United Energy

Review of United Energy IT Systems

FINAL report version EXTERNAL 1.0
16 September 2019

Contents

01. Executive Summary

The acquisition of United Energy (UE) introduced a separate IT environment into VPN

EXECUTIVE SUMMARY

United Energy's (UE) IT environment continues to operate separately from VPN's IT environment.

- In 2018 Victorian Power Networks (VPN's) parent company **Cheung Kong Infrastructure (CKI) acquired the DUET Group**.
- As a result **United Energy's (UE's) IT** systems, processes and people were effectively **acquired by CHED Services**.
- Following the acquisition the **immediate focus was on continuing to operate and run UE's IT environment**, and retain and transition knowledge to CHED Services.
- **Minimal integration of UE and VPN IT systems and networks** has occurred, and the two IT environments continue to run separately today.
- A key reason for maintaining separate IT environments in the immediate term was to **isolate any potential operational risks and security threats** arising from the UE IT environment.

UE's IT program of work for the 2021-2025 regulatory period forecasts an ~35%-40% uplift in capital expenditure.

- Due to recent periods of instability and several security audits, it is anticipated that **the current "health" of UE's systems is contributing in large part to the uplift in IT capital expenditure** for the next regulatory period.
- The health of the systems may be further compounded by changes in the IT architecture, movement of key staff with tacit knowledge, and changes to the strategic direction of the technology landscape.

In light of this uplift, VPN's Regulatory team commissioned an independent review of UE's IT systems.

- The purpose of the review was to understand the history of UE's IT systems and the implications for stability and security, **identify key stability and security issues**, understand existing and proposed work to address the issues, and **recommend any additional remediation** required.
- The review was conducted over a **six week period**, and was based on **document review**, **IT operational data**, and **stakeholder interviews** across the business and IT.
- The review was structured around industry **standard frameworks** for **IT asset lifecycle management, IT operations, and cyber security**.

VPN inherited a number of UE’s IT stability issues and security risks which it has sought to remediate

EXECUTIVE SUMMARY

Most of the recent stability challenges are associated with existing UE IT architecture decisions.

- The **majority of UE’s corporate and some key operational (DMS and UiQ) IT systems were hosted on the Supercluster platform**, resulting in a high level of dependency on this platform in order for UE’s IT and OT systems to be available to business users
- A key issue with the existing Supercluster architecture is the **inability to run the full production environment in an alternate site on failure** – as evidenced during the major 11 day outage in June 2018
- An initiative is currently underway to **re-architect UE’s primary application hosting platform, the Supercluster,** to address significant performance, stability and resilience issues
- The in flight Supercluster remediation initiative is **migrating critical applications** to an alternative platform **however, non critical applications will remain** on the Supercluster platform pending approval of a subsequent phase of work to migrate them
- The offshore Customer Technology **customer servicing** team is **dependent on an unstable mailbox** rather than a strategic CRM solution.

A number of initiatives are underway to address identified security risks.

- Recent internal audits and penetration tests highlighted **significant risk areas requiring remediation**
- In particular, the audits and tests identified the need to:
  - **Increase the security of the network** from unauthorised external access
  - **Secure the boundary between corporate and operational technology domains** to contain access and increase safety.
- There are also opportunities to **increase vulnerability management and threat detection** through improved monitoring of IT assets and IT operational processes.

Unplanned non-recurrent initiatives totalling ~$18M are underway to help remediate known issues

EXECUTIVE SUMMARY

This review of UE's IT Systems focused on the four areas below as requested by VPN:

1. Evaluate all IT categories, both recurrent and non-recurrent, applying at the program level.

- A number of stability and security issues are under remediation, estimated at **~$18M * in unplanned non-recurrent costs in 2018**, including:
  - Workplace Technology is **rebuilding core IT foundations (e.g SuperCluster, refreshing legacy network devices)**
  - Network operations is focussed on **domain segregation**
  - Customer Technology is **responding to compliance issues**, e.g. Life Support
  - IT Operations (Run) is **consolidating systems and improving reporting**.
- Some of these activities will result in an **uplift to future recurring costs**, including:
  - Maintaining currency of newly **reinstated SAP support**
  - New **core infrastructure platforms** such as the Supercluster replacement
  - **Refreshed network devices**.

2. Evaluate IT system health, stability and security according to good asset management practices.

CHED Services inherited an IT capability with limited:

- **IT governance, strategy, architecture**, operational processes, business alignment
- **Maintenance and support contracts (IT lifecycle management)** - critical support contracts expired or exited, limiting UE IT ability to obtain maintenance and support from vendors for IT assets
- **Formal IT risk management** or security controls
- Resilience and no effective **DR for critical applications**.

3. Consider work undertaken during the 2016-2020 period and the IT system implications for the 2021-2025 period.

- Current remediation activities will provide an **improved foundation for IT for the 2021-2025 period**, in particular:
  - Re-engaging strategic SAP support for growth
  - Implementing some IT controls to manage risk and threats
  - In sourcing and right sourcing to simplify the operating model.

4. Identify additional remedial activities required to supplement projects in the proposed 2021-2025 IT portfolio.

Many in flight remediations are anticipated to be completed in the current regulatory period. If scoped correctly, they are intended to enable and support delivery of projects in the proposed 2021-2025 IT portfolio. Remediations include:

- **Continued prioritisation of the Service Improvement Program** to uplift operational performance management
- Conducting a **full review of UE's DR capabilities** with a risk assessment, and a refresh of priorities for critical DR services
- Implementing an **IT operational risk framework**
- **Integrating security and threat management** with the ServiceNow IT service management tool.

The full recommendations can be found in the following section.

Note:

- * ~$18M remediation cost referenced from the following documents provided:
- UE Infrastructure Remediation 16 August 2018 V4 (UE Template).pptx
- UE Investment Committee _Supercluster_Remediation Gate B v2.1.pptx

Additional remediation opportunities exist to further improve UE IT (1)

EXECUTIVE SUMMARY

IT Domain	Additional remediation initiative	Description	Priority	Duration Estimate
IT Governance	**IT Risk Framework Development**	Design and implement an IT operational risk framework.	In progress	6-12 months
IT Governance	**Create / refresh and maintain enterprise IT architecture**	Establish an enterprise architecture capability to create / refresh and maintain an accurate and current view of the UE IT architecture landscape.	Started	12 months (enduring activity)
IT Resilience	**Disaster Recovery Review**	Conduct a detailed review of disaster recovery capabilities, including a deep dive and risk assessment of the current status of DR in UE. Specifically: ● Review and refresh the DR policy and process ● Determine how to obtain greater alignment with business requirements, BCM, and VPN ● Document known risks where testing history is unknown and has not occurred. Note: A number of existing DR issues are captured, but are not logged as risks.	High	3-6 months
IT Lifecycle Management (Maintenance and Support)	**Production and Non-production Environment Review**	Understand the risks that exist through differences in production and non-production environments: ● Perform a gap analysis of the current non-production environments against the current production environments to ascertain the scale of misalignment ● Risk assess the gaps discovered, and prioritise mitigation plans required to address known gaps and risks ● There may be an opportunity to align this to broader service based risk reviews (see above) linked to an understanding of software and hardware support.	Medium - align to immediate change plan to prioritise and schedule as required	3-6 months

Status / Priority Rating Key:

- In progress: In flight > 1 month
- Started: Recently mobilised < 1 month
- Not Started - High: Mobilise in next 0-3 months
- Not Started - Medium: Mobilise in next 6 months
- Not started - Low: Mobilise in next 12 months

Additional remediation opportunities exist to further improve UE IT (2)

EXECUTIVE SUMMARY

IT Domain	Additional remediation initiative	Description	Priority	Duration Estimate
IT Service Management	**Service Improvement Program** incorporating a detailed Problem & Incident Management Review	**Ensure that the Service Improvement Program** has priority and focus on critical uplift of operational performance management, including: ● Conducting a detailed review of **problem and incident management**, and other core IT Service Management processes ● **Baselining the performance** of all core IT Service management processes ● Identifying improvement opportunities to increase performance in the **investigation and identification of root cause problem management** ● Uplifting and implementing governance, and **SLA and KPI driven performance management**. Note: A Service Improvement Plan (SIP) exists. Data provided is high level and does not include detailed plans, targets or results achieved to date, therefore the priority, status, progress and outcomes of the SIP are presently unclear.	In progress	6-12 months
IT Service Management	**Vendor Support Review**	Prioritise and schedule a series of reviews to identify issues and risks related to the currency of software and hardware support for critical services. Include: ● Identification of gaps related to key IT assets underpinning critical services / applications ● Performing appropriate risk assessments, and accepting or planning to remediate as required ● Ensuring all relevant service owners in UE IT and the associated business area are aware and have transparency of the risk position.	High	6-12 months
IT Service Management	**Managed service provider rationalisation**	● Simplify the operating model by consolidating Infrastructure services onto a single managed service agreement for CHED Services	In progress	6-12 months

Status / Priority Rating Key:

- In progress: In flight > 1 month
- Started: Recently mobilised < 1 month
- Not Started – High: Mobilise in next 0-3 months
- Not Started – Medium: Mobilise in next 6 months
- Not started – Low: Mobilise in next 12 months

Additional remediation opportunities exist to further improve UE IT (3)

EXECUTIVE SUMMARY

IT Domain	Additional remediation initiative	Description	Priority	Duration Estimate
IT Service Management	**Define business services**	Scope a project to define and document business services, including service definitions and alignment of business services to technical services and configuration baselines. Note: This initiative is referenced in the SMO service improvement plan, however, the current detail is high level and is not sufficient to determine the scope, objective, timing or coverage and how this will create greater business and IT alignment. It is anticipated there is a dependency on completion of the in flight ServiceNow discovery project to provide accurate IT asset and service configurations that define IT services that will underpin business services.	Medium	3-6 months
Cyber Security	**Privileged Access Management**	Design and implement a privileged access management process that governs elevated access and controls segregation of duties.	High	3-6 months
Cyber Security	**Security Threat Profiling**	● Embed enduring security threat profiling into an operational risk process ● Align threat profiling to an enduring enterprise risk framework that enables ongoing governance, identification and treatment of new and emerging threats.	Medium	6-12 months
Cyber Security	**Joiners, Movers, Leavers (JML) process Update**	Review and enhance the JML process to include controls for identity management, and automated identity access removal when employees change roles or leave the organisation.	High	3-6 months

Status / Priority Rating Key:

- In progress: In flight > 1 month
- Started: Recently mobilised < 1 month
- Not Started – High: Mobilise in next 0-3 months
- Not Started – Medium: Mobilise in next 6 months
- Not started – Low: Mobilise in next 12 months

Additional remediation opportunities exist to further improve UE IT (4)

