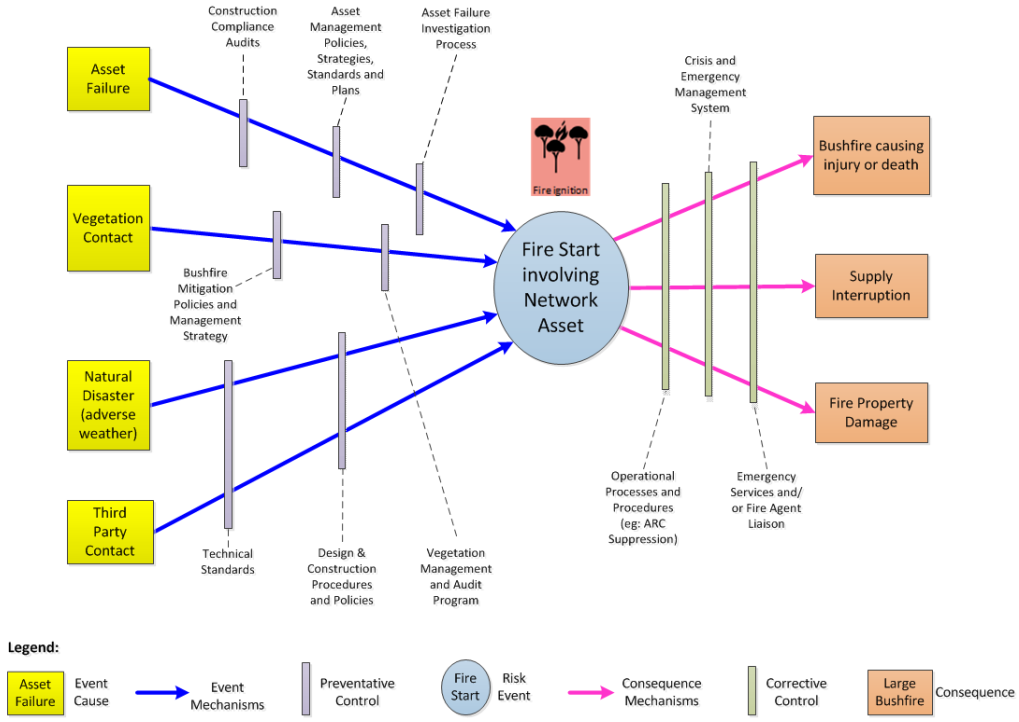
Powercor AUSTRALIA

14-00-CP0001

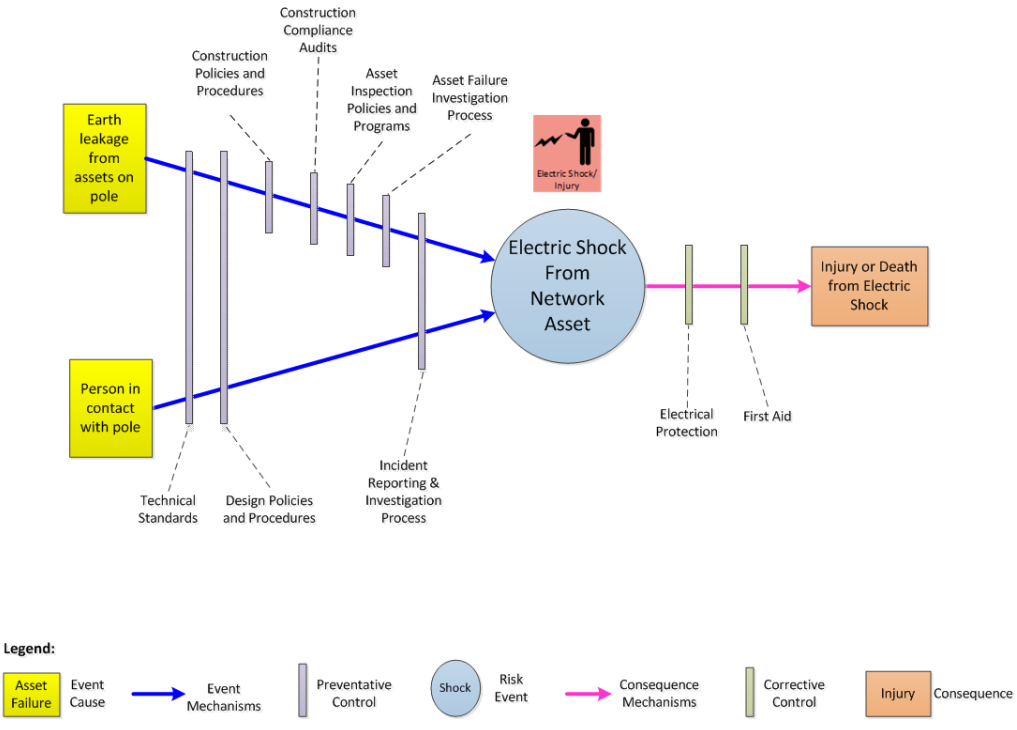
Appendix 2. LV PHASE ROTATION CONFIGURATION



