TISN

FOR CRITICAL INFRASTRUCTURE RESILIENCE

Generic SCADA Risk Management Framework For Australian Critical Infrastructure Developed by the IT Security Expert Advisory Group (ITSEAG)

(Revised March 2012)

Disclaimer: To the extent permitted by law, this document is provided without any liability or warranty. Accordingly it is to be used only for the purposes specified and the reliability of any assessment or evaluation arising from it are matters for the independent judgement of users. This document is intended as a general guide only and users should seek professional advice as to their specific risks and needs.

Document Change History

Version	Change Description
1.0a	Initial version for internal review
1.0b	Incorporated internal review feedback
1.1	Final changes for ITSEAG presentation
1.2	Incorporated monitoring cycle into section 3.7.
2.0	Added preface and addressed final review comments.
2.1	Reviewed and updated to latest standards – Dec 2011

Table of Contents

Preface

SCADA systems have traditionally been viewed as being isolated and therefore 'safe' and less exposed to remote cyber attacks. Risk assessment and management methodologies, correspondingly, have largely been directed at legacy SCADA systems in which underlying protocols were designed without modern security requirements in mind.

Business drivers for SCADA integration with enterprise management systems, load management and smart grid environments has meant that SCADA systems have become interconnected with corporate business networks, customer premises and directly or indirectly with the Internet. This, together with the rapid advancement of technology, shifting threat landscape and the changing business environment, is increasing the exposure of SCADA systems to network vulnerabilities and Internet security threats.

Recent incidents such as Aurora and Stuxnet demonstrate that a directed cyber attack can cause physical harm to critical infrastructure. Traditional threat sources have evolved to now include focused foreign nation cyber intrusions and industrial espionage capabilities.

Such changes and attitudes require a new all hazards approach to risk management – one that takes into account Industrial Control Systems, IT, Communications, physical security, supply chains and services and the interconnection of SCADA systems with corporate, partner and service provider networks and the Internet. Organisations are encouraged to foster a culture of security for SCADA system management, operations and procedures.

The SCADA Community of Interest, an Information Technology Security Expert Advisory Group[1] (ITSEAG) working group, has identified risk management as a key issue in maintaining continuity of business and in protecting Australia's critical infrastructure.

[1] *The ITSEAG is part of the Trusted Information Sharing Network (TISN) for critical infrastructure resilience which enables the owners and operators of critical infrastructure to share vital information on security issues. The TISN consists of a number of Sector Groups (SGs) and Expert Advisory Groups (EAGs) which are overseen by the Critical Infrastructure Advisory Council (CIAC). One of the expert advisory groups is the ITSEAG providing advice to the TISN on IT security issues relating to critical infrastructure. The ITSEAG consists of academic specialists, vendors and government representatives who are leaders in the information technology/e-security field. More information on the TISN can be found at http://www.tisn.gov.au. For more information on the ITSEAG, please contact the Secretariat in the Department of Broadband, Communications and the Digital Economy (DBCDE) on (02) 6271 1595 or SCADA@dbcde.gov.au.*

The Generic SCADA Risk Management Framework (RMF) is a high-level document that provides a cross-sector approach to identifying and assessing risks for owners and operators of SCADA systems. The RMF can be tailored to suit a particular sector or organisation and also contains advice on how information security risks can be simplified, included in existing corporate risk management frameworks and presented to senior management.

1 Introduction

1.1 Background

1.1.1 The Australian Government Critical Infrastructure Advisory Council (CIAC) oversees a number of expert advisory and sector groups and advises the Attorney General's Department on matters associated with the national approach to Critical Infrastructure Resilience (CIR).

1.1.2 Sector Groups (SGs), cover key industry sectors across Australia. The IT Security Expert Advisory Group (ITSEAG) advises all SGs on IT Security matters affecting all industry sectors.

1.1.3 This report has been commissioned via the ITSEAG's SCADA working group that contributes to the TISN objective of enhancing the resilience of critical infrastructure (CI) and systems of national importance by assisting with the assessment and implementation of security for SCADA systems across industry sectors.

1.2 Scope

1.2.1 The scope of this report is to detail an industry-wide framework whereby owners and operators of key SCADA systems can assess security risk exposures of these systems and implement security controls to mitigate and manage these risk exposures within acceptable limits.

1.2.2 SCADA systems considered within the scope of the report comprise distributed control systems designed to deliver essential and stabilising services within the Australian economy.

1.3 Key Terms and Definitions

Term	Description
ISM 2012	The Australian Government Information Security Manual published by DSD containing minimum information security standards for Commonwealth Government organisations and often used as a reference by other Australian organisations. ISM 2012 is available from DSD at: http://www.dsd.gov.au/infosec/ism/index.htm
DSD	Defence Signals Directorate.
All hazards approach	A risk assessment approach intended to identify generic risks common to most, if not all, SCADA systems.
AV	Antivirus.
BCP	Business Continuity Plan.
COTS	Commercial Off The Shelf – a term used to describe software and devices that can be purchased and integrated with little or no customisation.
DR	Disaster Recovery – a component of business continuity management.
DRP	Disaster Recovery Plan.
ITSEAG	Information Technology Security Expert Advisory Group.
NII	National Information Infrastructure.
OS	Operating System.
PSPF	Australian Government Protective Security Policy Framework – published by the Australian Attorney General's Department PSPF is available from AGD at: http://www.ag.gov.au/pspf
ISMP	Australian Government Information Security Management Protocols specify information security controls to be used in Commonwealth Government organisations and often used as a reference by other Australian organisations. ISMP is available from AGD at: Information Security Management Protocols
QoS	Quality of Service.
SCADA	Supervisory Control and Data Acquisition.
SRMS	SCADA Security Risk Management System.
TRA	Threat and Risk Assessment.
RTP	Risk Treatment Plan.
Current risk exposure	The level of risk associated with an asset before the application of any risk mitigation measures.
Treated risk exposure	The level of risk associated with an asset after the application of risk mitigation measures.
Controlled risk	Level of risk posed to system assets after specific/additional risk mitigation controls are implemented to address current risk exposure.
Residual risk	Level of risk remaining after additional risk treatment.

1.4 References

- International Critical Information Infrastructure Protection (CIIP) Handbook 2008/2009.
- ISM 2012 – Australian Government Information Security Manual, Defence Signals Directorate.
- Defence Signals Directorate Top 35 Mitigations July 2011.
- IEC 60870.1 Telecontrol Equipment and Systems – General Considerations.
- IEC 60870.5 – 101 to 104 Telecontrol Equipment and Systems – Transmission Protocols.
- AS/NZS 31000:2009 Risk Management – Principles and Guidelines, Standards Australia.
- ISO/IEC 27005:2011 Information Security Risk Management, Standards Australia.
- AS/NZS ISO/IEC 27001:2006 Information Security Management systems requirements, Standards Australia.
- AS/NZS ISO/IEC 27002:2006 Code of practice for information security management, Standards Australia.
- Australian Government Protective Security Policy Framework 2010, Attorney General's Department, June 2010.
- Australian Government Information Security Management Protocols and guidelines 2011, Attorney General's Department, July 2011.
- System Protection Profile – Industrial Control Systems, National Institute of Standards and Technology (NIST), Version 1.0.
- The Cross-Sector Roadmap for Cyber Security of Control Systems, 30 September, 2011(developed by the Industrial Control Systems Joint Working Group (ICSJWG), with facilitation by the US Department of Homeland Security's National Cybersecurity Division (NCSD)).