EXECUTIVE SUMMARY

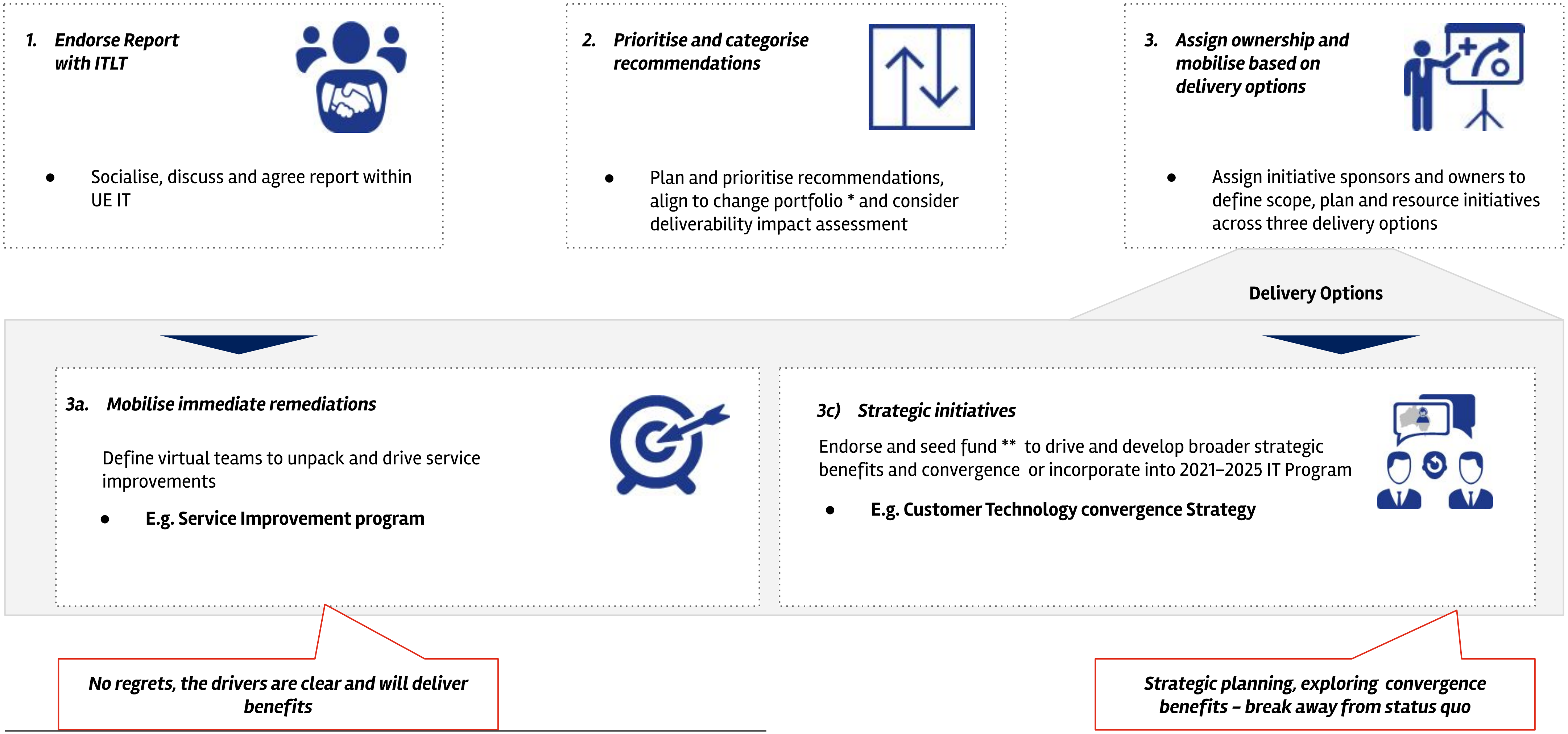
IT Domain	Additional remediation initiative	Description	Priority	Duration Estimate
Cyber Security	**Security and Service Management Integration**	**Integrate Threat and Vulnerability Management (Tenable) with the Enterprise CMDB (ServiceNow)** to enable vulnerability scanning against an approved and accurate asset inventory baseline to improve the accuracy of scanning results. **note:** this initiative has a key dependency on completion of the in flight BAU ServiceNow discovery project.	Medium	3-6 months
Business Alignment	**Customer Technology Strategy**	Develop a **strategy for Customer Technology**, in order to: ● **Remove UE CRM-related stability issues** by automating some manual processes associated with the Probe contact centre in the Philippines, ahead of on-shoring in preparation for FIRB compliance ● **Plan the migration of VPN billing system** from the legacy CIS-OV system used in VPN to the UE IT strategic billing platform (e.g. SAP-ISU). Note: A Customer Technology Roadmap exists and is under an update and refinement process. However, the mobilisation and implementation of the roadmap and its recommendations are not currently funded.	In progress	0-6 month Strategy, scope and plan 2-4 yr Implementation

Status / Priority Rating Key:

- In progress: In flight > 1 month
- Started: Recently mobilised < 1 month
- Not Started - High: Mobilise in next 0-3 months
- Not Started - Medium: Mobilise in next 6 months
- Not started - Low: Mobilise in next 12 months

Additional remediation must be prioritised and aligned to appropriate delivery options

EXECUTIVE SUMMARY



1. ***Endorse Report with ITLT***

- Socialise, discuss and agree report within UE IT

2. ***Prioritise and categorise recommendations***

- Plan and prioritise recommendations, align to change portfolio * and consider deliverability impact assessment

3. ***Assign ownership and mobilise based on delivery options***

- Assign initiative sponsors and owners to define scope, plan and resource initiatives across three delivery options

Delivery Options

3a. Mobilise immediate remediations

Define virtual teams to unpack and drive service improvements

- **E.g. Service Improvement program**

3c) Strategic initiatives

Endorse and seed fund ** to drive and develop broader strategic benefits and convergence or incorporate into 2021-2025 IT Program

- **E.g. Customer Technology convergence Strategy**

No regrets, the drivers are clear and will deliver benefits

Strategic planning, exploring convergence benefits – break away from status quo

Notes:
* alignment of recommendation to existing strategic change portfolio
** provide seed funding to plan and validate greater strategic options that can optimise ongoing spend through to end of next regulatory period 2025

02. Context

Over the past 10+ years changes in UE's operations led to varying IT operating models & IT architectures

CONTEXT

Pre-2009

UE IT outsourced to Jemena

- United Energy's operations including **IT are fully outsourced** to Jemena under a long term operational services agreement
- Majority of **IT systems are shared** with Jemena
- Management and operation of all IT systems performed by Jemena, and third parties engaged by Jemena
- **Minimal IT organisation resided within United Energy** (e.g. approx. 3 FTEs)
- From 2009 (approx.) **planning** commenced to establish a **greenfields**, **standalone IT capability for UE** (and Multinet Gas) to coincide with the end of the operational services agreement.

2010

UE IT brought in-house

- Implementation of **SAP ECC6** to provide **ERP, asset management and billing** system functionality
- Business processes designed to adopt SAP standard processes
- **Transition of network management systems and OT** (e.g. DMS, OMS, SCADA) back to UE IT
- Establishment of an **IT organisation** including CIO, Architecture, Service Management
- Establishment of a **managed services agreement** with Accenture to provide infrastructure and application management services
- Commencement of the implementation of **AMI IT capabilities** in conjunction with Jemena, including UIQ, Itron, and a separate SAP-ISU instance for MDM, asset management, and billing system functionality.

2011-2016

Changes to UE IT environment

- Organisation-wide **cost reduction initiative** implemented in 2015
- Project Rightsize initiated to **consolidate the IT environment**, including the transition of systems to the Supercluster platform
- Issues encountered with the Supercluster platform after its deployment
- **Design choices and budget constraints** during Project Rightsize are thought to have contributed to performance issues, including[1]:
  - Only **partial redundancy** was implemented
  - **Operation and maintenance impacts not considered** (e.g. design did not encompass rolling patching)

2017 onwards

Transition to CHED Services

- **May 2017** – CKI buys DUET Group and retains service contracts with Accenture for service management and application support, and with ASG for infrastructure and network support
- **January 2018** – CHED Services identifies deviations from security best practice[1]
- **February 2018** – UE's Service Management Office goes live and brings service management support in-house
- **June 2018** – major Supercluster outage, lasting 11 days, affecting all UE IT systems and requiring BCP practices to be implemented
- **July 2018** – Application management services go live, transferring application support from Accenture to Wipro
- **October 2018** – Network support contract is transferred from ASG to Dimension Data
- **February 2019** – Multinet Gas separates from United Energy[2].

Decisions & changes made during UE's previous ownership impact the current stability & security of IT

Notes:-

[1] Anecdotal evidence based on UE stakeholder interviews.

[2] Multinet Gas, also formally owned by the DUET Group, shared some IT systems with UE. It is understood at the time of writing that some IT systems are yet to be separated and are still shared.

03. Approach

Scope of this review was the stability & security of UE's regulated IT systems and necessary remediation

SCOPE

Scope of this review

VPN defined the following scope for this review:

- Review the health, stability and security of the IT Systems at United Energy, including:
  - Evaluation of all IT categories, both recurrent and non-recurrent, applying at the program level
  - Evaluation of the health, stability and security according to good asset management practices
- Consider work undertaken during the 2016-2020 regulatory period and describe the implications for the IT portfolio ver the 2021-2025 regulatory period
- Provide a set of recommendations of remediation activities required in addition to those currently being undertaken, and activities required to maintain the stability and health of the system in the 2021-2025 period. (The quantification of the cost of remediation activities and IT systems which serve un-regulated activities is out of scope)

Key questions addressed

In response to this scope, the review set out to answer the following key questions:

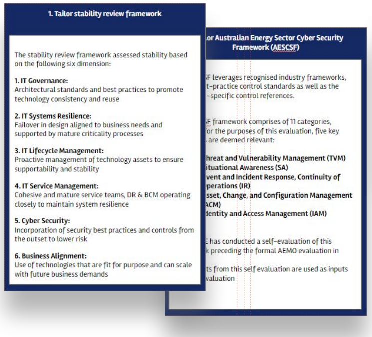
- How does UE's IT environment enhance or detract from IT stability and security?
- How does the management and operation of UE's IT environment enhance or detract from IT stability and security?
- What initiatives are underway in the current regulatory period (2016-2020) to remediate known stability and security issues?
- What additional initiatives are required in the next regulatory period (2021-2025) to remediate, or help prevent, stability and security issues?

Key inputs for this review

The following inputs were obtained to address the key questions, in conjunction with tailored stability and security frameworks based on industry standard practices:

- IT infrastructure architecture including DR capability
- Customer Technology, Workplace, and Network Management application portfolios
- IT operations including service management
- IT operating model including third party service providers
- Cyber security
- IT programs of work for the 2016-2020 and 2021-2025 regulatory periods

Tailored review frameworks



1. Tailor stability review framework

The stability review framework assessed stability based on the following six dimension:

1. IT Governance:
Architectural standards and best practices to promote technology consistency and reuse

2. IT Systems Resilience:
Failover in design aligned to business needs and supported by mature criticality processes

3. IT Lifecycle Management:
Proactive management of technology assets to ensure supportability and stability

4. IT Service Management:
Cohesive and mature service teams, DR & BCM operating closely to maintain system resilience

5. Cyber Security:
Incorporation of security best practices and controls from the outset to lower risk

6. Business Alignment:
Use of technologies that are fit for purpose and can scale with future business demands

or Australian Energy Sector Cyber Security Framework (AESCSF)

F leverages recognised industry frameworks, t-practice control standards as well as the -specific control references.

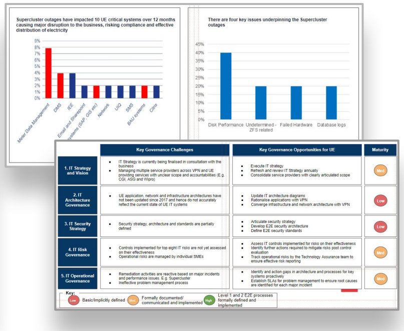
F framework comprises of 11 categories, or the purposes of this evaluation, five key are deemed relevant:

hreat and Vulnerability Management (TVM)
ituational Awareness (SA)
vent and Incident Response, Continuity of perations (IR)
sset, Change, and Configuration Management ACM)
lentity and Access Management (IAM)

E has conducted a self-evaluation of this k preceding the formal AEMO evaluation in

ts from this self evaluation are used as inputs valuation

Outputs



Supercluster outages have impacted 10 UE critical systems over 12 months causing major disruption to the business, risking compliance and effective distribution of electricity

There are four key issues underpinning the Supercluster outages

	Key Governance Challenges	Key Governance Opportunities for UE	Maturity
1. IT Strategy and Vision	• IT Strategy is currently being finalised in consultation with the business • Managing multiple service providers across VPN and UE providing services with unclear scope and accountabilities (E.g. CGI, ASG and Wipro)	• Execute IT strategy • Refresh and review IT Strategy annually • Consolidate service providers with clearly articulated scope	Med
2. IT Architecture Governance	• UE application, network and infrastructure architectures have not been updated since 2017 and hence do not accurately reflect the current state of UE IT systems	• Update IT architecture diagrams • Rationalise applications with VPN • Converge infrastructure and network architecture with VPN	Low
3. IT Security Strategy	• Security strategy, architecture and standards are partially defined	• Articulate security strategy • Develop E2E security architecture • Define E2E security standards	Low
4. IT Risk Governance	• Controls implemented for top eight IT risks are not yet assessed on their effectiveness • Operational risks are managed by individual SMEs	• Assess IT controls implemented for risks on their effectiveness • Identify further actions required to mitigate risks post control evaluation • Track operational risks by the Technology Assurance team to ensure effective risk reporting	Med
5. IT Operational Governance	• Remediation activities are reactive based on major incidents and performance issues. E.g. Supercluster • Ineffective problem management process	• Identify and action gaps in architecture and processes for key systems proactively • Establish SLAs for problem management to ensure root causes are identified for each major incident	Med

Key: Low Basic/Implicitly defined; Med Formally documented/ communicated and implemented; High Level 1 and 2 E2E processes formally defined and implemented

The review of UE's IT stability and security was based on tailored stability & security frameworks

APPROACH

1. Tailored stability and security review framework

The stability review framework assessed stability based on the following six dimensions:

1. IT Governance:
Architectural standards and best practices to promote technology consistency and reuse

2. IT Systems Resilience:
Failover in design aligned to business needs, Disaster recovery and business continuity

3. IT Lifecycle Management:
Proactive management of technology assets to ensure supportability and stability

4. IT Service Management:
Effective IT performance underpinned by mature operating processes and governance

5. Cyber Security:
Incorporation of security practices and objectives from the Australian Energy Sector Cyber Security Framework (AESCSF). The AESCSF framework comprises of 11 categories, however, for the purposes of this evaluation, five key categories are deemed relevant:

A. Threat and Vulnerability Management (TVM)
B. Situational Awareness (SA)
C. Event and Incident Response, Continuity of Operations (IR)
D. Asset, Change, and Configuration Management (ACM)
E. Identity and Access Management (IAM)