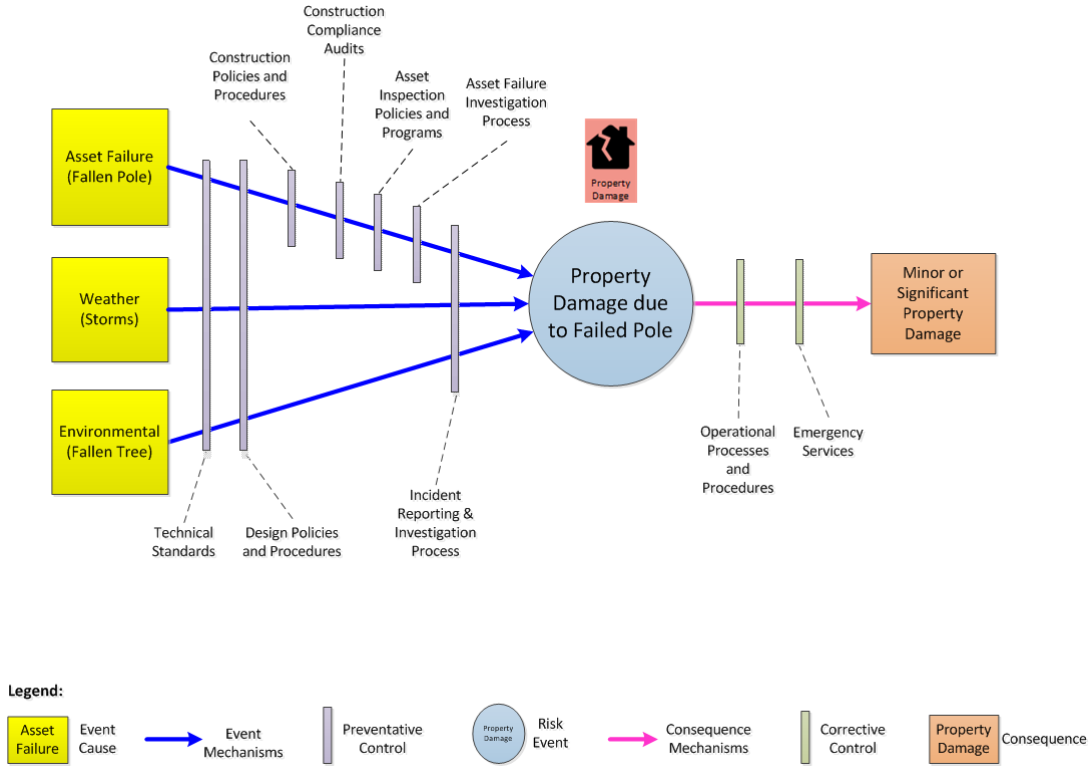
Appendix 3. BOW TIE DIAGRAMS



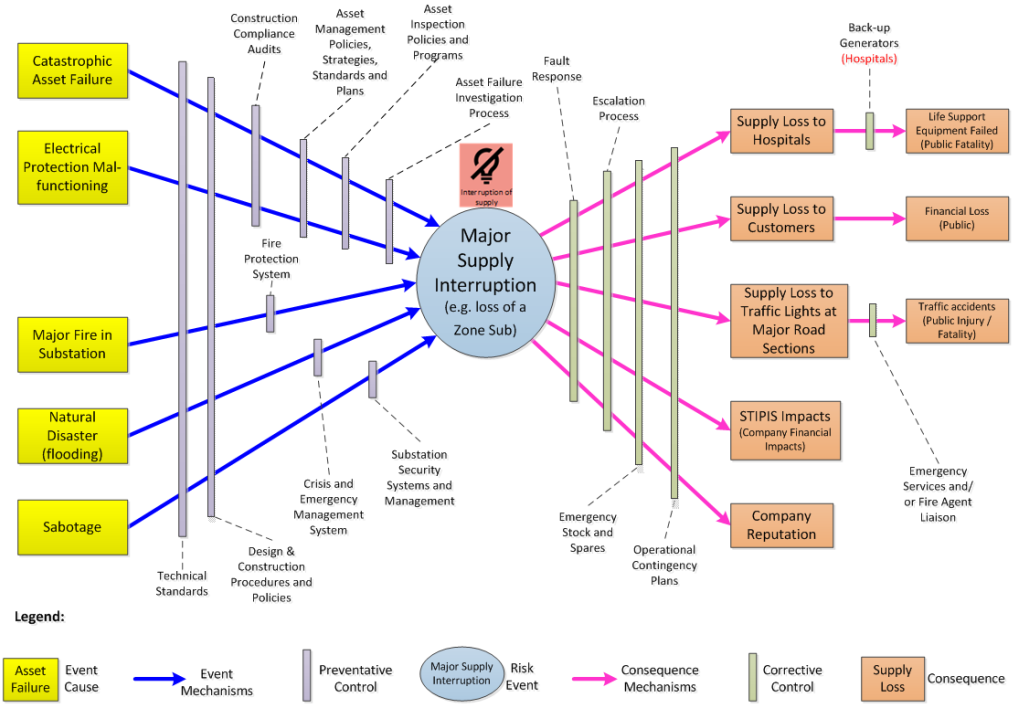
Bowtie example for the risk of fire ignition



Bowtie example for the risk of electric shock



Bowtie example for the risk of property damage



Bowtie example for the risk of interruption of supply

Appendix 4. ESMS RISK EVENT CONTEXT

Table Appendix 4– ESMS Risk Event Context

ESMS Risk ID	Risk Event (Scenario) Description	Context
01	A service insulation, neutral conductor, meter and/or connection fails	Risks to General Public associated with O/H or U/G Service Connection asset failure
03	Third party contact or interference with elevated network assets	Risks to third party due to contact or interference with O/H assets and assets at ground level (such as pillars and public lighting poles)
05	Third party contact or interference (including 'dig-in') with Underground assets, pillars, pits and cabinets.	Risks to third party due to contact or interference with Underground (such cables, cabinets, pillars pits, ducts and conduits) Assets
08	Connection/restoration/removal of supply to an installation is not performed correctly.	Risks to General Public associated with inappropriate Service Connections
10	Interference with Network assets [other than overhead lines]. -- (Unauthorised / forced access, other utilities / 3rd parties working near or on network assets)	Risks associated with Vandalism and Unauthorised access to Network Assets (other than O/H assets).
11	Conductive pole or network structure becomes energised.	Risks to General Public associated with excessive leakage currents and inappropriate earthing of network assets at ground level.
13	Employee inadvertently makes contact with live equipment.	Risks to employees and direct contactors associated with accidental contacts with exposed live parts of network assets.
14	Damage to network assets associated with natural disaster or major event	Risks associated with natural disaster or major events (such as flooding), including all Assets
15	Failure of overhead network assets, for e.g. Surge Arrester, Fuse, ACR, pole, Conductor, Joints, Cross-arm and Insulator, etc.	Risks associated with O/H asset failure (excluding O/H Services as covered within risk scenario 01), including Overhead Mounted Secondary Equipment Assets.