1.5 Acknowledgements

Saltbush would like to acknowledge those who contributed to the 2012 review of this framework:

- **CERT Australia**: Clint Felmingham
- **Water** : Helen Foster
- **Energy** : Andrew Tanner, Babu Srinivas, Rob Evans
- **Police** : Barry Blundell, Tom Cleary
- **Transport** : Darren Wolff
- **DBCDE, SCADA CoI Secretariat**: Chris Marsden, Peter Webb

2 Tailoring the Risk Management Framework

2.1.1 When tailoring this Generic SCADA RMF to suit a particular sector or organisation, the following points should be noted:

- The framework has been developed to cover the basic functions of a distributed SCADA system. Organisation and sector-specific risks will need to be evaluated, and if necessary, incorporated into SCADA risk management frameworks at the sector or organisational level.
- Where organisations have existing Corporate Risk Management and Security Frameworks in place it is important that this SCADA risk framework aligns with the corporate frameworks to ensure organisational consistency.
- The definition of threat likelihood, consequence of risk realisation, and the matrix in which risk is calculated at a National Information Infrastructure level is given in Section 3.5 and Section 3.6. It is recommended that organisations align these values to their internal corporate risk parameters.
- When establishing the context of any sector or organisational risk management activities, Figure 3-2 should be assessed and possibly refined as appropriate to the applicable sector or organisation – this will also lead to a re-evaluation and update of SCADA process enablers as shown in Figures 3-2, 4-1 and Table 4-1.
- Risks associated with external interdependencies such as an incident impacting multiple organisations (for instance with supply chains and business partners) should be considered.

2.1.2 In accordance with the definitions in Section 3.4, the ‘Current Risk’ columns in the Section 6 TRA will need to be updated should these values be altered.

2.1.3 Treatment options in Section 7 (RTP) are in some cases opportunistic. A significant goal of this RTP is to highlight the ‘desirable’ requirements of a secure SCADA system, and it is recommended that each of the RTP security controls be used when determining the most appropriate information security configuration for a secure SCADA system.

2.1.4 Finally, the determination of information security risk exposures, and the level to which they are reported to senior management, often results in the confusion of security issues with technical and operational details. Section 8 of this framework suggests a mechanism by which such information can be summarised and presented.

3 Risk Management Methodology

3.1 Overview

3.1.1 The methodology is adopted for the generic SCADA risk management process is detailed in the following subsections.

3.1.2 The methodology is compliant with recognised standards including

- ISO/IEC 31000:2009 Risk Management – Principles and Guidelines.
- ISO/IEC 27005:2011 Information Security Risk Management.
- ISO/IEC 27001:2006 Information Security Management Systems Requirements.
- ISO/IEC 27002:2006 Code of Practice for Information Security Management.

3.1.3 Of note is that the risk management methodology encompasses an all hazards approach to risk management for SCADA systems and can be used to identify and analyse the risk exposures presented through a wide variety of potential security vulnerabilities.

3.2 Framework

3.2.1 The RMF is based on traditional standards based risk management frameworks, as described in ISO/IEC 31000 - Risk Management and ISO/IEC 27005 – Information Security Risk Management standards and shown in the following figure.

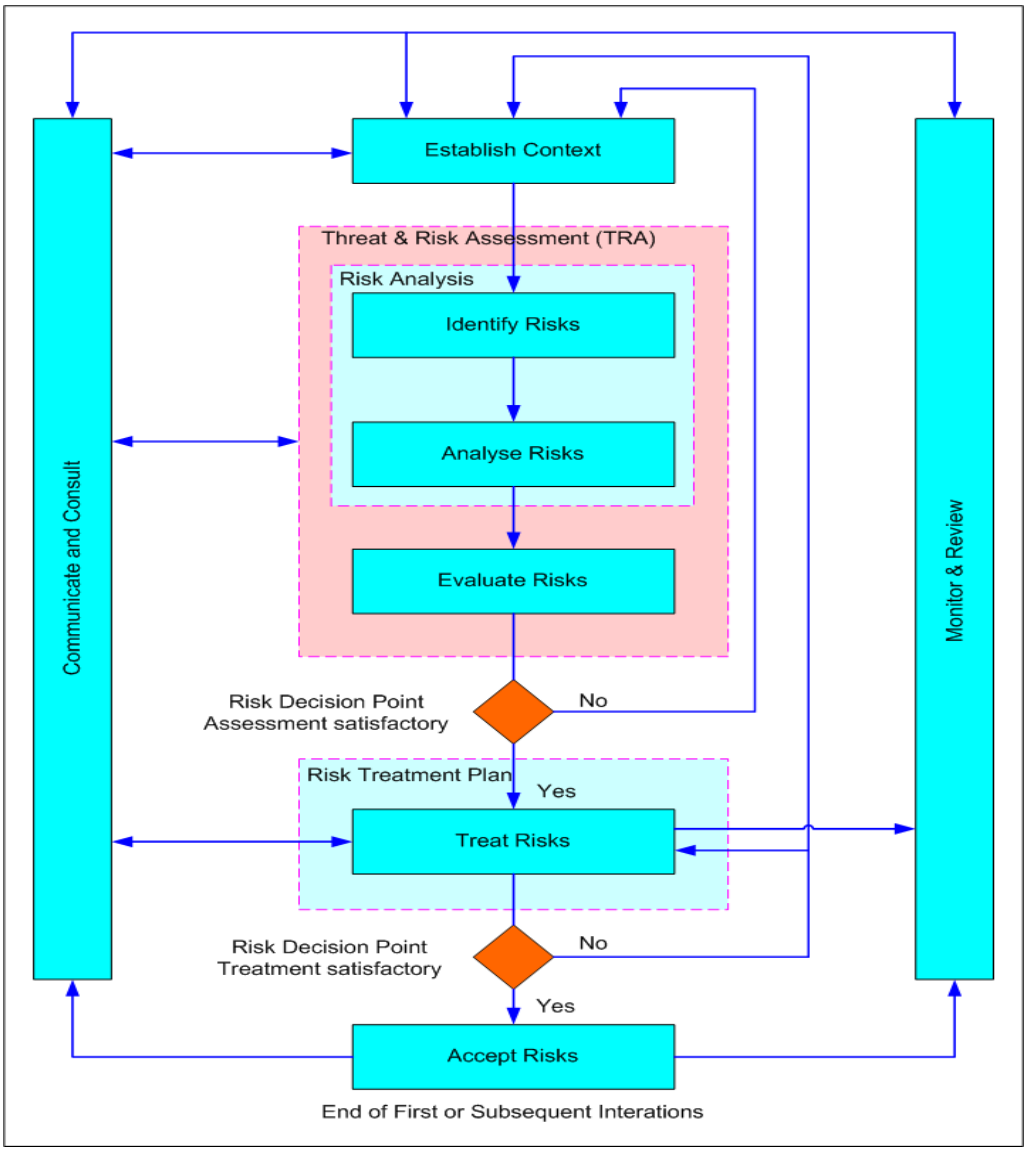

Figure 3-1 Risk Management Framework ISO 31000 and ISO27005

3.2.2 Establishment of the context for the Generic SCADA RMF involves defining the framework scope and identifying the assets that are potentially at risk.