6. Business Alignment:
Technology alignment with business context that is fit for purpose and can scale with future business demands

2. Conduct review and develop final report

1. Conduct document review
2. Interview business and IT stakeholders across UE and VPN
3. Review IT operational data e.g. incident and problem management logs
4. Develop UE IT Systems Review report:

   01 Executive Summary
   02 Context
   03 Approach
   04 Findings and Recommendations
   - **A** IT Governance
   - **B** IT Systems Resilience
   - **C** IT Lifecycle Management
   - **D** IT Service Management
   - **E** Cyber Security
   - **F** Business Alignment

   05 Next Steps
   06 Appendices

04A. IT Governance

By uplifting IT governance, a number of challenges impacting stability and security can be addressed

IT GOVERNANCE SUMMARY

IT Governance Domain	Findings	Recommended Remediation	Maturity
1. IT Strategy and Operating Model	• Limited IT strategy planning process to date however a newly introduced strategic planning process has recently finished • Complex supply chain requires management of multiple service providers across CHED Services to deliver application, network and infrastructure services (E.g. CGI, ASG and Wipro)	• Publish, execute and maintain the new IT strategy • Simplify the operating model by consolidating Infrastructure services onto a single managed service agreement for CHED Services	Med
2. IT Architecture	• UE application, network and infrastructure architectures have not been updated since 2017 and hence do not accurately reflect the current state of UE IT systems	• Establish architecture capability to create / refresh and maintain an accurate and current view of the UE IT landscape • Investigate the opportunities to further converge and consolidate infrastructure, network and application architecture with VPN	Low
3. IT Security Strategy	• Security strategy, architecture and standards are partially defined	• Formalise the security strategy • Develop E2E security architecture • Define E2E security standards and update security policies	Low
4. IT Risk	• IT controls implemented for top eight IT risks however assessment of their effectiveness has not yet occurred • IT operational risks are managed by individual SMEs in distributed registers / spreadsheets	• Assess existing IT controls effectiveness • Design and implement an IT operational risk framework • Embed tracking of IT operational risks to ensure effective risk reporting	Med
5. IT Operations	• Some remediation activities are reactive based on major incidents and performance issues. E.g. Supercluster • Ineffective problem management process, resulting in aged problems (e.g. ~39% of closed problems are ~100 days old)	• Service performance improvement review, to include a deep dive into the current status of Problem Management in UE with establishment of SLAs for problem management to ensure root causes are identified for all major incidents	Med

Key:

Low	Reactive IT
Med	Emerging IT
High	Mature IT

united energy

Improved IT governance supports the mitigation of UE's top eight IT risks (1)

IT GOVERNANCE AND RISK MANAGEMENT SUMMARY

#	IT risk*	IT Strategy and Op. Model	IT Architecture	IT Security Strategy	IT Risk Governance	IT Operational Governance	Recommended governance improvement to mitigate risk
1	Malicious or unauthorised access or change to our hardware, software or data that compromises availability, integrity or confidentiality		●	●	●	●	● Formalise the management and monitoring of IT operational risks by the Technology Assurance team ● Define and endorse a roadmap to remediate security risks
2	Ineffective process and controls in place to adequately maintain IT performance and service levels leading to significant impact on availability or performance of core IT systems	●	●			●	● Develop E2E Enterprise Architecture ● Develop detailed processes and controls ● Define future state of the E2E architecture aligned to IT Strategy
3	Failure of an IT asset/s (software, hardware, service) causing significant impact on availability and performance of core IT systems	●	●			●	● Develop E2E network architecture ● Identify single points of failure ● Assess impact of failure on the business ● Define future state of the architecture aligned to IT Strategy
4	Failure to adequately deliver IT services in accordance with policies, procedures and standards causing significant impact on performance/availability of core IT systems				●	●	● Review and uplift vendor management capability ● Review and uplift problem management capability
5	Inadequate management of Information including unauthorised disclosure of sensitive information or inability to access information in a timely manner ie data loss	●		●			● Define E2E standards and security strategy ● Implement access rights, privacy policies and authorisation procedures ● Define information management strategy in IT strategy

* Data Source / reference: UE IT Risk Register

Improved IT governance supports the mitigation of UE’s top eight IT risks (2)

IT GOVERNANCE AND RISK MANAGEMENT SUMMARY

#	Top 8 UE IT Risks*	IT Strategy and Op. Model	IT Architecture Governance	IT Security Strategy	IT Risk Governance	IT Operational Governance	Recommendation
6	Failure to comply with contractual obligations		●		●	●	• Review and uplift vendor management and contract management capability • Review and uplift problem management capability
7	Failure to deliver projects to schedule, cost & quality	●	●		●	●	• Establish appropriate program and project governance, based on a suitable delivery model • Ensure architecture standards are adhered to by projects (e.g. through a design authority) • Manage and monitor operational risks by the Technology Assurance team
8	Failure to manage the growth and complexity of Information Technology for the future needs of electricity distribution e.g. Smart Grid, competition	●	●	●	●		• Execute IT strategy and IT security strategy • Refresh IT strategy and IT security strategy annually, including a review of the IT architecture to align with * enable the strategies • Ensure architecture standards are adhered to, and that the architecture establishes a foundation to manage increasing complexity (e.g. through simplification of the current environment, establishment of common platforms) • Anticipate and mitigate significant / critical IT risks to avoid the IT portfolio / program of work becoming overly compliance focused at the expense of growth initiatives

* Data Source / reference:

- UE IT Risk Register

04B. IT Systems Resilience

Key resilience issues arise from the Supercluster, email, network architecture, and disaster recovery

IT SYSTEMS RESILIENCE – KEY FINDINGS

	Findings	Recommended Remediation	Maturity
1. Supercluster	- Eight outages over a 12 month period* impacted the business including delays in sending meter data to the market - 11 day outage in June 2018 forced the business to revert to manual BCP practices - Scheduling maintenance windows for routine patching requires ~30 hours downtime due to technical design - Single point of failure results in inadequate backup options	Scope and fund a subsequent phase of work to migrate non-critical apps off the Supercluster platform.	Med
2. Email Sharepoint and Citrix	10 service outages of Email, Sharepoint and Citrix occurred over a 12 month period*, primarily affecting the offshore Probe contact centre productivity and customer experience for ~ 9 days.	- Assess the use of a CRM system by the offshore Probe team as an alternative to Email for managing customer enquiries - Assess the appropriate approach to improve CRM capabilities for Probe given the FIRB requirement to onshore the contact centre - (For further information, see page 40**).**	Low
3. Network	There are two inflight projects (network segregation and IT/OT border remediation projects) that are addressing the following issues: - Lack of redundancy creating single points of failure - Unrestricted access to IT administrative interfaces - Users on the corporate network have access to AMI & SCADA systems	- Execute a second penetration test once the network projects are complete to test their effectiveness - Prioritise and execute recommendations from the penetration test - Embed an enduring testing and remediation approach to ensure network risks are assessed and mitigated on an ongoing basis.	Med
4. Disaster Recovery	- There is no clear record of the current status of DR testing, previous results and / or the subsequent risk position - Limited testing of UE IT DR has been conducted in the past 18 months - Critical systems such as SCADA last tested in 2014 - DR policy last updated in 2016	Review and Refresh DR policy and process including greater alignment to Business requirements and BCM, the VPN continuity process and approach.	Low

Key:

Low	Reactive IT
Med	Emerging IT
High	Mature IT

* **Note**: Major Incident data is from Feb 2018 – Feb 2019

Remediating Supercluster stability issues has resulted in unplanned costs of ~$5M over 12 months

SUPERCLUSTER CASE STUDY

Introduction

The United Energy Supercluster was implemented in 2013 with the objective of centralising a fragmented IT environment which operates the majority of UE's critical systems. Suitability of the solution for UE became less effective over time due to growing business volumes, coupled with a lack of available options to change the Supercluster without a full replacement of the technology.

Business disruption and impact to key services

Since the acquisition of UE, the Supercluster has experienced persistent performance and stability issues, impacting most of UE's IT systems across both corporate and OT domains.

Ongoing challenges and implications

1. **Persistent failures:** Repeated and prolonged system downtime impacting critical business services such as dispatch management, meter data to market, billing and finance systems.
2. **Inflexible technical design:** System requires major IT downtime (~30 hours) to apply essential and recommended routine maintenance fixes.
3. **Maintenance is not possible:** Critical systems, e.g. 24/7 distribution services running on the Supercluster mean there is not enough downtime available for maintenance required.
4. **Single point of failure:** No viable alternative fall back systems when production experiences problems due to lack of failover capability and under specified disaster recovery.

An IT failure in June 2018 had a major impact on UE business and customers for 11 days

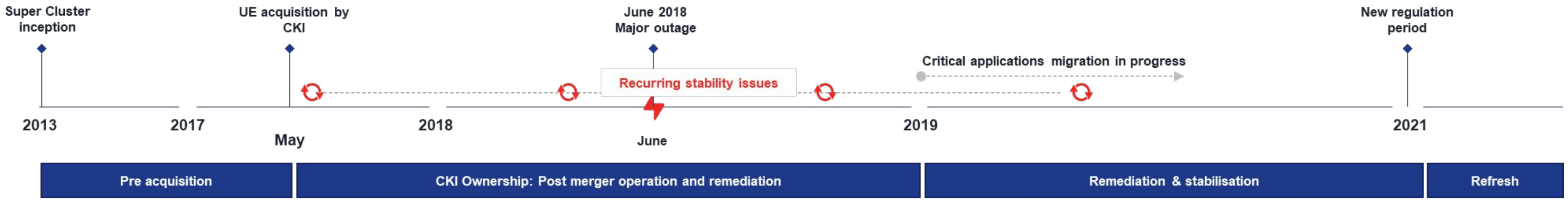
Critical UE systems impacted

- Meter Management (Itron)
- Geospatial systems (GIS)
- Billing systems (SAP)
- IT Management (integration and scheduling)
- Distribution management systems (DMS)
- Network Demand (Utility iQ)

+

Customer Impacts

- Suspended meter reading, risking regulatory compliance
- Billing delays impacting ~$12M revenue
- Inability to access work schedules and service orders
- Unavailability of life support reporting
- High call times as FoH had to default to manual service requests
- Extended customer outage times, and delays in Live Line and Tree Clearing

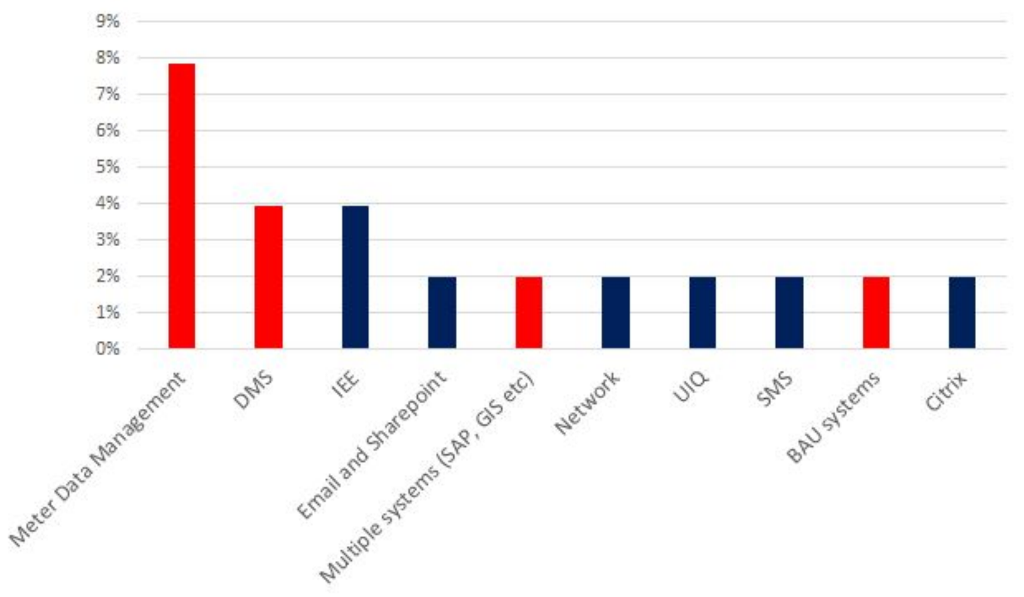

Super Cluster inception
UE acquisition by CKI
June 2018 Major outage
Critical applications migration in progress
New regulation period
Recurring stability issues
2013
2017
May
2018
June
2019
2021
Pre acquisition
CKI Ownership: Post merger operation and remediation
Remediation & stabilisation
Refresh

Securing adequate investment in critical technology is essential – to avoid instability and disruption to the network and customers

In 2018, 29% of all known root causes linked to major incidents were attributable to the Supercluster