ESMS Risk ID	Risk Event (Scenario) Description	Context
16	Overload of Network Assets.	Risks associated with overload of network assets, including Overhead, Underground, Distribution Sub, Zone Sub, Service Connections (both O/H & U/G setup) and Secondary Equipment Assets.
19	Poles and assets (transformers on poles, stays and pillars at ground level, etc.) struck by vehicles.	Risks associated moving vehicle impacts on network assets at ground level, including power pole, service pole, public lighting pole, SWER Pole, Switch pole.
25	Failure of underground network assets.	Risks associated with underground network assets, including Underground Assets in Zone & Distribution Sub U/G Assets
26	Cables, trenches, enclosures and/or pit lids in unsafe condition.	H&S Risks to General Public associated with Underground Network Assets such as Cables (during construction), trenches (during construction), enclosures and/or pit lids at ground level.
27	Failure of equipment in Zone substations	Risks associated with assets (primary equipment) in Zone substation.
30	Failure of Electrical Protection and/or Control System	Risks associated with failure of secondary equipment.
31	Contact made or interference with earthing systems including SWER.	Risks associated with third party contacting or interfering Earthing Systems.
32	Distribution substation equipment failure.	Risks associated failure of O/H network assets, including pole-mounted transformers, ACRs and fuses.
33	Network impacted by adjacent infrastructure failure or works, including Customer Installations, e.g. Solar Systems.	Risks due to external impacts (adjacent structure failure, works done by others, customer assets, etc.) to network assets, including Overhead, Distribution Sub, Zone Sub, Service Connections (both O/H & U/G), Public Lighting.
34	Fire Starts involving overhead network assets.	Risks associated with fire starts from O/H network assets, including pole-mounted transformers, ACRs and fuses.

Appendix 5. ESMS RISKS AND ASSET GROUPS

For a risk event involving multiple asset groups, the highest value of the residual risk rating is used to represent all other asset groups for subsequent control identification and analysis. Below is a Risk Matrix Table showing Risk Scenarios across Asset groups.

ESMS Risk Scenarios	Assets involved/impacted						
	Poles and towers Pole top structures OH conductors Service lines	UG cables	Dist sub plant misc. Dist transformers Property and facilities Dist switchgear Earthing system	Zone transformers Zone sub plant misc. Zone switchgear Property and facilities Earthing system	Metering	Public lighting	SCADA & communications Protection and control
Employee inadvertently makes contact with live equipment.	Y	Y	Y	Y	Y	Y	Y
Third party contact (Including Vegetation) or interference with elevated network assets	Y					Y	
Third party contact or interference (including 'dig-in') with Underground assets, pillars, pits and cabinets.		Y				Y	
Interference with Network assets [other than overhead lines]. -- (Unauthorised/forced access, other utilities/third parties working near or on network assets)		Y	Y	Y	Y	Y	Y
Contact made or interference with earthing systems including SWER.			Y				Y

ESMS Risk Scenarios	Assets involved/impacted						
A service insulation, neutral conductor, meter and/or connection fails					Y		
Failure of overhead network assets, i.e. Surge Arrester, Fuse, pole, Conductor, Joints, Cross-arm and Insulator, etc.	Y						
Failure of underground network assets.		Y					
Distribution substation equipment failure (other than electrical protection)			Y				
Failure of equipment in Zone substations (other than electrical protection)				Y			
Failure of Electrical Control and Protection Systems.							Y
Conductive pole or network structure becomes energised.	Y	Y				Y	
Poles and assets (transformers on poles, stays and pillars at ground level, etc.) struck by vehicles.	Y	Y				Y	
Network impacted by adjacent infrastructure failure or works, including Customer Installations, e.g. Solar Systems.	Y		Y	Y	Y	Y	Y
Damage to network assets associated with natural disaster or major event	Y	Y	Y	Y	Y	Y	Y
Fire Starts involving overhead network assets.	Y		Y				Y
Overload of Network Assets.	Y	Y	Y	Y	Y		Y

ESMS Risk Scenarios	Assets involved/impacted						
Connection/restoration/removal of supply to an installation is not performed correctly.					Y		
Cables, trenches, enclosures and/or pit lids in unsafe condition.		Y			Y	Y	

ESMS Risks and asset groups

Appendix 6. ESMS CAUSES - RISK EVENTS / SCENARIOS – CONSEQUENCES MAPPING

Possible Causes

Personal / Equipment Contacts / Interference				External Interference											Network Internal Factor										Others		
3rd Party work / equipment in proximity	Employee / direct contractor work in proximity	General Public lack of understanding of Electrical Hazard	Vandalism / Sabotage / Unauthorised Access (Copper theft)	Animal / Bird / Termite interference	Aircraft contacting O/H Assets	Trees / Vegetation Contacts	High Vehicle contacting O/H Assets	Severe Lightning Storm / High Wind	Water Ingress / Flooding	External Fire	Natural Disaster / Major Event	Electricity Loading increased	Vehicle Driver error	Impacted by Adjacent Infrastructure: Clearance / Accumulated fume or flammable gas	Asset Internal defect, corrosion or deterioration	End of Asset Service Life	Movement of Asset Overtime	Equipment Not Fit for purpose	Design Deficiency	Inadequate Clearance	Poor Workmanship or Work practices	Operational / Human Error	Inadequate Asset Location / Depth / Records	Work Order (Instruction) error / mis-interpretation	Open Trench Work	Ground Surface Level of assets changed	Assets at ground level in vulnerable location
			✓									✓						✓	✓			✓			✓			
													✓					✓	✓			✓						
													✓					✓	✓									✓
																			✓							✓	
✓		✓																✓	✓								
✓		✓																✓					✓			✓	
✓																		✓									
	✓																	✓		✓							
✓																		✓					✓			✓	
				✓		✓									✓	✓	✓	✓	✓		✓						
				✓					✓						✓	✓	✓	✓	✓		✓						
				✓	✓	✓	✓	✓		✓			✓		✓	✓	✓	✓	✓		✓	✓					
									✓				✓		✓	✓		✓	✓		✓	✓					
			✓						✓	✓					✓	✓	✓	✓	✓		✓	✓					
			✓						✓	✓					✓	✓		✓	✓		✓	✓					
									✓	✓					✓	✓		✓	✓		✓	✓					
											✓							✓	✓								
														✓				✓	✓								
✓				✓		✓		✓							✓	✓	✓	✓	✓		✓	✓					