3.2.3 Identification, analysis and evaluation of risks together comprise the Threat & Risk Assessment (TRA) component of the framework.

3.2.4 The risk treatment component comprises the development of a Risk Treatment Plan to address the risk exposure to the assets identified in the threat and risk assessment process.

3.2.5 There are two Risk Decision points that ensure sufficient and accurate information has been obtained or that another iteration of risk assessment or risk treatment is initiated.

3.2.6 The risk acceptance activity ensures that residual risks are explicitly accepted by the SCADA stakeholders and senior management of the organisation.

3.2.7 During the whole security risk management process it is important that communication and consultation with stakeholders and operational staff associated with the secure implementation and operation of the SCADA system under consideration.

3.2.8 The monitor and review component of the process comprises the controls put in place specifically to ensure that the Generic SCADA RMF operates effectively over time.

3.3 Establish Context

3.3.1 The scope of the Generic SCADA RMF encompasses the core components of a distributed SCADA network that would be expected to be found in the majority of critical infrastructure service provider organisations.

3.3.2 This comprises the process components as shown in Figure 3-2.

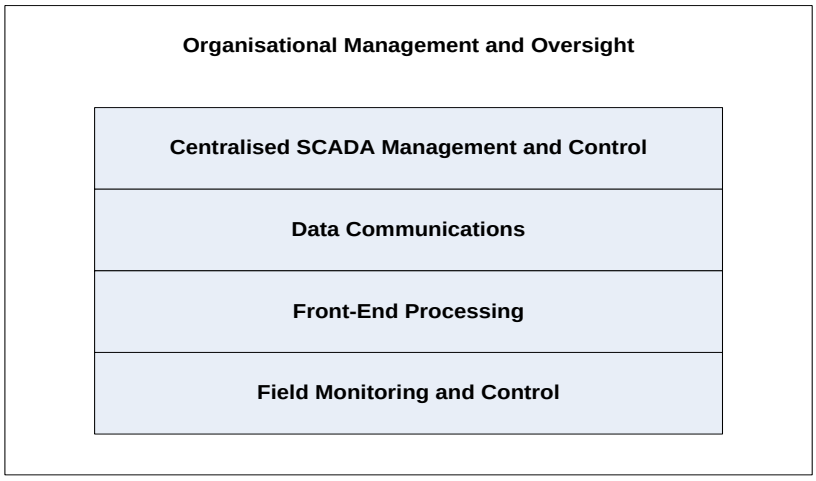

Figure 3-2 Generic SCADA Processes

3.3.3 The assets that are likely to be threatened can therefore be derived by considering the enablers[2] that allow the identified processes in Figure 3-2 to occur.

3.3.4 These enablers can be derived by identifying the people, the places, and the products required to ensure the processes can be carried out.

3.3.5 Each enabler is owned. The owner is the responsible authority within operational sections of the organisation for ensuring that mitigating controls are appropriately implemented.

3.3.6 The typical authority responsible for the enablers is contained in the "Owner" column; however each organisation using this guide ultimately determines who the responsible authority is.

3.3.7 The owner and description should be modified to suit the positions in each organisation.

3.3.8 Examples of typical owners:

Owner	Description
CEO	Chief Executive Officer – Head of organisation
CIO	Chief Information Officer – IT infrastructure and architecture
HR	Human Resource Executive – personnel and contracting
SA	Security Advisor – covering physical and environmental enablers
ITSA	Information Technology Security Advisor – covering information security and logical access controls
CFO	Chief Financial Officer – covering asset purchasing/disposal and financial delegation
Senior Engineer	Senior Engineer – Manager of technical services

Table 3-1 Owners of Enablers

[2] Enablers are those assets that support the delivery of in-scope business processes

3.3.9 Each organisation should identify their internal asset “owners”.

3.3.10 Section 4 of this framework identifies example generic enablers through the analysis of the generic SCADA processes.

3.4 Identify Risks

3.4.1 Having identified the assets required to enable generic SCADA processing to occur, the next activity is to identify the vulnerabilities to which each asset is exposed.

3.4.2 Vulnerabilities to assets can be identified through consideration of the potential threats, whether they are malicious, accidental, natural or environmental, to the:

- Confidentiality of systems and information;
- Integrity of systems and information; and/or
- Availability of systems.

3.4.3 Threat Sources

3.4.4 A threat is defined as an action perpetrated by a threat agent. While such sources are often people, natural and environmental factors can also contribute to the realisation of a threat. In addition, not all threat sources will attempt to enact a threat with malicious intent.

3.4.5 The following subsections list the general categories for threat sources that may lead to the realisation of a threat to the identified assets under consideration.

Trusted Sources with Malicious Intent – T1

3.4.6 Such sources comprise individuals or organisations with which the system owner shares some level of trust, but wish to deliberately cause harm to the in-scope control system.

3.4.7 Examples could include a disgruntled systems administrator or user, criminal elements within a partner organisation such as a business peer, or a subcontractor unhappy about the impending termination of their contract.

Trusted Sources without Malicious Intent – T2

3.4.8 Sources will generally be individuals or business partners with whom the system owner shares some level of trust, but who unknowingly cause harm to the in-scope system.

3.4.9 Examples could include an error by a control system administrator or user, a business partner being unable to supply critical system services, or a procedural operating error that leads to an undesirable system state or inappropriate information disclosure.

External Sources with Malicious Intent – T3

3.4.10 These sources are typically individuals or organisations that have a desire to threaten the in-scope system, but do not share an implicit trust relationship with the control system owner.

3.4.11 Examples could include industrial spies, hackers, activist groups, criminal elements, foreign government agencies.

External Sources without Malicious Intent – T4

3.4.12 Such sources will have neither an implied level of trust within the in-scope assets nor the desire to cause harm to the system.

3.4.13 Examples could include users of communications infrastructure and suppliers of services on which the control system indirectly depends.

Environmental – T5

3.4.14 Such sources are usually disruptive natural events, or significant man-made accidents such as an aircraft crash, or oil refinery explosion.

3.4.15 Examples could include fire, flood or storm and additionally the potential effect on control system assets from dangerous goods (e.g. a nearby chemical factory) and epidemics (bird flu, swine flu etc).

3.5 Analyse Risks

3.5.1 Having identified vulnerabilities to assets, they should be analysed to determine the asset's **current** risk exposure with current controls in terms of:

- **Likelihood** of occurrence; and
- **Consequence** of realisation.

3.5.2 Each of these parameters is to be determined in accordance with appropriate scales suited to the organisation's internal risk management framework. The scales used in this generic framework are shown in Tables 3-2 and 3-3, and correspond to those used by the Australian Government NII agencies.