IMPACT ANALYSIS OF UE SUPERCLUSTER

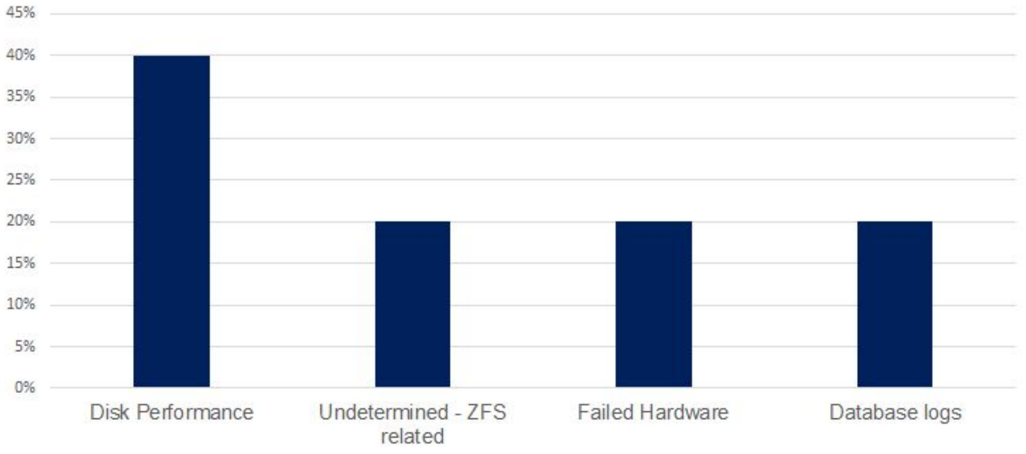
Supercluster outages have impacted 10 UE critical systems over 12 months causing major disruption to the business, risking compliance and effective distribution of electricity



Key: 🟦 Major incident 🟥 Critical incident

- UE critical systems such as Meter Data Management, SAP, Distribution Management System (DMS) and BAU systems are hosted on the Supercluster
- Supercluster is the primary central node for supporting UE's business operations, including compliance management and electricity distribution – and any failure of the Supercluster results in a Major or Critical incident

Key issues underpinning Supercluster outages



- The storage layer (Disk performance and ZFS) are responsible for 60% of Supercluster incidents
- Two projects have targeted reducing the severity of business impact resulting from Supercluster outages:
  - **Real Time Systems (RTS) Infrastructure Project** has migrated UIQ and DMS systems onto new infrastructure away from Supercluster in 2018
  - **Supercluster Migration Project** is deploying new infrastructure to support critical corporate applications such as SAP and Meter Data Management
- There is an intent to migrate non-critical applications to additional non-Supercluster infrastructure in the future but no project is currently confirmed. Until such time non-critical applications remain at risk of further Supercluster outages

Limited testing of disaster recovery capabilities has occurred over the past 18 months

DISASTER RECOVERY

Limited testing* has been performed in the past 18 months. For many critical systems, it is unclear when they last had a successful DR test performed and subsequently it is unclear how successfully critical systems would or could recover in the event of a major production failure.

1) Significant technology remediation projects have occurred / are in progress to remove barriers and constraints:

- **Real Time Systems (RTS) Infrastructure / OT zoning –** migrated critical OT systems DMS and UiQ away from unstable infrastructure (SuperCluster ZFS storage)
- **Super Cluster remediation –** in progress to remove major single points of failure and DR risk
- Total combined segregation and remediation project cost of **~$7.4M**
- A number of non-critical applications will remain on Supercluster, posing a further risk of outage due to untested DR

Major systems with unknown disaster recovery capability:

Corporate Technology	Operational Technology
● Itron (IEE & MTS) ● SAP ● GIS (Network Viewer/EDMS/DBYD) ● Webmethods ● Control-M ● Corporate File shares	● DMS ● UiQ ● SCADA

2) The Current DR approach has risk due to a lack of clarity regarding the current status of DR for major UE IT systems, and may not have priority linked to a number of issues:

- Current **UE DR policy was last updated in 2016**, is **not aligned with VPN** and is **not aligned with IT criticality definitions**, therefore, **plans and testing may not align with business needs**
- A **provisional schedule for 2019 is in place**, but appears subject to disruption by project delays and **may not have sufficient priority ****
- Some **OT systems (inc. SCADA)** may **not** have been **tested since 2014** and **old hardware (OSI PI) may not cope well with a testing scenario**
- There is **no clear record** of the **current status of DR testing**, **previous results** and / or the **subsequent risk position**
- The Supercluster project has not proven / attested DR capability prior to handover to BAU, therefore, DR capability remains unproven

Recommended Next Steps

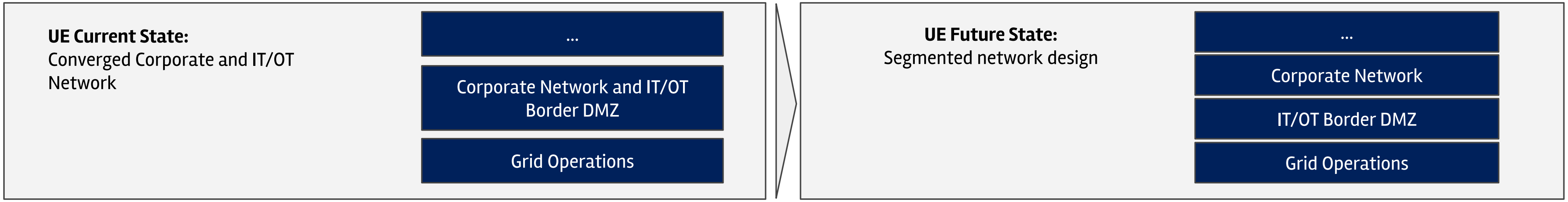
A deep dive into the current status of DR in UE. Include a review and refresh of DR documentation including policy, process and BCM alignment for critical services. Introduce a comprehensive DR test results capture to supplement the current one line status indicator (DR Test Schedule). This will provide greater transparency and understanding on specific gaps, rationale for failure, and related mitigating actions.

Testing history is logged in an issues spreadsheet, and remediation appears to have a dependency on many in flight projects to mitigate those weaknesses. To further formalise those issues a risk assessment should be performed in alignment with the risk framework. This will provide greater clarity, governance and control over status, including clear ownership and accountability. It will also create transparency with the business to increase awareness and prioritised planning.

Notes:-
* Anecdotal feedback during interviews that a process was undertaken to prove limited capability for some regulated systems, however no further information was provided.
** The UE DR policy provided was incomplete and it's effectiveness and enforcement may be contributing to a lack of clarity and process to escalate DR issues and to clearly allocate ownership for resolution, also impacted by an emerging risk and IT operating model

The network architecture lacks segregation, creating risk to application availability

NETWORK ARCHITECTURE



UE Current State:
Converged Corporate and IT/OT Network

UE Future State:
Segmented network design

Issues with current network design

Internal audit* has raised critical and high rated security issues:

- Security architecture segregating the operational IT networks, corporate and guest wireless network requires remediation to prevent unauthorised access
- Security controls for wireless networks were previously found to be weak
- Incident logging and monitoring process is inadequate
- General employee awareness over removable media security practices is weak
- Access over the internet to internal systems and apps is not restricted to authorized personnel
- Software configuration management is inadequate

These give rise to the following **distribution risks:**

- Electricity network is compromised impacting the ability to supply reliably, and the quality of electricity to consumers
- Disruption of IT network traffic, affecting availability of applications
- Unauthorised access to confidential corporate/customer information

Inflight remediation projects: 2016 – 2020 period

Two key projects are inflight in this regulatory period:

1. **Network Segregation:** segment the corporate network from the IT/OT border DMZ
2. **IT/OT Border Remediation:** Remediate access, incident management, configuration management issues

These projects will ensure:

- Minimised impact of incidents from single points of failure
- Reduced number of single points of failure
- Only privileged users have access to the intended systems

Recommended Next Steps

- Standardise E2E security controls
- Evaluate the effectiveness of these controls
- Conduct regular penetration testing to ensure the implemented solutions are addressing security gaps

* Data Source / reference: UE Internal Security Audit report, 2019

04C. IT Lifecycle Management

Note: in context of this report IT Lifecycle management refers to a lack of support and maintenance capability.

Lack of lifecycle management resulted in several one off unplanned costs for UE IT to reinstate support

LIFECYCLE MANAGEMENT – KEY ISSUES

	Findings	Recommended Remediation	Maturity
1. Critical Services – Software Support	● Stakeholder interviews and evidence of recent projects revealed a lack of appropriate spend in UE IT over a period of years, resulting in some software agreements lapsing and / or being substituted with lower grade agreements ● One off costs* to reinstate full SAP support have been incurred ● Requirement for ongoing investment and currency to maintain SAP support and maintenance status	● Ensure that appropriate ongoing budget and investment is allocated to retain currency of SAP support and maintenance status	Med
2. Network and Security – Hardware and Software Maintenance	● Due Diligence performed to consolidate network services support under a single supplier (Dimension Data) for CHED Services identified many end of life and unmanaged assets from a support perspective requiring remediation to enable full support ● Un-planned remediation cost of ~$650K in 2018, with potential ongoing renewal beyond 2019	● Ensure the ongoing maintenance costs are budgeted on an ongoing annual basis to stay in current vendor approved support ● Where support is not aligned to vendor recommended lifecycle, perform a risk assessment and manage through a formal risk management process and lifecycle	Med
3. Environment Maintenance	● Project delivery since the acquisition of UE has experienced repeated challenges while promoting changes through non-production and production environments due to inconsistent environment build and configurations ● Recent unplanned remediation costs incurred ~$70k in the first quarter of 2019 to reinstate test environments in order to support project delivery ● An Environment Manager was recently appointed	● Perform a gap analysis of the current non-production environments against the current production environments to ascertain the scale of misalignment ● Risk assess the gaps discovered, and prioritise mitigation plans required to address known gaps and risks ● Provision for ongoing refresh on an ongoing annual basis to stay in current vendor approved support	Low

Key:

Low	Reactive IT
Med	Emerging IT
High	Mature IT

Notes:

- * Details of the cost to reinstate SAP support have not been disclosed
- A potential source linked to the exit of formal maintenance contracts and associated risk of doing so, has anecdotally referenced a set of cost reduction recommendations in a pre-2016 McKinsey report during interviews with the PowerCor IT team. No artefact has been provided to substantiate this.

Reinstating maintenance agreements for critical software required unplanned investment

SOFTWARE LIFECYCLE MANAGEMENT – KEY ISSUES

United Energy has invested in bringing a number of critical Technology assets back under formal support and maintenance contracts in the last 12-18 months, with examples including two critical UE IT Systems, providing 24/7 monitoring services and mission critical and strategic SAP systems.

1) Software maintenance SAP software suite

Historically and prior to acquisition UE IT opted to withdraw from official SAP vendor support to save costs, and opted for a 3rd party support agreement with Rimini Street who provide an alternative software support service from the Product vendor.

The implications of this decision for UE included:

a. There would be no future upgrade path available from the software vendor SAP for any of the UE SAP systems
b. Short term and tactical thinking impacted the ability for to explore future billing systems convergence onto UE's SAP ISU platform.
c. The ability for UE to modernise the ERP SAP suite, through the planned migration to the strategic SAP cloud solution S4HANA during the next regulatory period (2021-2025)

The tactical savings achieved from the switch to Rimini Street (not provided during review**), effectively represented wasted / sunk costs. This is due to UE IT having to repay and back date all support costs to SAP, to reinstate full support and maintenance status – over and above any costs paid to Rimini Street.

This initiative also resulted in an ongoing financial commitment for UE IT to commit to ongoing support and maintenance with SAP to remain current. Therefore, the ongoing implication has increased the scale of ongoing recurrent investment in the SAP suite of products over and above the reduced Rimini Street costs.

2) Software maintenance reinstatement and increased licensing for Enterprise monitoring software HP Operations Manager (HPOM)

HP Operations Manager provides UE IT with the ability to monitor UE IT assets on the network in relation to their health and performance status – enabling and facilitating corrective preventive and reactive action to be undertaken in times of failure.

○ The lack of a valid support agreement with MicroFocus for HPOM, resulted in two issues requiring remediation:

   a. UE IT reached maximum licensing capacity for IT assets able to be monitored under the maintenance contract, presenting a risk that new IT assets deployed by the RTS infrastructure project for DMS and UiQ would go un-monitored
   b. A risk that if the enterprise monitoring software failed or had a problem, that no ongoing support, maintenance or patches would be available from MircoFocus that could have an ongoing impact on UE ability to monitor critical IT systems

○ **Remediation action**: UE re-invested with a one off investment for a support agreement and increased licensing with MicroFocus, and has successfully on boarded critical new DMS assets under the monitoring service – the cost of this was **~$225k** until the end of 2019. A decision is yet to be made if this will be retained and represent ongoing recurrent support costs.

Notes:-
***** The decision to switch to Rimini Street support would have been a suitable option if UE / VPN were not planning to retain SAP as a strategic core billing and ERP systems. However, as UE / VPN consider it to be strategic, then Rimini Street was no longer a viable option to gain access to the latest releases and contemporary SAP software.
** The costs incurred by UE IT for Rimini Street reduction and the subsequent increase to return to SAP have not been provided during the review period.