Potential Consequences

ESMS Risks			Health & Safety Impacts				(Financial) Property Damage			(Reliability) Supply Interruption		Others					
Hazard Group	ID	Event / Scenario Description	Electric Shock	Personal Injury (including Fatality) - 3rd Party / Public	Personal Injury (including Fatality) - Employee / Direct Contractor	Fire	3rd Party / Public Property Damage	Network Asset Damage	Network Property Damage	Customer Supply Interruption	Major Supply Interruption	Customer Services	Environment	Compliance	Reputation	Employee Satisfaction
Network Assets in Unsafe Situations (Specific Risks based on characteristics of incidents)	08	Connection/restoration/removal of supply to an installation is not performed correctly.	✓	✓	✓			✓				✓		✓		
	16	Overload of Network Assets.		✓	✓	✓		✓		✓	✓	✓		✓	✓	
	19	Poles and assets (transformers on poles, stays and pillars at ground level, etc.) struck by vehicles.		✓			✓	✓		✓	✓		✓			
	26	Cables, trenches, enclosures and/or pit lids in unsafe condition.		✓				✓						✓	✓	
Person / Equipment in Contacts / Interference with Network Assets (Human Factors)	03	Third party contact or interference with elevated network assets	✓	✓		✓	✓	✓		✓	✓	✓		✓	✓	✓
	05	Third party contact or interference (including 'dig-in') with Underground assets, pillars, pits and cabinets.	✓	✓		✓	✓	✓		✓	✓	✓		✓		
	10	Interference with Network assets [other than overhead lines]. - - (Unauthorised / forced access, other utilities / 3rd parties working near or on network assets)	✓	✓		✓	✓	✓		✓	✓	✓				
	13	Employee inadvertently makes contact with live equipment.	✓		✓			✓		✓	✓	✓		✓	✓	✓
	31	Contact made or interference with earthing systems including SWER.	✓	✓				✓		✓	✓	✓			✓	
Failure of Network Assets (Asset Performance)	01	A service insulation, neutral conductor, meter and/or connection fails	✓	✓				✓		✓		✓		✓	✓	
	11	Conductive pole or network structure becomes energised.	✓	✓				✓						✓	✓	
	15	Failure of overhead network assets, for e.g. Surge Arrester, Fuse, ACR, pole, Conductor, Joints, Cross-arm and Insulator, etc.		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	
	25	Failure of underground network assets.		✓	✓	✓	✓	✓		✓	✓	✓		✓	✓	
	32	Distribution substation equipment failure.		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	27	Failure of equipment in Zone Substations		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
	30	Failure of Electrical Protection and/or Control System		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	
	14	Damage to network assets associated with natural disaster or major event		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
	33	Network impacted by adjacent infrastructure failure or works, including Customer Installations, e.g. Solar Systems.		✓	✓	✓	✓	✓	✓	✓	✓	✓				
Bushfire (Specific Risk based on Particular Concerns)	34	Fire Starts from O/H Network Assets		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

Appendix 7. DETERMINING THE LIKELIHOOD RATING OF RISK EVENT

Below is an example to demonstrate how the risk rating of a risk event is determined:

ESMS Risk ID 01 "A service insulation, neutral conductor, meter and/or connection fails".

i) Risk Ratings based on Statistic Data between year 2011 and year 2015 (a 5-year period):

- 224 incidents with Minimal Consequences
  - Qualitative Assessment

    Likelihood Rating = "Almost Certain"
    Consequence Rating = "Minimal"
    Risk Rating (based on Table 3-4 – Risk Profiling Matrix) = "Medium"
- 453 incidents with Minor Consequences
  - Qualitative Assessment

    Likelihood Rating = "Almost Certain"
    Consequence Rating = "Minor"
    Risk Rating (based on Table 3-4 – Risk Profiling Matrix) = "High"
- 1 incident with Moderate Consequence
  - Qualitative Assessment

    Likelihood Rating = "Possible"
    Consequence Rating = "Moderate"
    Risk Rating (based on Table 3-4 – Risk Profiling Matrix) = "Medium"

ii) Assessment carried during FSA Workshop

Statistic data were presented for reviews and discussions during the FSA workshops.

Initial discussion was to change the likelihood rating to "Unlikely" with the H&S consequence changed to "Major" (worst case), the corresponding risk ratings:

- Qualitative Assessment – Risk Rating = "Medium"

Final Decision was to keep the likelihood rating as "Almost Certain" with the H&S consequence rating remained at "Minimal" (with the final risk rating = "High") to reflect the ultimate situations of the risk event.

Appendix 8. RISK RATING EXAMPLE

Calculation example for overall Consequence Rating:

Financial:	Consequence Rating = Minimum,
Health and Safety:	Consequence Rating = Major,
Customer Services:	Consequence Rating = Minimum,
Reliability:	Consequence Rating = Minor,
Reputation:	Consequence Rating = Minimum,
Environment:	Consequence Rating = No Impact,
Compliance:	Consequence Rating = Minimum,
Employee Satisfaction:	Consequence Rating = No Impact,
Overall Consequence Rating	= Highest of the above i.e. Major
	Therefore, consequence rating = Major

Appendix 9. ERM CONTROL IMPROVEMENT

The following table outlines the improvement actions to be carried out depending on the control's effectiveness and reliance assessment.