3.5.3 Likelihood of Occurrence – Example

Likelihood Descriptor	Likelihood Description Statements
Almost Certain	The event is EXPECTED to occur in most circumstances.
Likely	The event will PROBABLY occur in most circumstances and is expected at some time.
Possible	The event MIGHT occur at some time but is not expected.
Unlikely	The event COULD occur at some time.
Rare	The event MAY occur in exceptional circumstances.

Table 3-2 Likelihood of Occurrence

3.5.4 Consequence of Realisation - Example

Consequence Descriptor	Financial	Safety	Business Productivity	Operational	Reputation	Legal Regulatory
Catastrophic	Possible loss >$40M	Permanent injuries/ deaths	Catastrophic impact on operations	Supply disrupted > 2,000,000 customers Major Failure to entire Grid Black Start	Extended media coverage; major government embarrassment or loss of public support; public enquiry Removal of CEO	Loss of operating licence or directors/senior management charged and convicted
Major	Possible loss $16M - $40M	Permanent injury /stress	Failure of one or more key organisational objectives leading to major disruption	Supply disrupted > 1,000,000 customers Major Failure to parts of the Grid	Heavy media coverage; government embarrassment or loss of public support.	Inquest in to business resulting in an enforcement order fine and court conviction
Moderate	Possible loss $4M - $16M	Injury requiring medical treatment / long term incapacity.	No threat to achievement of objectives but could result in some moderate disruption	Supply disrupted > 200,000 customers From a single event	Customer comments escalated to management; minor media coverage.	Likely fine or prosecution. Administrative undertaking
Minor	Possible loss $1M - $4M	Injury requiring first aid treatment / temporary loss of time.	Minor reduction in effectiveness and efficiency for a short period	Supply disrupted to < 1000 customers for less than 1 week	Adverse customer comments	Warning issued by regulator
Insignificant	Possible loss <$1M	Injury resulting in no loss of time	Negligible impact to effectiveness and efficiency	Supply disrupted to < 100 customers for less than 1 day	Manageable adverse customer comments	No legal or regulatory consequence.

Table 3-3 Consequence of Realisation

3.6 Evaluate Risk

3.6.1 Risk Matrix - Example

3.6.2 Current risk exposure, in terms of likelihood and consequence values, can be determined using the risk matrix table below:

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

Table 3-4 Risk Calculation Matrix

3.6.3 Risk Exposure & Risk Acceptance - Example

3.6.4 Risk exposure levels and responsibility for acceptance or residual risk are as follows:

Risk Rating	Responsibility for Risk Acceptance	Action
Extreme	Board; CEO	Would be expected to seriously damage the organisation's ability to continue to operate with the confidence of its customer base or corporate owners. Could result in serious social or economic damage and may affect the organisation's ability to continue operations.
High	CEO; Executive; Risk Manager	Would be expected to have a significant impact on corporate budgets and organisational reputation. Could lead to extended service disruption and seriously inconvenience or have health impacts on a wide section of the customer base.
Medium	Risk Manager Senior Manager	Likely to result in short term, localised, disruption to services and require escalation through line management. Could generate localised adverse media comment and moderate penalties or costs unable to be borne via normal operational budgets.
Low	Risk Manager Senior Manager	Unlikely to have an impact that could not be satisfactorily dealt with via normal operational procedures.

Table 3-5 Risk Exposure Levels & Risk Acceptance

3.7 Treat the Risk

3.7.1 Once risk exposure has been determined all risks must be treated. Treatment options include:

a) ***Accept***: - do nothing and accept the current level of evaluated risk;
b) ***Avoid***: - cease doing the business activity that brings about the possibility of the threat occurring;
c) ***Transfer***: - pass the responsibility for implementing mitigating controls to another entity. Responsibility for threat and risk management remains the responsibility of the organisation, and
d) ***Reduce***: - implement controls to reduce risk to an acceptable level.

3.7.2 The risk table provided in Section 5 contains a column for recording risk treatment. It also contains a cross-reference to the Risk Treatment Plan (RTP) which is shown in Section 6.

3.7.3 This plan details the controls that may be used to reduce risk to an acceptable level. Organisations may interpret these controls for their own use – and

provide additional controls if required. The cross-reference in the RTP points to where the identified threat has been addressed.

3.7.4 The RTP provides for a reassessment of risk, once controls have been selected and implemented. The RTP can also act as a management plan to provide a "status" of implementation.

3.7.5 An example work through is provided in Section 4, illustrating the process flow used in this risk framework.

3.8 Communication and Consultation

3.8.1 This environment comprises the identification and involvement of all stakeholders involved in the operation of the SCADA network and the management of corporate risk across the organisation.

3.8.2 In addition to the day-to-day operation of the SCADA system(s), it is important to ensure that risk information is communicated through the organisation's management and is highlighted (generally in summarised form) to the executive forum charged with overall organisational risk management.

3.8.3 The manner in which this environment is implemented will be highly dependent on the operation of each affected organisation, and is therefore considered to be outside the scope of this report, however suggested management reporting techniques are included in section 8.

3.9 Monitor and Review

3.9.1 The monitoring and review component needs to be implemented to ensure that:

a) Risk exposures are monitored, re-evaluated and revised as appropriate over time;
b) Risk exposures are updated in a timely fashion in response to significant events such as changes to the organisation's operations and influencing external events;
c) Ensuring that identified remediation controls are effective and efficient in both design and operation;
d) Identification of emerging risks; and
e) The risk management framework itself is operating effectively.

3.9.2 As with the communications and consultation environment, the mechanism(s) used to implement this component of the risk management framework need to be implemented within current organisational management and monitoring processes.

