Meeting Date: 8 August 2019

# THE SYSTEM OPERATOR'S BUSINESS CONTINUITY PLANNING AND INCIDENT MANAGEMENT

SECURITY AND RELIABILITY COUNCIL

Transpower, in its capacity as the system operator, will attend the 8 August 2019 SRC meeting and give a presentation about its business continuity planning and incident management.

**Note:** This paper has been prepared for the purpose of the Security and Reliability Council. Content should not be interpreted as representing the views or policy of the Electricity Authority.

# The system operator's business continuity planning and incident management

## Background

The 8 August 2019 SRC meeting was scheduled with less advance notice than usual, as it was in response to an invitation from the Electricity Authority Board to join them for a meeting and lunch. As the timing and other agenda items firmed up, the secretariat identified the opportunity to add a paper early in the day.

At its 20 June 2019 meeting, the SRC received a paper from its secretariat about the Risk Management Framework.[1] An appendix to that paper contained a dashboard of 30 topics, ranked by risk. The third item on that list was "SRC could obtain information on the system operator's emergency preparedness and business continuity planning."

The secretariat asked the system operator whether they could provide a paper or presentation to the 8 August 2019 SRC meeting on the almost identical topics of 'business continuity planning and incident management'. These are topics the system operator is preparing for an Authority Board committee. The system operator advised it would not be able to meet the deadlines for the pack of SRC papers, but could provide a presentation at the SRC meeting.

As such, the system operator will attend the 8 August meeting to present on the topics of business continuity planning and incident management. There are no slides or papers attached to this paper.

## Questions for the SRC to consider

The SRC may wish to consider the following questions.

**Q1. In light of how the system operator plans on managing an incident, does the SRC have any views on how well aligned their plans are with the other industry participants involved in managing an incident?**

**Q2. What further information, if any, does the SRC wish to have provided to it by the secretariat?**

**Q3. What other advice, if any, does the SRC wish to provide to the Authority?**

[1] Available from https://www.ea.govt.nz/development/advisory-technical-groups/src/meeting-papers/2019/src-meeting-20-june-2019/

# BUSINESS CONTINUITY PLANNING / MAJOR INCIDENT MANAGEMENT

**ELECTRICITY AUTHORITY – SECURITY AND RELIABILITY COUNCIL**


## MATT COPLAND

**SO POWER SYSTEMS GROUP MANAGER**

TRANSPOWER


**AUGUST 2019**

**POWERING NEW ZEALAND TODAY + TOMORROW**

# PURPOSE

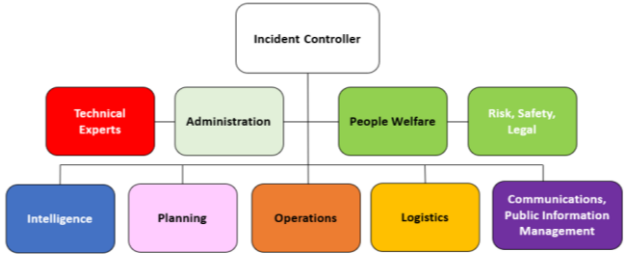
The purpose of this presentation is to:

- Provide an overview of the System Operator's business continuity (BCP) preparations including:
  - Approach to responding to BCP incidents
  - Identified threats, controls and assurance
- Provide an overview of the System Operator’s preparations for an operational response to a major incident including:
  - What could cause a major incident
  - Key risks and controls

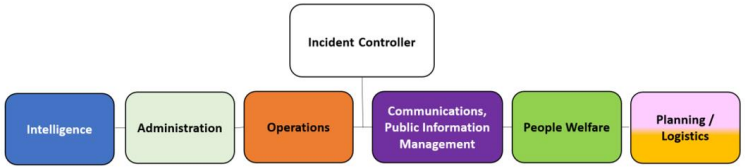
# BUSINESS CONTINUITY PLANNING

# BUSINESS CONTINUITY PLANNING - CIMS

- Transpower utilises the coordinated incident management system (CIMS) approach for incident management
  - Separate system operator and grid owner incident management teams (IMT)
- Scalable based on the size of the incident
- Standard approach used in New Zealand
  - Provides a common language and approach for inter-agency interactions
  - Government agencies, Civil Defence, Police, Fire and Emergency Services
- Still developing our CIMS maturity
  - 17 system operator staff trained in CIMS
  - Annual facilitated BCP exercise
  - Annual South Island simulated black start restoration exercise