Control Reliance	Control Effectiveness	Control Improvement
Critical	Fully Effective	No Improvement Plan required.
	Mostly Effective	Improvement Plan to be developed and implemented as required to address control deficiencies.
	Partially Effective	Improvement Plan to be developed and implemented to address control deficiencies.
	Ineffective	Improvement Plan to be developed and implemented as a high priority matter to address control deficiencies.
Significant	Fully Effective	No Improvement Plan required.
	Mostly Effective	Assess improvement options and confirm management of the control. Improvement Plan to be developed if required.
	Partially Effective	Improvement Plan to be developed and implemented as required to address control deficiencies.
	Ineffective	Improvement Plan to be developed and implemented to address control deficiencies.
Important	Fully Effective	No Improvement Plan required.
	Mostly Effective	No Improvement Plan required.
	Partially Effective	Assess improvement options and confirm management of the control. Improvement Plan to be developed if required.
	Ineffective	Assess improvement options and confirm management of the control. Improvement Plan to be developed.
Routine	Fully Effective	No Improvement Plan required.
	Mostly Effective	No Improvement Plan required.
	Partially Effective	Assess improvement options for the management of the control.

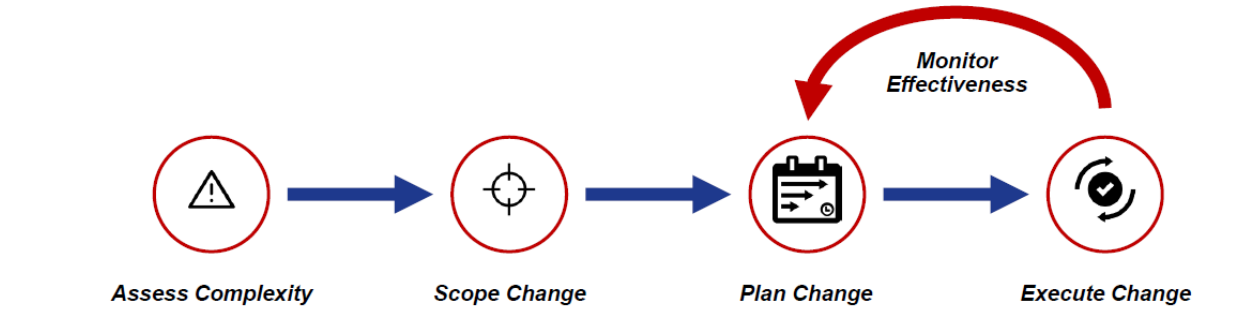
Control Reliance	Control Effectiveness	Control Improvement
	Ineffective	Assess improvement options and confirm management of the control. Improvement Plan to be developed if required.
Trivial	Fully Effective	No Improvement Plan required.
	Mostly Effective	No Improvement Plan required.
	Partially Effective	Assess improvement options for the management of the control.
	Ineffective	Assess improvement options and confirm management of the control. Improvement Plan to be developed if required.

Priority List of Identified Control Improvements

The Formal Safety Assessment Workshops (FSA) conducted in 2016 yielded the following results:

- High Risks – five risk events were rated as High, including the risk "Fire starts involving overhead network assets", Risk ID 34. These risks are in the tolerable region where risk mitigation is considered in accordance with AFAP principles.
- Medium Risks – five risk events were rated as Medium. These risks are in the tolerable region where risk mitigation is considered in accordance with AFAP principles.
- Low Risks – two risk events were rated as Low. This risk is in the broadly tolerable region where risk mitigation is considered in accordance with AFAP principles.
- Negligible Risks – one risk event was rated as negligible. This risk is in the broadly tolerable region where risk monitoring is considered in accordance with AFAP principles.

Appendix 10. ORGANISATIONAL CHANGE MANAGEMENT FRAMEWORK



	Assess Complexity	Scope Change	Plan Change	Execute Change
DELIVERABLES	• Change Complexity Assessment	• Stakeholder analysis • High-level Change Impact Assessment • Risks & Issues register	• OCM Strategy and Plan • Communications Plan • Change Support Network • Training and Learning Plan	• Detailed Impact Assessment • Communications schedule • Readiness checks • Knowledge materials
OUTCOMES	• Project assessed to determine level of change complexity • Level of SP&C involvement known	• Size of change defined • Stakeholders identified • Impact to stakeholders identified	• Change strategies and plans developed • Key messages developed • Stakeholders aware of and engaged in the change	• Stakeholders fully informed of and committed to the change • Stakeholders have the required knowledge and support to sustain the change

Appendix 11. CP-PAL CRISIS & EMERGENCY SEVERITY MATRIX

Category	Tactical (INCIDENT) Managed Locally	Operational (ESCALATION) Management Level	Strategic (CRISIS) Executive Level
Injury to staff, contractor or service provider	Minor injury requiring first aid treatment	Injury or disease requiring medical treatment.	Multiple/ or the potential for multiple significant injuries resulting in hospital admission and/or resulting in more severe consequences. This includes Fatality or permanent disability.
Personal injury to a member of the public involving CP/PAL/UE assets or personnel	Minor injury requiring first aid treatment.	Injury requiring medical treatment.	Hospital treatment of member/s of the public. Potential of significant legal action, including potential criminal charges on CP/PAL/UE or staff member.
Personal asset loss by member of the public		<$100k personal damage to property with alleged involvement of CP/PAL/UE assets.	>$250k personal damage to property with alleged involvement of CP/PAL/UE assets. Threatened legal action. Potential for criminal charges on CP/PAL/UE or staff member.
Information Technology/ Operational Technology	An asset, service or process is either lost, altered, impaired or unavailable that is notably impacting business.	An asset service or process is either lost altered, impaired or unavailable that is seriously impacting business.	Unauthorised or malicious changes to systems or data that impact confidentiality, integrity or availability.
Fire (Grass and or Bushfire)	Localised fire. Minimal impact to CP/PAL/UE assets.	CP/PAL/UE Assets at risk or involved in fire. Coordination with regional or state level emergency services.	Fire/s burning out of control in CP/PAL/UE areas threatening CP/PAL/UE assets or staff. Allegation of CP/PAL/UE assets being involved in starting a substantial fire/s.
Loss of supply	Minimal restriction to supply, managed locally; Possibly resulting in a negligible threat to public safety	Moderate restriction to supply. Complex or multi-jurisdictional event; **1% Customer disruption >24 hrs.** minor load shedding. Potential for increased threat to public safety.	Significant loss of supply. **>2% Customer disruption >24 hrs.** Potentially serious threat to public health or safety. Major load shedding.
Asset Damage	Measurable effect restored locally	Measureable effect requiring complex repairs. Field Resource capacity exhausted	Significant repairs required impacting on operations (20% or more damage).
Major contractor, supplier or partner Issue		Supply or services potentially disrupted with threat to operations.	Impact to a critical business function due to supply or services disruption impacting operations.