3.9.3 The following diagram and table provides a guide to successful implementation and ongoing effectiveness.

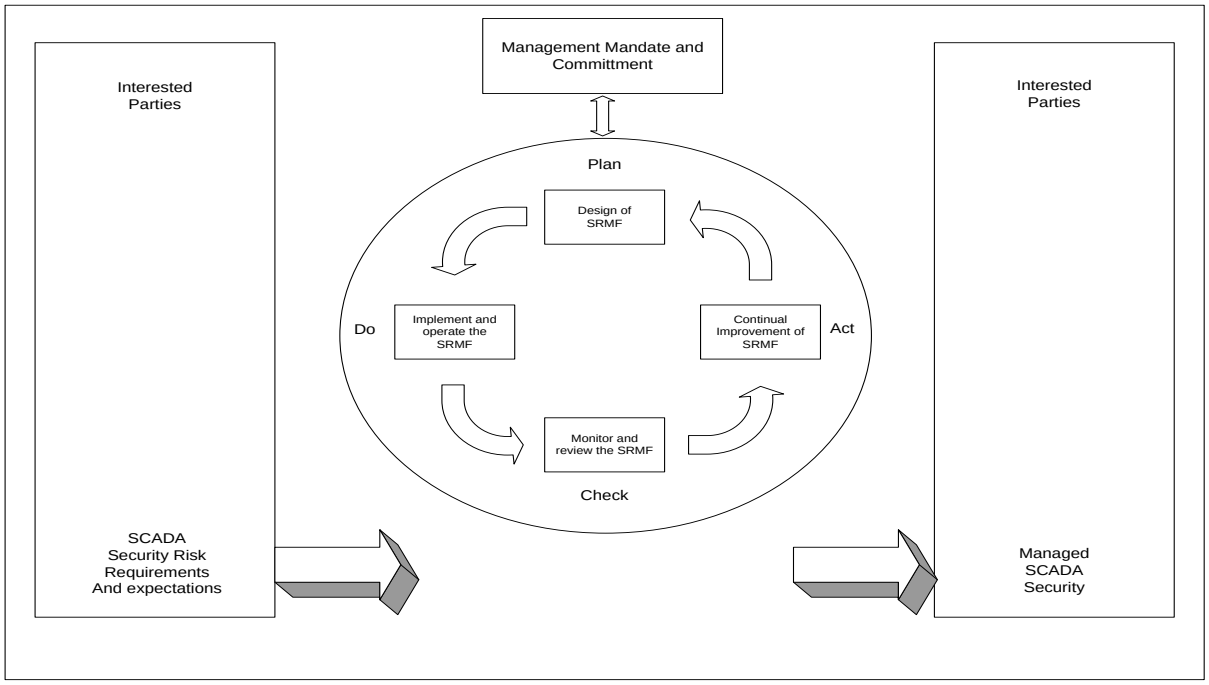

Figure 3-3 PDCA model applied to SCADA Security Risk Management System

ISO 27001 Information Security Management System Process (ISMS)	SCADA Security Risk Management System
Plan	Establish SCADA Security Risk Management Framework, applicable policies, objectives, processes and procedures relevant to managing risk and improving security to deliver results in accordance with an organisation's overall policies and objectives.
Do	Implement and operate the SCADA Security Risk Management Framework policy, controls, processes and procedures.
Check	Assess and, where applicable, measure process performance against SCADA Security Risk Management Framework policy, objectives and practical experience and report the results to management for review.
Act	Take corrective and preventative actions, based on the results of the internal audit and management review or other relevant information to achieve continual improvement of the SCADA Security Risk Management Framework.

Table 3-6 SRMS Management and Monitoring Guide

3.10 Risk Assessment Terms and Conventions

3.10.1 Terms

Risk levels referred to throughout this Generic SCADA RMF(and which are recommended for use in any Security risk management plans) are:

- *Current Risk* is the level of risk posed to system assets with existing and implemented risk mitigation controls;
- *Controlled Risk* is the level of risk posed to system assets after specific/additional risk mitigation controls are implemented to address current risk exposures; and
- *Residual Risk* is the level of risk remaining after additional risk treatment.

3.10.2 Conventions – Risk Assessment

The following table describes the abbreviations used within the Risk Assessment below.

Term	Value	Description
Threat Type	C	Confidentiality – refers to unauthorised disclosure
	I	Integrity – refers to unauthorised alteration
	A	Availability – refers to unauthorised loss or destruction
Risk Rating	E	Extreme Risk
	H	High Risk
	M	Medium Risk
	L	Low Risk

Table 3-7 Conventions of Risk Assessment

3.10.3 Conventions – Risk Treatment Plan

The following table describes the abbreviations used within the Risk Treatment Plan to demonstrate the effective implementation of controls documented.

Term	Value	Description
Controls Legend		Proposed security control or mitigation strategy
		Proposed security control that has been rejected by management
		Security control that is not implemented and effective
		Security control that is only partially implemented and effective
		Security control that is fully implemented and effective

Table 3-8 Conventions Risk Treatment Plan

4 Generic SCADA Assets

4.1 Generic SCADA Process Model

4.1.1 The following diagram illustrates the generic nature whereby the SCADA-related processes have been decomposed in order to implement a generic risk management framework.

4.1.2 This facilitates the identification of affected organisational SCADA assets through the identification of the enablers associated with these processes.

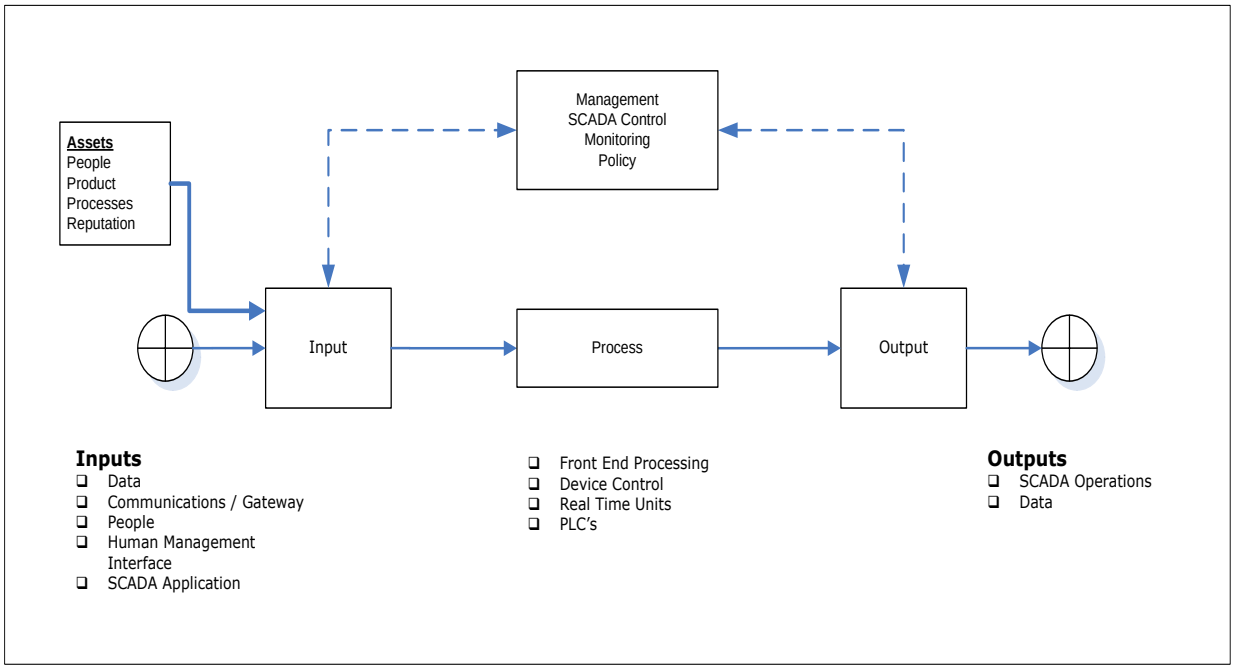

Figure 4-1 Generic SCADA Process Model

4.2 Generic SCADA Enablers - Example

4.2.1 As partially identified in the previous subsection, the following table identifies the enablers likely to be found in a generic SCADA system:

Category	Enabler	Owner	Asset ID
People	Users and operators of the SCADA system	HR Mgr	Pe.1
Products	Buildings and Sites	Property Mgr	P.1
	Communications and Networks	CIO	P.2
	SCADA Application Software	Senior Engineer	P.3
	SCADA Hardware and Operating System (OS)	Senior Engineer	P.4
	SCADA Field Devices	Senior Engineer	P.5
	Supporting Utilities	CIO	P.6
Processes	Management Control and Feedback	CEO	Pr.1
	Information Management	CIO	Pr.2
Reputation	Corporate Reputation	CEO	Re.1

Table 4-1 Generic SCADA Process Enablers

5 Worked Example of Threat and Risk Assessment Framework

Step 1 – Identify what process we are protecting – in this instance it is SCADA system

Step 2 – We identify the enablers that make this process occur – in this example we will select "Application Software".