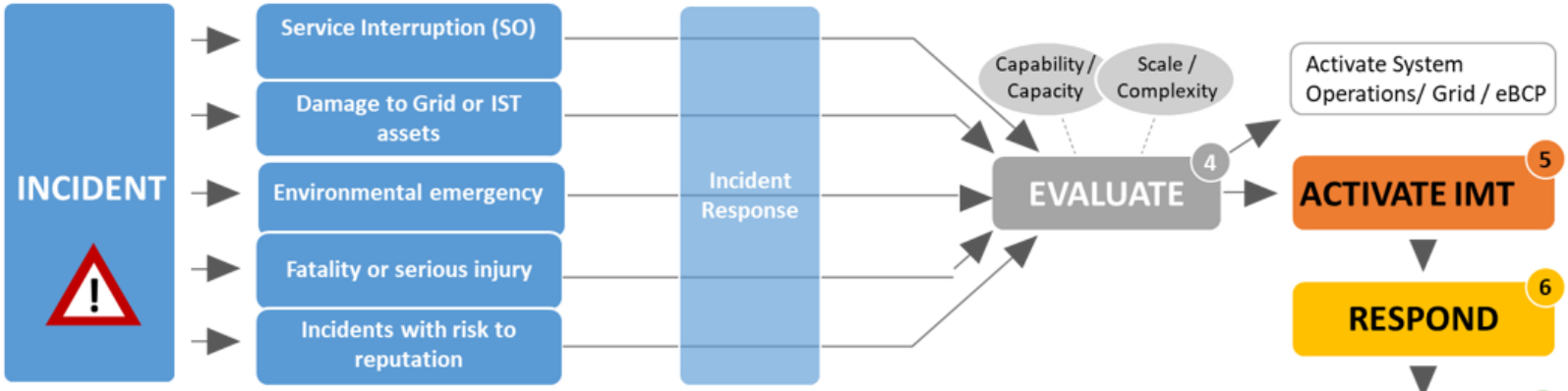



Full CIMS IMT




Scaled down CIMS IMT

# INCIDENT MANAGEMENT OVERVIEW




| | |
|---|---|
| PEOPLE | SAFETY – Is everyone safe?<br>WELLBEING – Are we looking after our peoples wellbeing?<br>FATIGUE – Are we managing the team's wellbeing? Do we have alternates for shifts? |
| ASSETS AND LOCATIONS | DAMAGE – Have our assets been damaged? Have customer assets been damaged?<br>LOCATION – Is the location / site still available to us?<br>CONTAINED – Is further damage or flow-on damage to be expected? |
| SERVICES | EXTERNAL – What is the impact on our customers and external stakeholders? Has there been a major outage?<br>MARKET – Has the market been impacted?<br>INTERNAL – What is the impact on our internal services? |
| REPUTATION | AWARENESS – Is the public /media aware of the event?<br>STAKEHOLDERS – Do we know who to communicate with and how frequently?<br>CUSTOMERS – Do we know who is impacted? How are we communicating with them? (CAN) |

# BUSINESS CONTINUITY PLANNING – BEING PREPARED

- Identified threats to **our people** which could impact on business continuity

| Threat | Preparation / Response | Assurance |
|---|---|---|
| **Aging workforce** | Succession identification and planning | Annual skill gap and needs analysis (critical people, critical roles); three-monthly performance agreement discussions |
| **Widespread illness** | Cross-role skill training; working from home technologies; pandemic plan | Health and safety audits |
| **Lack of skilled staff** | Succession identification and planning; proactive skill-based recruiting | Annual skill gap and needs analysis (critical people, critical roles); three-monthly performance agreement discussions |
| **Lengthy training requirement** | Succession identification and planning; proactive skill-based recruiting; dedicated training function | Annual skill gap and needs analysis (critical people, critical roles); three-monthly performance agreement discussions; six-monthly performance testing of critical skills staff |
| **Single points of failure (knowledge or skills)** | Cross-role skill training; succession planning | Annual skill gap and needs analysis (critical people, critical roles); three-monthly performance agreement discussions |

# BUSINESS CONTINUITY PLANNING – BEING PREPARED

- Identified threats to **our facilities** which could impact on business continuity

| Threat | Preparation / Response | Assurance |
|---|---|---|
| **Loss of facility** | Critical site redundancy and resilience; virtual control centre; working from home technology | Weekly inter-site fail-over testing; weekly stand-alone dispatch (SAD) testing; control room simulation testing; annual CIMS simulation exercises |
| **Power Supply Loss** | UPS battery systems, on-site diesel generators | Regular scheduled testing of facilities services |
| **Transport Infrastructure failures** | Working from home technology | Technology review and testing; |
| **Failure or compromise of security systems** | Working from home technology; facility service agreements | Security audits; annual CIMS simulation exercise |
| **Sabotage or terrorist threat** | Security systems; critical site redundancy and resilience; virtual control centre; working from home technology | Security audits; weekly inter-site fail-over testing; weekly stand-alone dispatch (SAD) testing; control room simulation testing; annual CIMS simulation exercises |
| **Natural disaster, earthquake, tsunami, flood, hurricane, tropical storm, bush fire** | Critical site redundancy and resilience; virtual control centre; working from home technology; 0800 WHAT TO DO (Transpower's internal communications helpline) | Weekly inter-site fail-over testing; weekly stand-alone dispatch (SAD) testing; control room simulation testing; annual CIMS simulation exercises |