Category	Tactical (INCIDENT) Managed Locally	Operational (ESCALATION) Management Level	Strategic (CRISIS) Executive Level
Community / NGO action			Organised campaign or demonstration against the Company that may risk safety or impact operations.
Regulatory authority action		Breach resulting in increased Regulatory attention as an Asset Owner or threat of legal action.	Major breach of legislation. Foreseeable legal action. Major litigation possible
Human Resource and/or Industrial Relations Issues		Disruption affecting operations.	Disruption affecting ability to perform a critical business function.
Terrorism, crime, violence, vandalism or sabotage.		Broad range warning / alert to warn and account for staff. Incident in vicinity of CP/PAL/UE staff or Service Providers. Assets breached, no impact.	Staff member/s confirmed to have been impacted. Confirmed injury by a staff member or service provider of a criminal/terror related incident. Member of staff or contractor suspected of involvement in terror / crime related activities CP/PAL/UE staff or Service Providers witnessing act of terror or crime. Malicious damage to CP/PAL/UE assets.
Business Systems Continuity		Significant disruption of communications, network, applications or hardware. Activation of Business Recovery Team or IT Escalation Team.	Loss of facilities incl. building, communications, network, applications or hardware exceeding BCP Maximum Acceptable Outage affecting critical business functions.
Loss of Capability to undertake emergency activities (i.e. Major Facility / Control Room)		Evacuation of a building/major facility or operational site interrupted. Switch to DR site.	Physical loss / damage to a major facility or control room resulting in loss of system redundancy.
Criminal / negligent allegations			Illegal / negligent act which threatens CP/PAL/UE governance or reputation.
Loss of Senior Personnel		Accident / Illness or Fatality affecting business unit / local operational management capabilities.	Accident / Illness or Fatality affecting CP/PAL/UE-wide management capabilities.

CP-PAL crisis & emergency management system levels

Appendix 12. SAI GLOBAL STANDARD WATCH

SAI GLOBAL

Dear Mr Technical Standards (TSG)

In the last 30 days, there have been no changes to the items you are watching in your list - **TSG List**

STANDARDSWATCH

Your e-mail notification service

We will continue to monitor the items in your list.

Our most popular resources and services include:

- Free Standards
- Free Standards Guides
- Free Standards Newsletters
- Manage your Standard Collections Online
- Apply for permission to copy or network a Standard

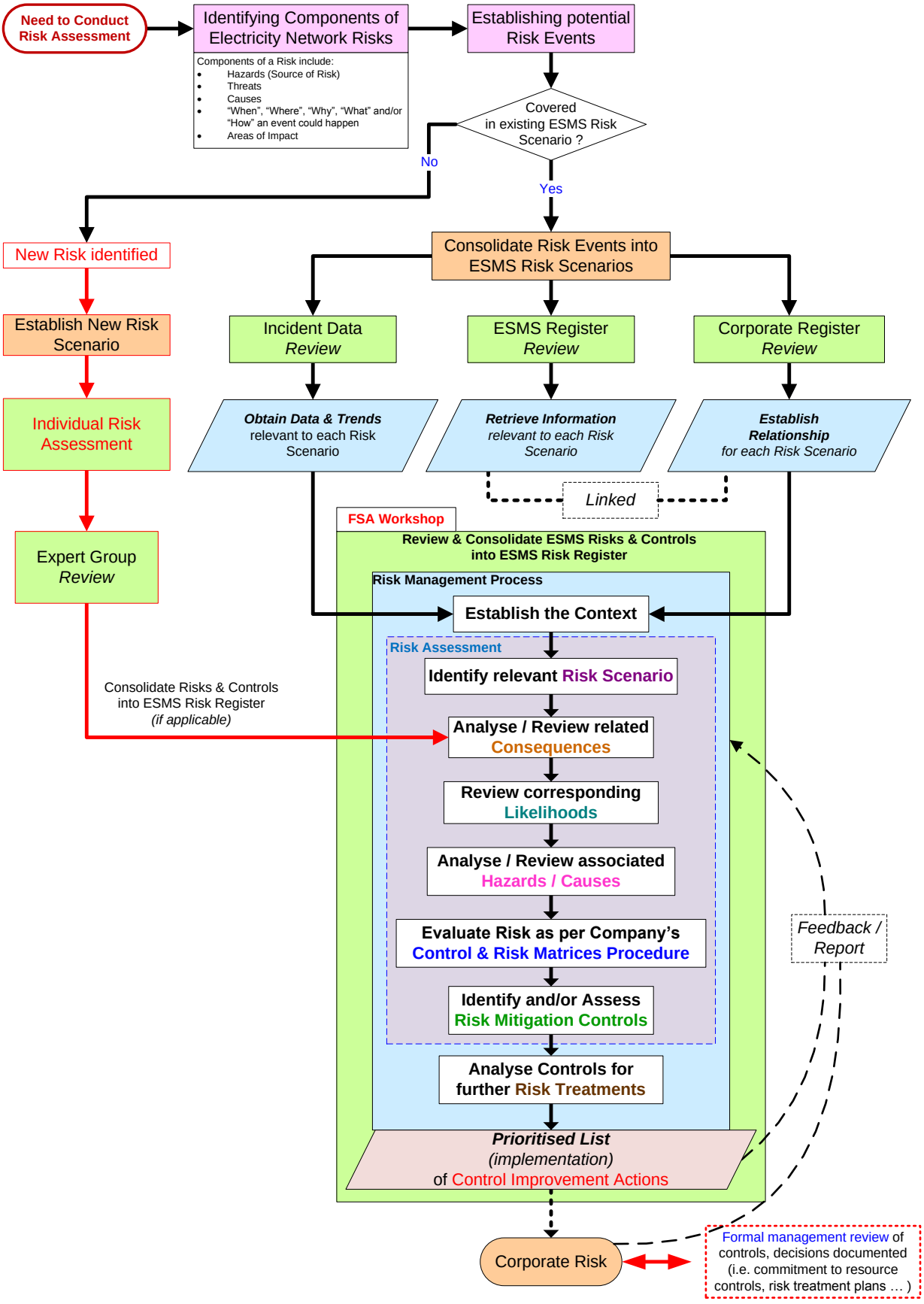
If you would like any assistance locating Standards and Regulatory Services appropriate to your area of operations, please call us.