Category	Enabler	Owner	Asset ID	Notes
Product	SCADA Application Software		P.3	SCADA Application that monitors and manages SCADA assets

Step 3 – Threat and Risk Assessment – Assess risk against the threat of the "Loss of Confidentiality, Availability or Integrity". This gives the Current Risk, which is the level of risk with existing and implemented controls in place. (NB: only loss of confidentiality is demonstrated in this example.)

Asset ID	Common potential points of failure and known vulnerabilities	Threat Type	Threat sources	Current Risk			Treatment Option & reference
				Con-sequence	Likeli-hood	Risk Rating	
P.3 (SCADA Application Software)	Lack of security hardening	C	T1,T2, T3,T4	Moderate	Likely	High	Reduce F1

Step 4 – Risk Treatment Plan – as the current risk rating in this example is "High", treat the risk by selecting the "Reduce" option. How this risk reduction is realised is detailed in the "Risk Treatment Plan" at "C2". An extract from the RTP is provided below

Ref	Control Objectives	Selection of controls to achieve objectives Controls	Controlled Risk		Residual Risk
			Con-sequence	Likeli-hood	

F1	To ensure software can withstand unauthorised access Attempts	Secure SCADA software configuration aligned with (ISO 27002), (CIP Standards)	Moderate	Unlikely	Medium

Table 5-1: linkage between the Asset Register, TRA and RTP

Step 5 – once the control can be proven to be in place, the controls are assessed for effectiveness and the risk level for that threat can be re-evaluated. In this example, risk has been reduced from “High” to “Medium” because the likelihood has been reduced from “Likely” to “Unlikely”.

A reference to a control identified in a standard is included to demonstrate compliance and linkage to the standard.

6 Example SCADA Threat and Risk Assessment

Asset ID	Common potential points of failure and known vulnerabilities	Threat Type	Threat sources	Current Risk			Treatment Option & reference
				Con-sequence	Likeli-hood	Risk Rating	
Pe.1 People	Social Engineering – obtaining information on system layout and on those who manage it. Known to have occurred	C	T1, T2, T3	Moderate	Likely	High	Reduce A1
	Employee vetting – employees with access to SCADA control systems do not have the appropriate background checking conducted prior to engagement resulting in possible data leakage, data corruption, damaged reputation and business relationships		T1, T2				
	Account management – sharing of passwords by employees leading to poor chain of evidence and/or information compromise		T1, T2				
	Information security breaches - past employees or service providers freely disclose information to unauthorised persons		T1, T2				
	Disgruntled Staff including contractors – who subsequently lose their integrity in relation to job performance	I	T1, T2	Moderate	Likely	High	Reduce A2
	3rd Party dependencies – where the integrity of the 3rd party is essentially unknown		T1, T2				
	Ineffective security awareness training - leads to the introduction of malicious code or viruses, disclosure/ theft of information via portable storage devices		T1,T2				
	Issue-motivated interference – leading to biased or one dimensional thinking which affects job performance		T1, T2				
	Loss of Key Personnel and/or Corporate Knowledge	A	T1, T2	Moderate	Almost Certain	High	Reduce A3
	Lack of skills / knowledge – leads to accidental issues with irregular data modification		T1, T2				
	Industrial relations breakdown – leading to staff not being available for long periods of time or to perform critical functions. Legal activity may result.		T1, T2				
	Health related event – absenteeism		T1, T2				
Pr.1 (Management	Inappropriate management structure, lack of security framework, poor allocation of security roles and responsibilities	C	T1, T2, T3, T4, T5	Catastrophic	Likely	Extreme	Reduce B1

Asset ID	Common potential points of failure and known vulnerabilities	Threat Type	Threat sources	Current Risk			Treatment Option & reference
				Con-sequence	Likeli-hood	Risk Rating	
Control & Feedback)	Ineffective change/configuration/release management – introduction of unapproved, untested hardware or software		T1, T2, T3, T4, T5				
	Ineffective management forum/committee, limited stakeholder participation or leadership, poor corrective and preventative actions for security issues, increased severity of incidents	I	T1, T2, T3, T4, T5	Catastrophic	Likely	Extreme	Reduce B2
	Ineffective or lack of defined service level agreements (SLA's) with business owners, ICT Teams and service providers		T1, T2, T3, T4, T5				
	Incident management – poor evidence gathering, preservation and inability to identify that a compromise has actually occurred		T1, T2, T3, T4, T5				
	Business functionality driven initiatives verses security - introduce vulnerable systems and applications		T1, T2				
	Failure in duty of care, lack of security policy and direction		T1, T2, T3, T4, T5				
	Project management – lack of security and/or system considerations during project planning, implementation, operation and review resulting in avoidable issues and/or incidents	A	T1, T2, T3, T4, T5	Catastrophic	Likely	Extreme	Reduce B3
	Business Continuity Management (BCM) – lack of resiliency and redundancy, lack of identification of Maximum Acceptable Outage, Recovery Point Objectives, Recovery Time Objectives resulting in variable business continuity responses		T1, T2, T3, T4, T5				
	Ineffective and/or one-way communication – no security committee to manage and provide oversight of security		T1, T2, T3, T4, T5				
P.1 Building / Site	Degraded security environment through site isolation	C	T1, T2	Minor	Possible	Medium	Reduce C1
	Vandalism	I	T1, T2	Minor	Possible	Medium	Reduce C2
	Poor maintenance		T1, T2				
	Environmental disaster		T1, T2				
	Natural disaster	A	T1, T2	Moderate	Unlikely	Medium	Reduce C3
	DR process failure		T1, T2				

Asset ID	Common potential points of failure and known vulnerabilities	Threat Type	Threat sources	Current Risk			Treatment Option & reference
				Con-sequence	Likeli-hood	Risk Rating	
	Accidental damage - environmental impact resulting in loss of service, damage to servers, infrastructure, possible harm to employees		T1, T2				
	Sabotage and wilful damage		T1, T2				
	OH&S non-compliance		T1, T2				
	Poor design & Planning – lack of input concerning physical and protective security resulting in unsafe and/or insecure buildings and sites.		T1, T2				
Pr.2 Information Management	Inappropriate access control – Overuse of Local administrative privileges	C	T1, T2	Moderate	Almost Certain	High	Reduce D1
	Inappropriate equipment disposal – No sanitisation		T1, T2				
	Account management – accounts not deactivated resulting in unauthorised access by past employees/service providers. Weak password policies leading to easy access to systems, accounts and infrastructure by unauthorised actors		T1, T2				
	Lack of security controls in contractual agreements		T1, T2				
	Poor version control and data quality	I	T1, T2	Moderate	Almost Certain	High	Reduce D2
	Lack of information ownership and information classification		T1, T2				
	Lack of monitoring and audit processes.		T1, T2				
	Too much information		T1, T2				
	Lack of documentation		T1, T2				
	Incorrect documentation		T1, T2				
	Untested procedures (Back-up etc.)	A	T1, T2	Moderate	Almost Certain	High	Reduce D3
	Lack of capacity planning		T1, T2				
	Change/Configuration/Release management – introduction of unapproved, untested hardware or software		T1, T2				
P.2 Communications & Networks	Unauthorised disclosure via 3rd party carrier services	C	T1, T2	Minor	Likely	Medium	Reduce E1
	Open communication protocols are used		T1, T2				
	Mis-configuration leading to unauthorised access and disclosure		T1, T2				