Hardware refresh performed for old network assets and uplift anticipated for non-prod environments

SOFTWARE LIFECYCLE MANAGEMENT – KEY ISSUES

1) Environment maintenance

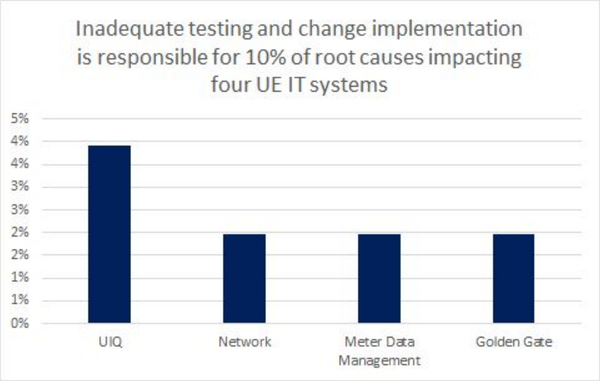
A number of areas of concern were identified in relation to historical environment management of non-production environments.

Inconsistencies were observed, and anecdotally noted during stakeholder interviews that impact Project delivery in UE. Key challenges include:

- Failed or unexpected results when promoting changes through non-production and production environments due to inconsistencies
- Lack of build guides and specifications
- Higher risk change delivery programs

Anticipated unplanned project remediation costs attributed to un-managed environments upto **~$70K in the last quarter 2019**

"During the last 12 months root cause investigations identified that un-managed environments resulted in a number of failed production deployments for critical systems"



2) Network and Security Remediation – Hardware and Software Maintenance

Since the UE acquisition a convergence and simplification project has brought all network support under a single Network supplier, Dimension Data.

During due diligence for support transition the supplier identified a number of items requiring remediation prior to full managed service take on:

- Upgrade out of support network and firewall software to latest supported versions
- Review and replace end of life hardware
- Clean up and tune firewall rules considered unused or risky
- Tune and optimise network security/threat prevention technology (intrusion detection)

The remediation cost to resolve the lifecycle management issues of the previous UE management regime were **~$650k** in 2018.

Recommended Next Steps

Production and Non-production Environment Review

- Perform a gap analysis of the current non-production environments against the current production environments to ascertain the scale of misalignment

Vendor Support Review

- Prioritise and schedule a series of reviews to identify issues and risks related to the currency of software and hardware support for critical services

Data Source / reference:

- Ched_UnitedEnergyDueDiligenceReport_V0-02 redacted (2).docx - 01/06/2018
- UEIC - IT Network & Security Remediation.pptx
- UE Program Manager: Webmethods, SAP and Itron IEE

04D. IT Service Management

A review of UE’s Service Management is ongoing under a Service Improvement program

IT SERVICE MANAGEMENT SUMMARY

	Findings	Recommended Remediation	Maturity
1. Service Management	● Scope of Service Management Office (SMO) support covers UE IT, VPN IT, SA Power Networks, Wellington Electricity and beon ● SMO coverage for UE IT is new, since ‘in-sourcing’ of Service Management from a 3rd party managed service ● Significant stability and repeating high priority incidents were experienced in last 12 months, including: ○ 20 Meter data to market incidents ○ Multiple Supercluster failures ● Misaligned standards exist across UE and VPN, e.g. different criticality definitions ● Multiple managed service providers represent a complex supply chain ● The UE IT core Service Management platform (ServiceNow) was extended to provide a single consolidate Strategic tool for management of all SMO services	Continue to prioritise and invest in the program, and where possible look to accelerate the activities linked to stabilising the environment through greater understanding of business impact and performance of IT, and eradicating root cause of systemic issues in the environment.	Med
2. Problem Management	● Limited governance of the problem management process and no SLAs for Problem Management root cause identification contributed to the following key issues: ○ Only 58% of High priority P2 incidents have had a root cause investigation, representing a potential risk of repeating high impacting incidents ○ Average age of root cause problem investigation records is high, at an average of 108 days for investigations related to P2 incidents	● A deep dive into the current status of Problem Management in UE IT, including a review and refresh of the problem management process with particular emphasis on metrics, KPIs and reporting to enable stronger governance and to drive greater performance around identifying, and removing root cause ● Automate creation of a root cause investigation for all P1 and P2 incidents on incident resolution	Low

Key:

Low	Reactive IT
Med	Emerging IT
High	Mature IT

Challenges to service management include major changes, increasing complexity & stability issues

IT SERVICE MANAGEMENT JOURNEY SO FAR

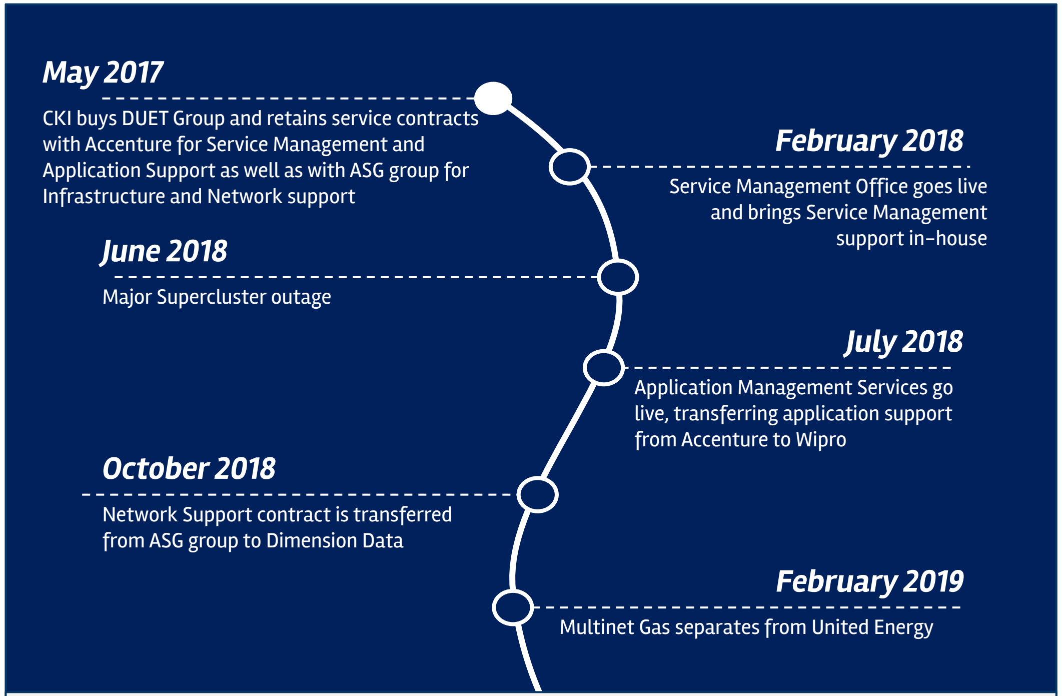
The Service Management Office (SMO) in CHED Services, is just over 12 months old since it was insourced from Accenture. It now provides extended Service Management Office (SMO) support to UE IT and VPN IT, in addition to a number of other entities in the CKI group – SA Power Networks, Wellington Electricity and beon.

Historically, UE IT operated a very lean IT organisation and was largely outsourced. Since the CKI acquisition, a significant set of changes occurred since May 2017 (see illustration – right), including a major whole of UE business continuity event resulting in ~11 days impact in June 2018.

Upon transition into CHED Services, the SMO function has been on a steep journey of learning and understanding of the IT environment, and experienced significant change, including:

- In-sourcing of service management from a 3rd party
- Dealing with significant and repeating high priority incidents:
  - 20 Meter data to market in 12 months
  - Multiple Supercluster failures
- Working with misaligned standards across two organisations, e.g. different criticality definitions across UE and VPN
- Managing and consolidating services across multiple managed service providers
- Integrating Core Service Management tools across CHED Services

In addition to the major changes and challenges, a high level review of sample problem management data and review of the process (see page 34), illustrates that opportunities for ongoing improvement still exist and benefit could be gained from a holistic performance review.



May 2017

CKI buys DUET Group and retains service contracts with Accenture for Service Management and Application Support as well as with ASG group for Infrastructure and Network support

February 2018

Service Management Office goes live and brings Service Management support in-house

June 2018

Major Supercluster outage

July 2018

Application Management Services go live, transferring application support from Accenture to Wipro

October 2018

Network Support contract is transferred from ASG group to Dimension Data

February 2019

Multinet Gas separates from United Energy

'Historically, UE IT operated a very lean IT organisation and were largely outsourced, including Service Management operations and governance to Accenture. Upon transition into CHED Services, the function have been on a journey of learning and understanding of the IT environment'

Recommended Next Steps

Continue to prioritise and invest in the program, and where possible look to accelerate the activities linked to stabilising the environment through greater understanding of business impact and performance of IT, and eradicating root cause of systemic issues in the environment.

Note: A Service Improvement Plan (SIP) exists. Data provided is high level and does not include detailed plans, targets or results achieved to date, therefore the priority, status, progress and outcomes of the SIP are presently unclear.

Problem Management data shows root cause investigation and performance is inconsistent

CORE PROCESS – HIGH LEVEL SAMPLE REVIEW

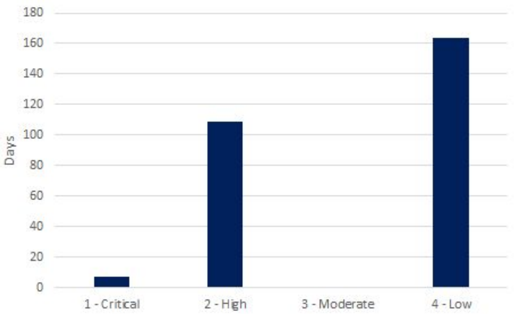
Problem management root cause metrics and performance

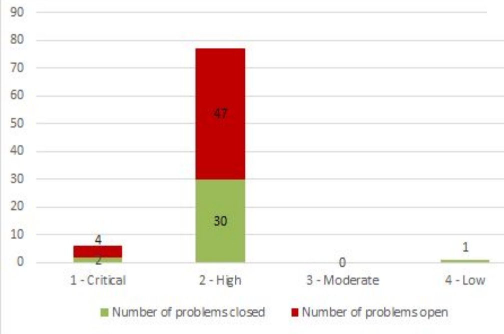
A high level review of the problem management process indicates there are options to track and measure approximately 20 KPI / metrics to assess process performance.

However there are **no performance SLA's** associated with **identification of root cause for major incidents –** a key driver and outcome of a typical problem management process.

Basic raw problem data analysis indicates that performance in terms of identifying and removing root cause is not optimised due to:

- **average age** of a High Priority **P2 root cause investigation is 100 days**
- **> 150 days for P4 low priority**





- **Root cause investigation versus major incidents** has a low ratio:
  - Out of 132 P2 incidents = **only 77 (58%) had a root cause investigation**

Opportunity

A sample data analysis and a review of the problem process documents identified at least two areas where simple changes could uplift effectiveness:

- Specify that all priority 1 & 2 incidents must have an associated problem record created to mandate root cause investigation for all high impacting incidents
- Implement performance targets to drive a performance culture regarding identification of root cause

Recommended Next Steps

- A deep dive into the current status of Problem Management in UE, including a review and refresh of the problem management process with particular emphasis on metrics, KPIs and reporting to enable stronger governance and to drive greater performance around identifying, and removing root cause.
- Once this is complete, it is recommended that UE engage and socialise with all suppliers (internal and external) to support review and sign up to the new performance regime for problem management, including contract amendment where necessary.
- It is recommended that UE investigate options to automate root cause investigation creation through ServiceNow on major incident closure (**note:** this may require amendment to existing major incident closure process).

united energy

04E. Cyber Security Review and Alignment

Alignment to the Australian Energy Sector Cyber Security Framework (AESCSF)

Integration with enterprise CMDB will enable an improved baseline for execution of Security controls

ACM-1: Manage Asset Inventory

UE has commenced several projects to address asset currency issues within the asset inventory, across both IT and OT environments. While the OT environment is process-driven and audited regularly, issues have been identified within the IT environment relating to the steps taken after an asset inventory review is conducted[1].

Maintaining an accurate and current asset inventory supports software tools such as Tenable in their ability to scan for vulnerabilities within UE's networked environment. Tenable will scan assets within the networked environment and present the results of the scan as actions for remediation. These results are incomplete, and remediation of vulnerabilities can be delayed, when there is an out of date asset inventory.

UE has implemented ServiceNow[2], a software tool which has functionality to establish and maintain an asset inventory. Consolidation of asset management activities through ServiceNow may support future operational needs, enhancing IT Operations and Service Management business functions.

ACM-2: Manage Asset Configuration

Completing this objective provides the basis for UE to adopt a "secure by design" culture that is broader than direct IT and OT support teams. It has been acknowledged as an area of opportunity[4] with specific regard to the quality and consistency of build/platform hardening.