With Regards

Customer Service
Information Services Division (Asia Pacific)
Within Australia: 131 242 (Press 1)
Outside Australia: +61 2 8206 6010 (Press 1)
standardswatch@saiglobal.com
http://www.saiglobal.com/information

Website: infostore.saiglobal.com/store Email: StandardsWatch@saiglobal.com SAI Global Privacy Policy

Appendix 13. ESMS FSA PROCESS



Appendix 14. METHODOLOGY FOR CALCULATING OVERALL CONTROL CRITICALITY

(Extracted from Corporate "Control and Risk Matrices Procedure" document 13-10-CP0001

Risk Control Score

The risk control score indicates the aggregated contribution of identified controls towards managing a risk.

Each risk is subject to control which is demonstrated by the shift from inherent risk to residual risk. The value that control brings is given by:

Risk Control Score = Inherent Risk Score – Residual Risk Score

Control Criticality Score

The control criticality score provides a guide to deciding which controls are important to the Business and which controls should be audited and at what frequency.

The overall criticality score for each control may be calculated as follows:

Control Criticality = $\sqrt{\sum_{1}^{n}(risk\ control\ score_n \times reliance_n \div confidence\ score_n)^2}$

for each risk where the control is a feature.

The control confidence values are illustrated in the table below.

Control Confidence	Value
Effective	1
Satisfactory	0.9
Improvement Required	0.8
Ineffective	0.7

Appendix 15. RELAYS STANDARD APPLICATION GUIDELINES

STANDARD APPLICATION GUIDELINES	RELAY
Auto Reclose	
Auto Reclose of 1 or 2 Circuit Breakers	SEL351A
MV Bus Auto Reclose	SEL2411
Bus Protection	
220kV and 132kV Bus Differential Protection	GE B30
220kV Bus Differential Protection	GE B90
22kV and 11kV Low Impedance Bus Differential Protection	GE B90
Selective Bus Overcurrent Protection	SEL351A
Single Zone Bus Distance Protection	SEL311A/311C-1
Two Zone Bus Distance Protection	SEL311B/311C-1
Capacitor Bank Protection	
Capacitor Bank Protection and CB Management	SEL351S
Capacitor Bank Neutral Balance Protection and Step Switch Management	GE F35
Capacitor Bank VAR Control	SEL2411
Circuit Breaker Failure	
Back Up for CB Failure Protection	SEL551
Circuit Breaker Protection and Management	
66kV Y CB Fail and CB Management	GE C60
CB Management and CB Fail	SEL351S
CB Management (Remote) – Breaker and a Half	GE C60
CB Management (Local) – Breaker and a Half	SEL451 5
CB Management	SEL2411
Back Up Earth Fault Protection	
Common BUEF and Y MEF Protection	GE F35
Common BUEF and Y MEF Protection	SEL351A
Distribution Feeder Protection	
Back Up Distance Protection	SEL311A/311C-1
Feeder Management	SEL351S
Feeder Management	Siemens 7SJ621

STANDARD APPLICATION GUIDELINES	RELAY
Interconnection Protection	
Generator Interconnection Protection	SEL751
Generator Interconnection Protection	Alstom P341
Line Differential Protection	
Line Differential, Distance and Directional Earth Fault Protection	Siemens 7SD522
Line Differential, Distance and Directional OC and Earth Fault Protection	GE L90
Line Differential, Distance and Directional OC and Neutral Displacement Protection	SEL311L
Line Distance Protection	
Line Distance and Directional Earth Fault Protection	SEL311C-1
Line Distance and Directional Earth Fault Protection	GE D30
Line Distance and Directional Earth Fault Protection	Siemens 7SA522
Line Loss Protection	
Line Overload, Overvoltage/Undervoltage and Line Loss Protection	SEL351-7
Line Overload, Overvoltage/Undervoltage and Line Loss Protection – Type 1	SEL351A
Master Earth Fault	
Master Earth Fault	SEL751A
Neutral Displacement Protection	
Neutral Displacement Protection and Auto Reclose of One or Two Circuit Breakers	SEL351A
Neutral Displacement Protection and Auto Reclose of One or Two Circuit Breakers	SEL351
Transformer Protection	
Transformer Differential Protection	GE T60
Transformer Differential Protection	SEL787-3
Transformer Differential Protection	SEL487E-3
Transformer Monitoring and Mechanical Protection	SEL2414

Appendix 16. ESMS COMMITMENTS

ESMS Commitment	Target Completion Date
Implementation of DMS strategy for the application and future application	Completed
Network Safety Strategy along with AFAP procedure publishing	Completed
ISO55000 alignment	Aligned
Protection and Control Performance Monitoring tracking and monitoring process implementation	Completed
AS 7000 Overhead Line Design compliance	Completed
Implementation of new asset planning & investment tool (Copperleaf)	Completed
Neutral Integrity Fault detection application implementation	Completed
FSA workshop preparation and facilitation guidelines publishing	Completed
ESI Worker System implementation	Completed
Inspection of all LV Dog Bone Services	31/12/2019