Asset ID	Common potential points of failure and known vulnerabilities	Threat Type	Threat sources	Current Risk			Treatment Option & reference
				Con-sequence	Likeli-hood	Risk Rating	
	Security holes in protocols and equipment		T1, T2				
	Data path over shared networks resulting in uncontrolled access to data		T1, T2				
	Failure to segment network – allowing entire network compromise		T1, T2				
	Unsecured wireless networks – allowing unauthorised access, network compromise		T1, T2				
	Lack of diversity in communication paths lead to communication failure	I	T1, T2	Moderate	Almost Certain	High	Reduce E2
	Data path interference – redirections, man-in-the-middle attacks, eavesdropping		T1, T2				
	Irregular system log analysis - resulting in information security incidents not being analysed to further improve information security		T1, T2				
	Poor or non-existent software patch management – vulnerabilities to communications equipment routers, switches, firewalls		T1, T2				
	Lack of monitoring capacity planning and QoS issues	A	T1, T2	Moderate	Almost Certain	High	Reduce E3
	No redundancy / false redundancy		T1, T2				
	Interference from other transmissions		T1, T2				
	Vendor pricing or service level changes		T1, T2				
P.3 SCADA Application Software	Lack of security hardening	C	T1, T2	Moderate	Likely	High	Reduce F1
	Poor or non-existent software patch management – vulnerabilities to operating systems and/or applications	I	T1, T2, T3, T4	Major	Likely	High	Reduce F2
	Loss of provider and no escrow agreement		T1, T2				
	Off shoring – vendor / service provider moves offshore or sub contracts application support		T1, T2				
	Takeovers and mergers		T1, T2				
	Change management and lack of flexibility to adapt to changing requirements and lack of user acceptance testing process		T1, T2				
	Technology changes – leading to software being outdated		T1, T2				

Asset ID	Common potential points of failure and known vulnerabilities	Threat Type	Threat sources	Current Risk			Treatment Option & reference
				Con-sequence	Likeli-hood	Risk Rating	
	System complexity		T1, T2				
	Unaware of implications in implementing security controls		T1, T2				
	Lack of visibility and access to source code	A	T1, T2	Major	Likely	High	Reduce F3
	Lack of scalability in software solutions		T1, T2				
	SCADA Application failure		T1, T2				
	Vested interests in particular products		T1, T2				
P.4 SCADA Hardware including operating System	Obsolete equipment or Operating System – unable to be patched	C	T1, T2	Moderate	Almost Certain	High	Reduce G1
	Lack of hardening – system open to vulnerabilities.		T1, T2				
	Poor Patch Management – Operating Systems		T1, T2, T3,T4				
	Inappropriate access controls		T1, T2				
	Improper patch management / change management	I	T1, T2	Moderate	Likely	High	Reduce G2
	Incompatibility with the application		T1, T2				
	Vested interests in particular products	A	T1, T2	Moderate	Almost Certain	High	Reduce G3
	Equipment failure		T1, T2				
	Environmental failure such as air conditioning, UPS		T1, T2				
	Damage as a result of lack of electrical isolation		T1, T2				
	Malicious software		T1, T2				
	Lack of capacity monitoring and planning		T1, T2				
	Lack of redundancy hardware		T1, T2				
	No spares management		T1, T2				
P.5 SCADA Field	As for SCADA HW, SW App	C	T1, T2	Moderate	Likely	High	Reduce H1

Asset ID	Common potential points of failure and known vulnerabilities	Threat Type	Threat sources	Current Risk			Treatment Option & reference
				Con-sequence	Likeli-hood	Risk Rating	
Devices	Open access – security issues including access back to central systems		T1, T2				
	Bypassing traditional security framework		T1, T2				
	Default security configuration		T1, T2				
	Default security configuration – retention of default user names and passwords		T1, T2				
	Lack of security hardening – also inability to security harden		T1, T2				
	As for SCADA HW, SW App	I	T1, T2	Minor	Likely	Medium	Reduce H2
	Dependency and use of COTS devices.		T1, T2				
	Introduction of open technology field devices (inc unstable operating Systems, less robust hardware)		T1, T2				
	As for SCADA HW, SW App	A	T1, T2	Moderate	Almost Certain	High	Reduce H3
	Failure to operate - dependence on communications links (Denial of Service)		T1, T2				
	More vulnerable to physical damage		T1, T2				
	Lacking in remote management capability		T1, T2				
P.6 Supporting Utilities	Breach of confidentiality when power fails	C	T1, T2	Minor	Possible	Medium	Reduce I1
	Lack of power & air-conditioning Quality and reliability	I	T1, T2	Moderate	Likely	High	Reduce I2
	Loss of power supply – leads to equipment shutdown and loss of availability		T1, T2				
	Loss of air-conditioning – Leads to equipment overheating, shutdown and loss of availability	A	T1, T2	Major	Likely	High	Reduce I3
	Lack of backup power – No alternative supply or generator installed		T1, T2				

Asset ID	Common potential points of failure and known vulnerabilities	Threat Type	Threat sources	Current Risk			Treatment Option & reference
				Con-sequence	Likeli-hood	Risk Rating	
	Lack of UPS, generator maintenance results in power failure		T1, T2				
	Non-diversity of supply leads to failure due to external influences in grid.		T1, T2				
	Damage to supporting utilities due to Lightning, Fire etc.		T1, T2				
	Lack of capacity planning – to cover peak loads		T1, T2				

7 Example SCADA Risk Treatment Plan (RTP)

Ref	Control Objectives	Selection of controls to achieve objectives (Control Reference)	Controlled Risk		Residual Risk
			Con-sequence	Likeli-hood	
A1 People Confidentiality	To ensure that people maintain the confidentiality of sensitive SCADA information	Confidentiality Agreements in employment contracts Include survivability clauses and obtain legal advice on drafting (ISO 27002 – Section 6.1.5 Confidentiality agreements).	Moderate	Unlikely	Medium
		Confidentiality Provisions in 3rd Party and outsourcing contracts Mandate security briefing for new providers who are working in critical areas to highlight obligations ISO 27002 – Section 6.2.3 Addressing security in third party agreements.			
		Position applicant references and referees are checked and reasonable care is taken to ensure the background of the applicant prior to employment. This includes a police background check to confirm suitability (ISO 27002 – Section 8.1.2) (ISM 0434) (PSPF Persec-01).			
		SCADA security training at induction and ongoing awareness training including security incident reporting. Incident reporting should define alert levels and timely reporting of critical incidents (ISO 27002 – Section 13 Information Security Incident Management, ISM – Information Security Awareness Training) (PSPF Gov-1).			
A2 People Integrity	To ensure that SCADA resources are appropriately trained, motivated and are trustworthy	Personnel vetting The Australian Government PSPF Personnel Security Protocol provides guidance on vetting (ISO 27002 – section 8 Human resources security).	Moderate	Unlikely	Medium
		Concise job descriptions in. (ISO 27002 – section 8 Human resources security).			
		On-going training and assessment in operating SCADA systems (ISO 27002 – 8.2.2 Information security awareness, education and training, ISM – Information Security Awareness and training).			
		Privileged accounts are not shared, uniquely identifiable for each user, approved only on a “need-to-have” basis, and used for administrative purposes only. A general user account is to be used for business as usual access. (ISM 0444).			
		Privileged accounts are audited in accordance with the security calendar to confirm access is required			