At least one project is currently in-flight[3], where the configuration of the assets could adopt a "secure by design" premise.

Similar to ACM-1 (left), ServiceNow[2] can be utilised as a Configuration Management Database (CMDB), to establish and maintain configuration baselines for assets.

1. UE AESCSF Self-Assessment Notes for ACM-1, 2018
2. ServiceNow is present within the UE Application System Landscape, 2017, and used within Market Systems/Customer Management and Enterprise Systems/Works Management
3. Project Register "Manual Meter Data Read Process"
4. UE AESCSF Self-Assessment Notes for ACM-2, 2018

The secure retirement of assets is not currently performed in all cases

ACM-3: Manage Changes to Assets

Change management of select assets that support critical Operational Technology functions, such as the Oracle SuperCluster, do not have change management processes in place[5].

Additionally, within the existing change management process, the secure retirement of assets is not currently performed in all cases – which may result in potential exposure where sensitive information (including asset configuration) remains on those assets[5].

Finally, as changes are made to all systems (including those deemed critical), there is not always an explicit focus on the three key constructs of information security, specifically the;

1. Confidentiality (C);
2. Availability (A), and;
3. Integrity (I).

CAI are considered in an ad-hoc manner within system change logs, and represent a future opportunity for UE as security change management processes become more mature[5].

Summary of Key Opportunities

- Establish and maintain an asset inventory that is centralised within a single piece of software (such as ServiceNow), keeping it current to a period of at least 24 months (less than 24 months for assets deemed critical).
- Utilise ServiceNow as the Configuration Management Database (CMDB) for UE.
- Establish and maintain a risk-informed change management process for IT and OT information assets, that considers the full life cycle of assets (i.e. acquisition, deployment, operation, and retirement). Include assessment of change impact against the three constructs of information security (CAI) for assets that follow this process.

[5] UE AESCSF Self-Assessment Notes for ACM-3, 2018

Review Privileged Access Management following the completion of the "IAM Replacement" project (1)

IAM-1: Establish and Maintain Identities

UE has commenced several projects seeking to uplift capability in establishing and maintaining identities. Generally, these projects align to the "infrastructure and security approach" presented to the UE Audit and Risk Committee (ARC)[6]. Through this approach, the IT and OT environments of both UE and Victorian Power Networks (VPN) are becoming strategically converged.

The "Identity and Access Management (IAM) Replacement" project was initially scheduled for completion by the end of 2018.

Privileged Access Management (PAM) has been acknowledged as an area of opportunity[7], with elevated access and segregation of duties principles to be targeted following the completion of the UE "IAM Replacement" project.

IAM-2: Control Access

The "IAM Replacement" project may not be scoped to include consideration of the link between logical and physical access to assets (ie. a password versus a physical key). As a result, UE may require an additional capability uplift to realise an efficient, automated process that links an identity to their logical and physical access across IT and OT environments[7].

Operational processes to manage identities and their access are not risk-informed at the current time[7]. Organisational risk-criteria applied within these processes introduces acknowledgement of the risk born from an identity (person) having access to a network control system versus their corporate email, and subsequently provides UE with a mechanism to manage that risk.

UE has acknowledged the risk arising from a malicious insider with access to a network control system at an operational[8] and strategic level[9] however this may not have been included as an area of priority within the current cyber security program and "IAM Replacement" project, as it is dependent on increased cyber risk awareness across the business.

6. UE Audit and Risk Committee (ARC) Minutes, pp. 89-93, 2018
7. UE AESCSF Self-Assessment Notes for IAM-1, 2018
8. Cyber Security Risk Register "Top 20", 2016
9. Enterprise Risk Register "Cyber Risk", 2019

Review Privileged Access Management following the completion of the “IAM Replacement” project (2)

Summary of Key Opportunities

- Establish and maintain a consolidated IAM process across the IT and OT environments of UE and Victorian Power Networks (VPN) (NB: This opportunity surrounds the consolidation of operational process where it is reasonable, rather than converging all IAM technical solutions).
- Review Privileged Access Management (PAM) and segregation of duties following the completion of the “IAM Replacement” project.

Improve threat profiling by adopting proactive assessments via an ongoing enterprise risk process (1)

TVM-1: Identify and Respond to Threats

Threat profiling occurs at least annually as a part of the cyber security program[10], however there remains an opportunity to embed threat profiling within enterprise-wide risk assessment and mitigation planning, ensuring that they become proactive interdependent processes rather than reactive siloed processes.

TVM-2: Reduce Cyber Security Vulnerabilities

Vulnerability identification and analysis occurs between an ad-hoc and structured manner depending on the environment (i.e. IT or OT). Once vulnerabilities have been identified and analysed, further opportunity surrounds the prioritisation of vulnerability remediation, the relationship between identified vulnerabilities and their enterprise risk (similar to TVM-1), and subsequent formalisation of these processes[11].

Automated vulnerability management activities do not currently occur in some OT environments, such as for Remote Terminal Units (RTUs) that exist in the field[11]. The vulnerability management process for these devices is highly manual, and represents an area of improvement to mature combined cyber security vulnerability and risk monitoring activities.

[10] UE AESCSF Self-Assessment Notes for TVM-1, 2018

[11] UE AESCSF Self-Assessment Notes for TVM-2, 2018

Improve threat profiling by adopting proactive assessments via an ongoing enterprise risk process (2)

Summary of Key Opportunities

- Embed threat profiling within enterprise-wide risk assessment and mitigation planning, ensuring that they become proactive interdependent processes rather than reactive siloed processes.
- Establish and maintain a risk-informed vulnerability remediation process that prioritises and results in a reduction of UE's enterprise cyber security risk.

Integrate OT security risk detection into an enterprise wide monitoring & detection capability (1)

SA-1: Perform Logging

Logging occurs in a structured manner within UE's IT environment, and is aggregated/centralised within McAfee and Splunk[12]. Conversely, logging occurs in an ad-hoc manner within UE's OT environment, and is not aggregated or centralised at present.

Additionally, some third party vendors have privileged access (see IAM[7]) that is not logged, which represents a key maturity gap and opportunity for UE to strengthen their security posture.

SA-2: Perform Monitoring

Operational environments, such as network control centres, have physical controls (such as doors, and locks) present to prevent and deter anomalous behaviour, however opportunities have been identified to monitor control systems for logical (or, computer-related) events that are considered anomalous[13]. These monitoring activities are dependent on the capability to first log events (see SA-1[12], IR-1).

Continuous monitoring and response within the OT environment, as well as risk and threat correlation to determine anomalous behaviour within control centres and control systems represent subsequent opportunities for UE, however more rigor surrounding fundamental logging and monitoring activities is first required.

[12] UE AESCSF Self-Assessment Notes SA-1, 2018
[13] UE AESCSF Self-Assessment Notes SA-2, 2018

Integrate OT security risk detection into an enterprise wide monitoring & detection capability (2)

SA-3: Establish and Maintain a Common Operating Picture (COP)

UE currently has no capability to establish and maintain a Common Operating Picture (COP) based on the lack of supporting activities to detect cyber security threats, vulnerabilities, risks, and events[14].

Establishing and maintaining a COP will provide UE with a "single pane of glass" view of their operating environment, to support network management activities as they pertain to cyber security, and inform operational through to strategic decision making.

Summary of Key Opportunities

- Establish and maintain a consistent process across IT and OT environments, to log and monitor system and network events, that may indicate a cyber security event. This opportunity may require significant upgrade of/uplift in select assets and systems that operate within UE's OT environments (based on asset/system age and other factors).
- Establish and maintain a consistent process to log and monitor the privileged access of third parties to assets and systems.
- Establish and maintain a Common Operating Picture (COP) (upon establishment of a consistent practice of logging and monitoring system and network events across IT and OT environments).

[14] UE AESCSF Self-Assessment Notes SA-3, 2018

Improved documentation on cyber security events will increase consistency across multiple teams (1)

IR-1: Detect Cyber Security Events

UE has acknowledged that cyber security event detection is an area of opportunity[15] [16] for improvement. Cyber security events and incidents are currently being detected in an ad-hoc manner, without structured or documented guidance that covers a range of threat events.

Criteria that determine what does, and does not, constitute a cyber security event, have been established in the OT environment using Commercial Off The Shelf (COTS) software. Similar criteria is present in the IT environment, however this is primarily managed through an outsourced provider[15].

UE has an opportunity to establish and maintain documented guidance that specifies what does, and does not, constitute a cyber security event within the context of their operations. These criteria should consider information within the cyber and enterprise risk registers, the threat profile, and the Common Operating Picture (COP).

IR-2: Escalate Cyber Security Incidents

Similar to IR-1 (left) UE has acknowledged an opportunity regarding the criteria used to escalate a cyber security event into a cyber security incident[17].

One project is currently in flight to replace traditional COTS anti-virus software with “next generation anti-virus” software[18]. This “next-generation” software should be tailored to UE’s IT and OT environments, based on risk, threat, and the COP.

Additionally, the criteria established through this project should be documented, communicated to incident responders, stored in a central location, and accessible to the appropriate personnel within IT and OT operational teams.

[15] UE AESCSF Self-Assessment Notes, IR-1, 2018

[16] August 2018 report to the Audit and Risk Committee (ARC)

[17] UE AESCSF Self-Assessment Notes, IR-2, 2018

[18] Project Register “Next Generation Anti-Virus”

Improved documentation on cyber security events will increase consistency across multiple teams (2)

IR–3: Respond to Incidents and Escalated Cyber Security Events

Event and incident response is outsourced to a third party, with a regular rhythm established for internal and external review[19]. Review of cyber security events and incidents occurs internally each fortnight, and externally with CGI each month[19].

These activities, however, are not risk-informed in a manner consistent with the cyber security risk management strategy, and UE's enterprise risk management strategy[19].

The outcomes of post-incident review are not always followed-up by the IT service management team[19].

IR–4: Plan for Continuity

Business Continuity Plans (BCP) are in place (as they relate to cyber) and include consideration of Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)[20]. Despite this, the BCP, RTO, and RPO are not explicitly risk-informed, in a manner consistent with the cyber security risk management strategy, and UE's enterprise risk management strategy[20].

[19] UE AESCSF Self-Assessment Notes, IR-3, 2018

[20] UE AESCSF Self-Assessment Notes, IR-4, 2018

Improved documentation on cyber security events will increase consistency across multiple teams (3)

Summary of Key Opportunities

- Establish and maintain documented guidance that specifies what does, and does not, constitute a cyber security event within the context of UE's operations.
- Establish and maintain (i.e. documented, communicated to incident responders, stored in a central location, and accessible to the appropriate personnel within IT and OT operational teams) cyber security incident declaration criteria.
- Establish and maintain clear requirements for post-incident review (PIR), as it relates to cyber security. Where the PIR identifies a vulnerability that requires remediation, ensure that the remediation occurs through the relevant UE team (i.e. enforce through organizational policy) and periodically gain external assurance on remediation activities completed (e.g. penetration testing, additional vulnerability assessments).
- Align UE's Business Continuity Plans (BCP) (from a cyber security perspective) with the cyber security risk management strategy and enterprise risk management strategy, updating Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) as required.

UE’s current security capability may be significantly lower than a level mandated in the future

Desired Future State of Cyber Security Operations

UE’s proposed IT program of work for the 2021-2025 period recognises the eed to optimise existing cyber security capabilities in order to secure the supply of electricity to UE’s customers[21].

Until the AER approves the IT Program of Work UE will continue to remediate its cyber security capability and maturity in a manner consistent with that presented to the Audit and Risk Committee (ARC)[6] by “remediating by consolidating” select IT and OT environments between UE and VPN.

UE was assessed as a Distribution Network Service Provider (DNSP) of High criticality[22] by the Australian Energy Market Operator (AEMO). As a result, a high level of cyber security maturity is expected across the IT and OT networked environments that power Victorians and support the National Electricity Market (NEM).

Whilst there is currently no mandate to achieve a target state maturity aligned to the Australian Energy Sector Cyber Security Framework (AESCSF), should this arise in the future, UE will have a significant gap between their current state of cyber security capability and maturity, and the potentially high target state maturity resulting from UE’s relative criticality[22].