# BUSINESS CONTINUITY PLANNING – BEING PREPARED

- Identified threats to **our tools** which could impact on business continuity

| Threat | Preparation / Response | Assurance |
|---|---|---|
| **Loss of tools** | Critical IST site redundancy and resilience; system enhancements; support service agreements based on service criticality | Weekly SCADA and market system performance testing; monthly cyber security testing, cyber security audits and control testing |
| **Loss of Market System functionality** | Critical IST site redundancy and resilience; system enhancements; support service agreements based on service criticality | Weekly SAD testing; control room simulation testing; annual CIMS simulation exercises |
| **Breach of system security** | Software updates and patching processes; international system knowledge base; industry groups membership | Weekly SCADA and market system performance testing; monthly cyber security testing, cyber security audits and control testing |
| **Loss of communication and information paths (e.g. SCADA)** | Critical IST site redundancy and resilience; System enhancements; support service agreements based on service criticality; alternative email and communication paths (Fleet-link radio, SAT phones) | Weekly SAD testing; control room simulation testing; annual CIMS simulation exercises |

# MAJOR INCIDENT MANAGEMENT

# WHAT IS A MAJOR INCIDENT?

| | |
|---|---|
| **Power system incident** | • A non-credible contingency event<br>• Multiple contingency events<br>• Multiple repeated events over a short period impacting industry or consumers<br>• Delayed or failed restoration after an incident that widely impacts industry or consumer |
| **Loss of supply or load shedding** | • An Automatic Under Frequency Load Shedding “AUFLS” or AUVLS (“Volts”) activation<br>• A regional loss of supply greater than 150MW for 4 hours (600MWh or >$10m value of load loss)<br>• A significant regional impact from a loss of supply e.g. Sustained multi-day loss of the West Coast<br>• A deliberate use of manual load shedding due to insufficient generation or reserves |
| **Role specific failure** | • An unplanned loss of Market System impacting market participation for more than one hour<br>• An unplanned loss of SCADA impacting management of the power system for more than one hour<br>• An unplanned outage of significant asset impacting supply or management of the power system<br>• A failure to meet Principal Performance Obligations that results in loss of generation or load |

# TRIGGERS & IMPACTS

- Weather or environmental event – storm, snow, earthquake, volcanic activity, solar activity
- Human or process error in the control room, in the field or connected party (typically related to change management).
- Malicious act – either cyber or physical

**Loss of Assets Grid/Generation**

**Power System Failure**

- Wide spread loss of the power system.
- Loss of Control Tools (e.g. SCADA or Dispatch System)
- Incorrect standing data, modelling or system error
- Human or process error in the control room, in the field or by connected party.
- Malicious act – cyber or physical

- Cascade Failure resulting in
  - Regional Separation
  - Island Blackout
- Severe Degradation in quality. e.g. brownout.
- Rolling Outages
- Loss of Supply
- Market Failure

**Major Incident**

# KEY RISKS & CONTROLS

| Identified Risks | Controls | Tools | Comment |
|---|---|---|---|
| Loss of Grid Assets through weather or environmental impact | Maintenance and Asset Management<br>Situational Awareness | RTCA (Contingency)<br>LTS2005 (Lightning)<br>SDTF (Distance to Fault)<br>MetService, Solar<br>FENZ (Emergency) | Introduced a risk based approach to circuit re closure.<br>Increased focus on asset management and enhanced resilience for critical assets with single points of failure.<br>Continued investment is underway enhancing situational awareness regarding faults |
| Power System Failure Regional Black Out or Black Island | Ancillary Service Contracts in place with two Generator sites in each island.<br>Regional and Black Island Plans<br>Experienced Controllers | OFA (Over Frequency Arming)<br>CSS tools (Automated Pre-prepared Switching Sequences) | Regular black start testing to confirm operability<br>Exercises run with industry annually in each island<br>Regional Contingency Exercises run with industry |
| People and Process Compliance (including errors in standing data, modelling or systems) | Trained Coordinators<br>Audits, Event Reviews<br>Quality Frameworks | Document System<br>TTSE (Simulation Environment)<br>ICAM | Documentation is all on controlled review cycle.<br>Training programme ensures all coordinators practice NI and SI major events scenarios developed to simulate pressure environment.<br>Robust method for identification of root causes and remedial actions. |

# KEY RISKS & CONTROLS

| Identified Risks | Controls | Tools | Comment |
|---|---|---|---|
| Loss of Access to Control Tools | BCP Standard Operating Procedures | SAD (manual dispatch) | Dual Locations in Hamilton and Wellington. We now have a warm standby capability to dispatch in Auckland and Christchurch. Medium term objective to have all Power System operating tools available in all 4 locations. |
| Loss of Generation Asset | Extended Reserves, Equivalences<br>Review post events<br>Relationship with providers | RMT | Increased focus on sharing of outage and other information has been well received by industry . This programme is ongoing and includes audio conferences ahead of major outages for industry input and transparency. |
| Malicious Act by a Third Party | Security and Risk Management Control Rooms require two layers of physical controlled entry. | Cyber Security Tools<br>Physical Security<br>Exit Processes | Physical checks following the recent government issued national High Security warning highlighted a gap in physical security at our Auckland location. This has now been addressed. |

# CONCLUSIONS

- Robust business continuity planning is in place
- CIMS allows for a co-ordinated inter-agency response
- Active threat identification and control assurance in place
- Regular exercises to practise our skills and test plans
- Learning and evolving based on our performance responding to incidents
- Our maturity in this area is still developing and remains a focus