Appendix 17. AMS AND ACS SUBJECTS

Asset Management Strategies subjects – the following table lists the asset management strategies that apply across all asset classes:

Asset management strategy subject	Purpose
Asset Operations and Utilisation	Structured approaches to improvements to a range of operational functions which together improve operational performance of the network.
Asset Information and Systems	Asset data and information types, relationships between them and the systems used to manage asset data and information.
Network Performance	Performance improvement programs to meet network reliability and performance requirements over the regulatory period, and an increasingly complex generation and distribution landscape requiring sophisticated technical responses from CP/PAL
Bushfire Mitigation	Structured approaches to prevention of bushfires associated with the design, operation, construction and maintenance of network assets.
Vegetation and Line Clearance	Integration of vegetation and line clearance requirements into the asset management system to align with asset management objectives and ensure ongoing regulatory and statutory compliance.
Connections, Augmentation and Replacement	Improvement programs to manage the connections, augmentation and replacement processes to ensure the network remains capable of distributing a reliable supply of electricity to customers
Asset Maintenance	The rationale behind various maintenance management initiatives, projects and plans that together ensure the right maintenance is delivered at the right time and in the right way.
Network Safety	Integration of network safety practices into the asset management system to ensure visibility of regulatory and statutory compliance obligations, and alignment with asset management objectives.
Future Grid	Technologies and smart networks (including batteries, solar and wind generation, decentralised generation, demand management, metering, demand management) and associated impacts on network design, dynamics, monitoring and corresponding changing skill requirements.
Environment and Sustainability *(planned for future)*	Integration of environment and sustainability requirements into the asset management system to ensure visibility of regulatory and statutory compliance obligations and alignment with asset management objectives.
Asset Management System Performance *(planned for future)*	Description of the strategies and objectives that CP/PAL use to measure asset management system performance, and ensure optimum asset management system effectiveness, efficiency and continued alignment with the SAMP objectives.
Asset Management System Resources *(planned for future)*	The assessment, selection, development, procurement or acquisition, deployment and application of human and non-human resources required to develop and implement the CP/PAL asset management system, and implement and monitor the asset management objectives.

Asset Class Strategies – the following table lists the asset class strategy subjects and the asset coverage of each strategy:

Asset class strategy	Asset coverage
Poles and towers	Wood, concrete, and steel poles Steel lattice towers
Pole top structures	Pole top structures including crossarms and insulators HV fuses Surge arresters
Overhead conductors	Bare conductors (aluminium, copper, steel) High voltage aerial bundled cable Low voltage aerial bundled cable Covered conductor
Underground cables	Subtransmission, high voltage and low voltage cables Cable pits Cable pillars Auxillary services Cascade LV lighting cables
Zone transformers	Zone substation transformers, regulators and autotransformers Transformer bushings Transformer tap changers Transformer water cooling systems
Distribution substation plant miscellaneous	Regulators Capacitors Capacitor balancing units
Public lighting	Luminaires PE cells Brackets
Zone substation plant miscellaneous	Capacitor banks Capacitor bank step switches Reactors Static VAR compensators Instrument transformers Surge diverters Steel work Fire walls Neutral earth resistors (NER) Rapid earth fault current limiter (REFCL) systems Direct current (DC) supply systems Station low voltage (LV) supply systems
Distribution transformers	Pole transformers Kiosk transformers Ground transformers Indoor transformers

Asset class strategy	Asset coverage
SCADA and communications	Optic fibre cable Supervisory cable Digital microwave radio Cellular radio Voice over IP (VoIP) system RTUs
Zone switchgear	Circuit breakers Switchboards Outdoor busses Switches
Protection and control	6.6kV, 11kV, 22kV, 66kV and zone substation protection schemes and relays Line and feeder protection schemes Bus and station protection schemes Transformer protection schemes Cap bank protection schemes
Property and facilities	Zone substation buildings Zone substations leases Non kiosk ground or below ground distribution substations Communications buildings
Metering	AMI network communications AMI single phase direct connected meters AMI three phase direct connected meters AMI LV CT connected three phase meters. Low voltage metering current transformers Pole top high voltage metering VT & CT transformers (CP/PAL owned) Boundary metering HV & EHV Zone substation metering transformers (CP/PAL owned) Legacy type 5 MRIM Meters Legacy type 6 (basic) Meters Timber meter boards (includes CP/PAL owned fuse or facia mounted service protective device (SPD) holders and neutral links)
Distribution switchgear	Circuit breakers Automatic circuit re-closers (ACRs) Switches Ring main units (RMUs)
Service lines	Overhead low voltage service assets Service cable attachment fittings Service protection devices Junction boxes

Appendix 18. ESMS KEY UPDATES

The table below summarises the key updates of ESMS post ESV acceptance of version 3.24:

Key updated sections	Key updates summary
Section 1. Basis of ESMS (Introduction)	Updated CP-PAL network statistics in section 1.7 based on latest data. Updated figures include: - Figure 1-3 - Figure 1-5 - Figure 1-14
Section 3. Planning	Updated sections 3.1 - 3.3 based on revised ERM framework[199]. Key updates include revisions to following tables naming convention changes as per revised ERM framework: - Consequences - Likelihood - Control Confidence tables
Section 4. Implementation – Risk Controls	Updated the following: - Section 4.2.1 based on revised Crisis Management Plan[200] - Section 4.2.3 asset management system and section 4.3.4 asset maintenance based on ISO 55000 alignment project. Key updates include updated Table 4-7 for pole maintenance inspection intervals.

[199] Enterprise Risk Management Framework – JEQA4UJ443MT-154-354

[200] Crisis Management Plan – JEQA4UJ443MT-154-386