[21] Regulatory Reset Business Case – Cyber Security UE

[22] UE Criticality Assessment Tool (CAT) Self-Assessment Response, 2018

04F. Business Alignment

Opportunities exist to increase IT and business alignment and employee engagement experience

BUSINESS ALIGNMENT SUMMARY

	Findings	Recommended Remediation	Maturity
1. Business context for IT Assets and IT Services	• IT assets are manually recorded in a central repository. An improvement project is in-flight which includes the implementation of automated discovery process. • The in-flight ServiceNow Discovery Project will automate IT asset discovery, but will not provide the full business context required to provide true business awareness in IT operations and service delivery.	• Articulate the scope for business services, including service definitions and alignment of business services to technical services and configuration baselines • Identify IT asset owners and assign clear accountabilities	Low
2. Customer Technology	• **Stability**: the offshore Probe contact centre experienced 3 major issues in 12 months and persistent performance issues.	• Avoid the potential for increasing costs in 2021, by accelerating plans to automate / migrate to a CRM solution for the Probe contact centre, ahead of the FIRB compliance mandate to on-shore services by 2021 • Develop a Customer Technology Strategy to address the stability issues	Low

Key:

Low	Reactive IT
Med	Emerging IT
High	Mature IT

UE has limited visibility of which business services utilise IT assets creating stability & operational risk

BUSINESS ALIGNMENT CONTEXT

Key risks

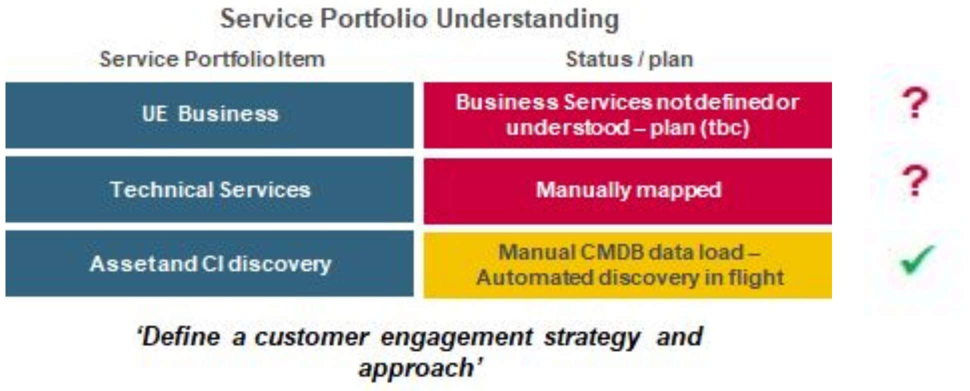
- Reduced ability to perform impact assessment when planning IT change
- Lack of transparency and understanding of the impact when a specific IT asset fails and it's associated impact to ongoing business operations
- Limited visibility of an accurate asset baseline to support ongoing security monitoring of UE assets (**ref: AESCF ACM-1: Tenable**)
- The current deployment of the UE Configuration Management Database (CMDB) is manually loaded, which represents high maintenance effort and risk that data inaccuracies could occur over time.

Unconfirmed planned projects in the future

A BAU project is in flight in IT Operations to enable automated ServiceNow discovery by May 2019. However the plan for mapping Technology Services to Business Services remains unclear, including who is accountable for delivery of this and within what timeframe.

Inflight remediation projects: 2016 – 2020 period

- The current **BAU ServiceNow project** is intended to facilitate automated asset discovery but will not map to Business Services
- A second phase is required to map technical services to business services to create ful business context for IT and to create accurate Business Alignment



Service Portfolio Understanding

Service Portfolio Item	Status / plan	
UE Business	Business Services not defined or understood – plan (tbc)	?
Technical Services	Manually mapped	?
Asset and CI discovery	Manual CMDB data load – Automated discovery in flight	✓

'Define a customer engagement strategy and approach'

Recommended Next Steps

Scope a project to define and document business services, including service definitions and alignment of business services to technical services and configuration baselines. **Note**: *This initiative is referenced in the SMO service improvement plan, however, the current detail is high level and is not sufficient to determine the scope, objective, timing or coverage and how this will create greater business and IT alignment.*

Data Source / reference:

- BAU ServiceNow project is owned and sponsored by John Vodopija, IT Operations
- A Proposed phase 2 to define business services and technical service mapping has been suggested but no confirmed approach, plans, timelines or owners are know at this time.

Customer Technology compliance investment needs have detracted from strategic investment & refresh

CUSTOMER TECHNOLOGY: STABILITY AND RISK

Background

Majority of investment since UE acquisition was focused on meeting compliance requirements

Due to increasing industry requirements and the need to adapt to new compliance standards, a high degree of investment in the Customer portfolio is aligned to compliance rather than optimisation.

Customer technology system	Last refresh (years)	Compliance project change
Itron IEE	4	Significant compliance requirements, such as the Life Support program have demanded high focus on compliance rather than strategy and refresh
Itron MTS	4	
SAP-ISU	3	
Webmethods	4	
Salesforce	NA	

In the current regulatory period it appears that IT instability is increasing and is visible in two primary ways

1) Persistent processing instability through email failure

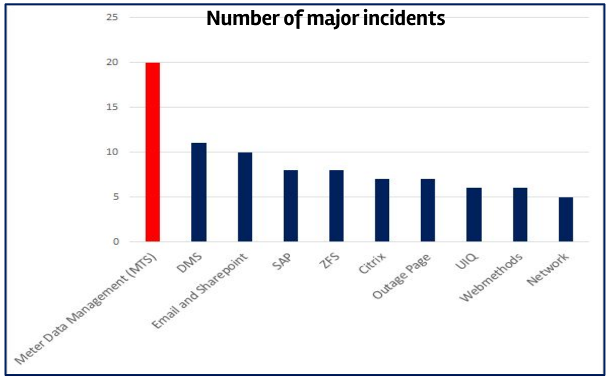
The customer service and back office processing teams (Probe contact centre) are dependant on a shared mailbox to accept and process work requests.

In the recent period the **mailbox was impacted** by at least **3 major incidents** (below). Further anecdotal **feedback points to frequent failure** impacting processing ability.

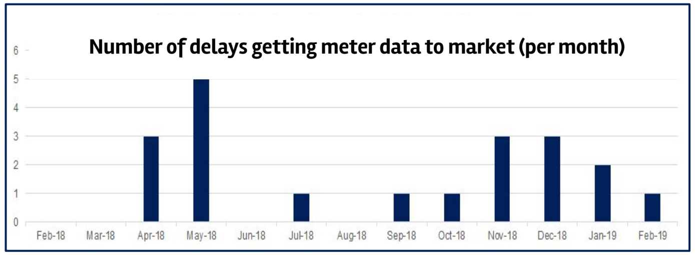
- Major Incidents related to the Probe shared mailboxes:
  - ○ Local Exchange Services not available for shared mailboxes (INC0155761) – 04/06/18
  - ○ UE Shared Inbox issue (INC0172299) – 24/07/18
  - ○ Probe staff cannot use in-box (INC0212692) – 04/12/18

2) Repeated failures to submit data to market

MTS system fulfils UE's daily data regulatory submission of meter data to the market. Consistent challenges in a 12 month period has seen this key system experience the highest frequency of Major Incidents in all of UE.



Over the past 12 months, data highlights this is a repeating and unresolved pattern.



Repeating patterns and a lack of in flight, prioritised initiatives and plans to mitigate the challenges, represent a real and increasing threat to UE in meeting its regulatory obligations.

05. Next Steps

Prioritise recommendations and align to most appropriate delivery options

NEXT STEPS – AGREE, PRIORITISE AND ACTION RECOMMENDATIONS

1. ***Endorse Report with ITLT***
   - Socialise, discuss and agree report within UE IT

2. ***Prioritise and categorise recommendations***
   - Plan and prioritise recommendations, align to change portfolio * and consider deliverability impact assessment

3. ***Assign ownership and mobilise based on delivery options***
   - Assign initiative sponsors and owners to define scope, plan and resource initiatives across three delivery options

Delivery Options

3a. Mobilise immediate remediations

Define virtual teams to unpack and drive service improvements

- **E.g. Service Improvement program**

3c) Strategic initiatives

Endorse and seed fund ** to drive and develop broader strategic benefits and convergence or incorporate into 2021-2025 IT Program

- **E.g. Customer Technology convergence Strategy**

No regrets, the drivers are clear and will deliver benefits

Strategic planning, exploring convergence benefits – break away from status quo

Notes:
* alignment of recommendation to existing strategic change portfolio
** provide seed funding to plan and validate greater strategic options that can optimise ongoing spend through to end of next regulatory period 2025

06. Appendices

A. 2016–2020 IT Program of Work

B. 2021–2025 Proposed IT Program of Work

C. Maturity Rating Definition

A. 2016 – 2020 Program of Work

Remediation Program	Program	Initiative	Description
SuperCluster	Supercluster	Replace by CHED Services solution	Resolve availability, DR and performance issues
SuperCluster	Disaster Recovery	Remediate apps	Insufficient DR capacity to support prod. Untested solutions with known gaps
Other – Network	Network Remediation	Refresh and Patch	End of life equipment Equipment not patched to a supported level
Security	Internet Gateway	Migrate UE to CHED Services solution	Resolve security deficiencies and improve availability and performance
Stability	Monitoring	Migrate to CHED Services solution	Not under support, cannot procure licences required for new projects
Stability	Backup	Deploy additional capacity	Insufficient capacity to meet requirements Lack secure solution for OT backups
SuperCluster / Other	Data Centre	Deploy new infrastructure in CHED Services data centres	Pinewood lacks capacity
Security	Desktop Build	Deploy a new build (SOE)	Security controls gaps addressed
Stability	Network Segmentation	Migrate to CHED Services solution	Reduce deployment cost, Accelerate deployment

A. 2016 – 2020 Program of Work

Remediation Program	Program	Initiative	Description
Stability	Infrastructure Support	Consolidate onto a single provider (FIRB implications being assessed)	Maintaining two providers inhibits application sharing, and complicates project activities (including remediation)
Stability	Network design	Redesign UE network	Remove single points of failure Provide full separation between UE sites
Security	OT border remediation	Redesign and implement effective system separation based on CHED Services design	Controls will be placed in an appropriate network zone
Security	IAM Replacement	Extend CHED Services identity management platform to UE	Increase control of access to systems and automate auditing
Security	Security Monitoring	Consolidate UE and VPN security monitoring solutions	Provide a scalable, modern platform
Security	SCADA Whitelisting	Whitelist applications	Provide additional protection against malware to control room workstations
Security	Next Generation Anti Virus	Deploy Crowdstrike	Provide greater visibility and protection against modern threats.
Security	Remote Access	Place under support, or Migrate to CHED Services solution	Part of the solution is not under support EOS working party highlighted remote access as a high priority issue

B. 2021 – 2025 Initiatives

#	Program	Initiative	Description
1	Cloud Migration	Cloud IaaS net capex savings	IaaS migration. BDO Scenario 2 capex savings Labour/materials breakdown
2	Digital Engineering	Activities supporting Digital Engineering	Initiatives that enable the people to retool with new capabilities and tools to make faster, more complex decisions for customer outcomes: BIM/Advanced Design Tools Additional LiDar Capability GIS Data Additions and Improvements 4D/5D/Autonomous Design
3	Device Replacement	Device Replacement (UE, recurrent)	Desktop PC, Laptop PC, iPhone
4	Enterprise Management Systems – SAP	SAP Modernisation S/4 HANA	Move away from unsupported (from 2025) SAP ERP and BW to S/4 HANA. Greenfields or Conversion TBC. Spit from 17 which was for all 3. 17 now just CP/PAL. 17A for UE.
5	Security	Security (UE)	Maintain the reliability and security of the distribution network by mitigating, detecting and responding to cyber attacks
6	Customer Enablement	UE External Portal	*NP: to be updated using CE Business Case – see placeholder item 162/162a*

B. 2021 – 2025 Initiatives

#	Program	Initiative	Description
7	Customer Enablement	eConnect (dependent on roll out of extended MTS functionality to UE)	Online application for receiving and processing Connections, Solar Pre-Approvals (up to 30kWh) and Meter Additions, Alterations and Abolishments. Provides a modern, paperless, web enabled, multi-channel tool for Registered Electrical Contractors, customers and retailers that automates and digitalises their requests and keeps them engaged with the process as it progresses. Will deliver simpler, standardised processes, visibility of status, and SMS/email notifications to keep customers informed. Delivers additional business efficiencies, which are detailed in the supporting models.
8	Flexible Grid	Flexible Grid – placeholder initiative	Catch-all placeholder for Litmus piece (other FG projects marked as TBC to be rolled into this)
9	Enterprise Management Systems – Non SAP	Currency for Common Vegetation Management Solution Modernisation	Also known as FMC-VMS (Vegetation Management System). Currently in use by CP/PAL/UE. Note, this is shared between CP/PAL and UE. Break down into categories not yet completed. All cost added to labour.
10	Enterprise Management Systems – Non SAP	Currency for Common Asset Inspection Solution (Modernisation 2023)	
11	Enterprise Management Systems – BI/BW	Self Service Reporting Platform Currency	Enhancement to Self Service Reporting Platform
12	Compliance	MC Realisation (UE)	Deferred to be realised with the introduction of MC in Victoria

B. 2021 – 2025 Initiatives

#	Program	Initiative	Description
13	Compliance	5 minute settlement –Market Systems & Data Storage (UE)	Implementation of 5 min settlement rule changes
14	Customer Enablement	UE Customer Facing apps (not including eConnect)	• Migrate UE customer facing apps onto Salesforce platform (myEnergy & mySupply) • Salesforce is the platform for customer facing apps – single entry point for customers, consistent customer experience, track and trace capability, integrated branding is in place
		Improved customer navigation	• Implement Contact Centre AI / Speech Analytics, Website AI and Click to Chat
15	Market Systems	UE WebMethods (including Business Process Management and Automation)	Business Process Management and Automation (82a) 76a – Maintaining the current UE WebMethods solution. Upgrade would be required in 2023 if this solution is retained. 82a – • Implement a common platform for business process design, execution and monitoring to serve as the process orchestration layer in the integration architecture • Reduce complexity in the technical integration layer • Oracle Process Cloud Service is a candidate tool given CKI's relationship with Oracle • CP/PAL and UE will need to develop and improve its Business Process Management capability
16	Market Systems	UE IEE Upgrade	4 year cycle 1x upgrade required in the reset period (2023/2024)

B. 2021 – 2025 Initiatives

#	Program	Initiative	Description
17	Market Systems	FCS Upgrade (UE)	New product FCS implemented 2018 will require upgrade in 2023 for UE
18	Market Systems	MTS upgrade (UE)	4 year cycle (1 year prior to IEE upgrade) Last upgrade: 2018 2x upgrades required in the reset period
19	Market Systems	SAP ISU Currency	SAP ISU Upgrades to maintain health and currency
20	Network Management	SIQ software upgrades – std control component	UE SIQ Major & Minor AMI System Upgrades. Major upgrades in 2021 & 2025. Minot upgrade in 2023. It is all Standard Control for SIQ. An AMI component is not applicable. CA 12/9: Note, CP/PAL SIQ will be implemented under the Flexible Grid Power Quality Data Collection (for 2021). A conscious decision was made not to request currency capex for CP/PAL.
21	Enterprise Management Systems – Non SAP	UE Oracle Upgrade	Upgrade Oracle Database to 12c CA19/9: Program changed from Infrastructure to Enterprise Management Systems – Non SAP
22	Network Management	Maintain UE Spatial Viewer Platform (GE's Network Viewer plus)	Visualisation platform for UE employees who monitor, plan and manage assets across our network.
23	Network Management	GIS Smallworld Currency	Capex to maintain currency, including scheduled upgrades.

B. 2021 – 2025 Initiatives

#	Program	Initiative	Description
24	Network Management	SCADA/DMS/OMS Currency: – SCADA (Mosaic) – DMS/OMS (Oracle) – OSI PI	Capex to maintain currency, including scheduled upgrades.
25	Network Management	Outage Management Reporting Currency: – OUA – OBIEE	Capex to maintain currency, including scheduled upgrades.
26	Network Management	Switching Currency: – NARS	Capex to maintain currency, including scheduled upgrades.
27	Network Management	Outages & Emergencies application suite Currency: • Outages & Emergencies • HV Inject • Reclose Database • Phase Angle	Capex to maintain currency, including scheduled upgrades.

B. 2021 – 2025 Initiatives

#	Program	Initiative	Description
28	Network Management	Protection Systems application suite Currency: **Apps 1:** • Micom S1 • Windows Switchgear Operating System • Win ECP • SFT2841, SFT2801, Logipam SF2805, SFT 2826, SFT2821 • SEL–1510 Relay Assistant **Apps 2:** • SEMS Application • Power Quality Mgt	Capex to maintain currency, including scheduled upgrades.
29	Network Management	Network Analytics Currency: – Future Grid Postgres – SAS	Capex to maintain currency, including scheduled upgrades. Equivalent CP/PAL initiative is 115.
30	Enterprise Management Systems – Non SAP	External UE website – Maintain currency and capability	Capital expenditure costs associated with maintaining our existing external facing web sites.
31	Enterprise Management Systems – SAP	SAP Health & Currency	Capital expenditure costs associated with maintaining our existing SAP ERP Systems

B. 2021 – 2025 Initiatives

#	Program	Initiative	Description
32	Telephony	Common Corporate Telephony Solution (Corporate + Contact Centre)	As per Stuart Mason (11/4): – assume upgrade and integration with UE within Reset Period (rather than establishment of a whole new platform) As per Integration Roadmap: · Implement next generation UCS platform for corporate telephone solution and hardware · Consolidate UE and CPPAL into one platform
33	Telephony	Omni-channel uplift	
34	Telephony	Control Room Telephony Upgrades	As per Stuart Mason (11/4): – uplift just completed, will require an upgrade in 2021-25 period. Assume no consolidation. As per Integration Roadmap: Consolidate into one platform· Implement next generation UCS platform for SCADA telephony solution
35	Customer Enablement	Enhanced Embedded Generation (EG) Connections – project workflow tool	*NP: to be updated using CE Business Case – see placeholder item 162/162a* Currently all projects are tracked through Excel across different teams. With the increase in volume of projects, manual tracking becomes harder to maintain. We also have regulatory obligations in this space under the NER (chapter 5 and 5A).

B. 2021 – 2025 Initiatives

#	Program	Initiative	Description
36	Enterprise Management Systems – Non SAP	W1 – Finance, Tax, Treasury. Robotics Process Automation for Finance	Robotics Process Automation for Finance
37	Enterprise Management Systems – Non SAP	W1 – Finance, Tax, Treasury. RecWise	Maintenance of RecWise
38	Enterprise Management Systems – Non SAP	W2 – People, Culture and Learning. Payroll & Compensation module for Success Factors	Implementation of the 'Payroll & Compensation' module for Success Factors (People Central) in 2023
39	Enterprise Management Systems – Non SAP	W2 – People, Culture and Learning.PCL Electronic document management system upgrade	Upgrade of iManage or similar electronic document management system. Note, per Matthew van't Hoff 3/7, imanage infrastructure costs immaterial.
40	Enterprise Management Systems – Non SAP	W4 – Corporate Mgt, Property & real Estate. Insight/Tronsec – UE equivalent to BACS	Tronsec is standalone system providing physical access to sites. Manual works are required to reconcile this system with HR information to determine who should have site/asset access.
41	Enterprise Management Systems – Non SAP	W4 – Corporate Mgt, Property & real Estate. CCTV Upgrade	Currently only depots are covered by CCTV. We propose to expand the number of sites and high risk electrical installations covered by CCTV

B. 2021 – 2025 Initiatives

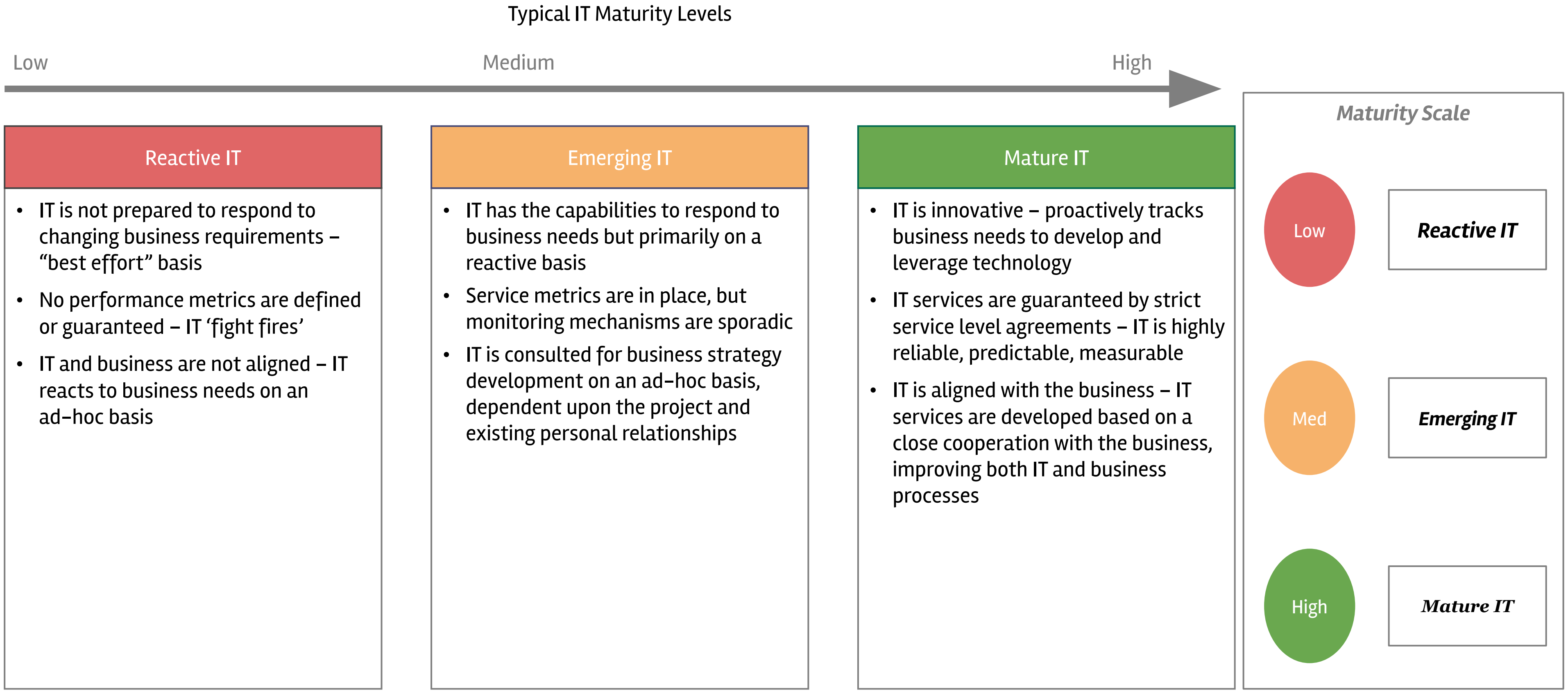
#	Program	Initiative	Description
42	Enterprise Management Systems – Non SAP	W6 – Works Scheduling & Dispatch. Emergency Dispatch Management	Emergency Dispatch Management Currency
43	Enterprise Management Systems – Non SAP	W6 – Works Scheduling & Dispatch. EDNAR (Electrical Dist Network Access Register)	EDNAR (Electrical Dist Network Access Register) Currency. Note EDNAR implemented in 2020/21 for UE to replace the NAR system.
44	Enterprise Management Systems – Non SAP	W7 – Dial Before you Dig & Doc Mgt System. Dial before you Dig (Pelican Corp AIRS software)	Dial before you Dig (Pelican Corp AIRS software)
45	Enterprise Management Systems – Non SAP	W7 – Dial Before you Dig & Doc Mgt System. Meridian Solution (EDMS)	Meridian Solution (EDMS)
46	Enterprise Management Systems – Non SAP	W8 – Copperleaf. Implement 'Asset Awareness' module 2021	Implement 'Asset Awareness' module 2021
47	Enterprise Management Systems – Non SAP	W8 – Copperleaf. Implement 'Predictive Analysis' module 2024	Implement 'Predictive Analysis' module 2024

B. 2021 – 2025 Initiatives

#	Program	Initiative	Description
50	Customer Enablement	*Placeholder – all Scene 2 initiatives (except eConnect)*	*NP: To be split into separate initiatives using CE Business Case.*
51	Infrastructure & Storage	Infrastructure, Storage	Consolidated Business Case – capex impacts of Cloud options (includes Server, Network, Software, SAP HANA, Storage, Exadata, Backup, capacity growth)
52	Enterprise Management Systems – BI/BW	Data Lake	Migrate data to data lake – establish platform
53	Enterprise Management Systems – BI/BW	Data Lake	Set up data lake (licencing, subscription, hosting, infrastructure etc) – establish platform
54	Enterprise Management Systems – BI/BW	Data Lake	UE BW to Enterprise Data Warehouse
55	Enterprise Management Systems – BI/BW	BW/4 HANA Currency Upgrade	Upgrade Enterprise Data Warehouse
56	Compliance	5 minute settlement – Exadata & Backup Storage Costs	Additional storage required for 5 minute settlement data (in addition to standard storage projections)

C. Maturity Rating Definition

The following rating scale has been used to rate IT



Typical IT Maturity Levels

Low Medium High

Reactive IT

- IT is not prepared to respond to changing business requirements – "best effort" basis
- No performance metrics are defined or guaranteed – IT 'fight fires'
- IT and business are not aligned – IT reacts to business needs on an ad-hoc basis

Emerging IT

- IT has the capabilities to respond to business needs but primarily on a reactive basis
- Service metrics are in place, but monitoring mechanisms are sporadic
- IT is consulted for business strategy development on an ad-hoc basis, dependent upon the project and existing personal relationships

Mature IT

- IT is innovative – proactively tracks business needs to develop and leverage technology
- IT services are guaranteed by strict service level agreements – IT is highly reliable, predictable, measurable
- IT is aligned with the business – IT services are developed based on a close cooperation with the business, improving both IT and business processes

Maturity Scale

Low	***Reactive IT***
Med	***Emerging IT***
High	***Mature IT***

A fully mature IT function acts as a Business Integrator and works with the business to deliver complex, technology enabled transformation programs, using innovative technology solutions that result in sustainable business outcomes.