Ref	Control Objectives	Selection of controls to achieve objectives (Control Reference)	Controlled Risk		Residual Risk
			Con-sequence	Likeli-hood	
		and account use is within the information security policy requirements. (ISO 27002 Section 11.2 User access management).			
		Defined Entry and Exit procedures. Different levels of briefing/interviews depending on the job performed. Exit interviews are particularly important for staff & management in operational areas (ISO 27001 – 8.3 Termination or change of employment, ISM Personnel Security).			
A3 People Availability	To ensure that appropriate resources are available to manage and operate SCADA systems	Fully documented operating procedures. Operating procedures should be in place to supplement training and reduce the risk of accidents. Training environments should be established to support learning objectives (ISO 27001 10.1 Operational procedures and responsibilities, ISM System Security Plans, Standard Operating Procedures).	Moderate	Unlikely	Medium
		Implement a combination of resource types – including contractors, 3rd parties. Have a different type of resource to backup primary resourcing.			
		Implement cross-skilling for critical areas.			
B1 Management Control & Feedback Confidentiality	To control SCADA Management information	Develop Security Framework – set security direction, objectives, allocate roles and responsibilities, reporting requirements, steering committee to provide oversight of security (ISO27001 Section 4.2.1).	Minor	Unlikely	Low
		Establish a data classification schema - (ISO 27002 – 7.2 Information Classification, ISM – Media Security)			
		Develop and implement change and configuration management process ISO27001 12.5.1 change control procedures. - (ITIL – Change Management), NIST 800-128.			
		Formal procedures for publication of SCADA management information. Information is often incorrectly published to web sites when it should be for internal use only – often as a result of confusing internal “unclassified” documents with information intended for the general public -.(ISO 27001 Section 7.2 Information Classification).			
B2 Management Control & Feedback Integrity	To provide correct and controlled access to SCADA information	Controlled repository for SCADA related information. An information/knowledge management system may assist with achieving a controlled and secure storage - (ISO 27002 Section 10.1.1 Documented operating procedures).	Minor	Unlikely	Low
	To provide incident response and readiness	Formal Incident response and readiness procedures are developed and implemented - NIST SP800-61 Incident handling guide.			

Ref	Control Objectives	Selection of controls to achieve objectives (Control Reference)	Controlled Risk		Residual Risk
			Con-sequence	Likeli-hood	
	processes	Forensic readiness is the ability of an organisation to maximise its evidence collection capability whilst minimising the cost of doing so. (draft ISO 27037 identification, collection, acquisition and preservation of digital evidence) – (Aus Standards HB – 171 Management of IT Evidence)			
	To provide competent and effective management support	Documented Management Outcomes These should be endorsed with executive support (ISO 27002 Section 6 Organisation of Information Security)			
	To assess management effectiveness	Establish Key Performance Indicators for Management These should be reportable, repeatable and achievable (ISO 27001 Section Management review of the Information Management System ISMS) (ISO 27001 Section 0.2b)			
B3 Management Control & Feedback Availability	To ensure that required management controls are defined	Approved and documented Roles and Responsibilities for Management (ISO 27001 Management Responsibility) (ISM Roles and Responsibilities)	Moderate	Unlikely	Medium
		Approved Management Framework and Charter Quality Management procedures provide guidance on how a management framework should function (ISO 27001 Section 4.2 Establishing and managing ISMS)			
	To provide dedicated and effective Management support for SCADA systems	Documented SCADA management policies and procedures These document should be brief and not change significantly over time (ISO 27001 Section 4.3 Documentation Requirements) (ISM Information Security Documentation)			
C1 Building / Site Confidentiality	To prevent compromise of assets and interruption to business activities	Equipment site standards for remote devices Suitable racks/cabinets may be identified for remote servers/switches. Do not allow unprotected, live network access points (ISO 27002 Section 9 Physical and Environmental Security) (ISM Physical Security)	Minor	Unlikely	Low
C2 Building / Site Integrity	To minimise impact of Site loss and damage	Disaster Recovery and Business Continuity Plans These site specific strategies should be aligned with the whole of organisation DR strategy (ISO 27002 Sections 13 Security Incident Management, 14 Business Continuity Management) (ISM Incident Response and Emergency Procedures)	Minor	Unlikely	Low
C3 Building / Site Availability	To prevent loss of assets and interruption to SCADA operations	Defined security perimeters Restrict access to sites – do not allow broad access simply for convenience (ISO 27002 Section 9 Physical and Environmental Security) (ISM Physical Security)	Moderate	Unlikely	Medium

Ref	Control Objectives	Selection of controls to achieve objectives (Control Reference)	Controlled Risk		Residual Risk
			Con-sequence	Likeli-hood	
		Redundant power supply Consider Uninterruptible Power Supply (UPS) or alternate power supply for key sites. (ISO 27002 Section 9 Physical and Environmental Security)			
		Implementation of cabling standards All cabling should be bundled, labelled and use proper layout trays. (ISM Communications Infrastructure) (ISO 27002 Section 9.2.3 Cabling Security)			
D1 Information Management Confidentiality	To control access to SCADA information	Documented SCADA access control policy A high level access policy should be part of Information management controls communicated to management and users (ISO 27002 Section 11 Access Control) (ISM Access Control)	Moderate	Unlikely	Medium
		Formal user registration procedures in place Registration should exist for all user types: staff, contractors, and contracted service providers (ISO 27002 Section 11 Access Control) (ISM Access Control)			
		Regular audit review of access rights Ensure that all remote and “temporary” accounts are also reviewed (ISO 27002 Section 11 Access Control) (ISM Access Control)			
		Encrypt sensitive information stored on Networks Encryption of certain classifications should be part of an organisational information classification schema. (ISO 27002 – 12.3 Cryptographic Controls), (ISM – Cryptography) (NIST FIPS encryption standards)			
D2 Information Management Integrity	To ensure the correct operation of information processing facilities	Documented SCADA operating procedures To have full effect; operating procedures should be consistent, available, clear and changes must be efficiently applied according to proper versioning control.	Moderate	Unlikely	Medium
		Incident management and response procedures Should be documented and tested regularly - Available tools include Network and Host Intrusion Detection Systems, System Integrity Verification , Log Analysis and Intrusion Repulsion – (ISO 27002 Section 13 Information Security Incident Management, ISM – Section Managing Security Incidents)			
		Appropriate segregation of duties for information processing tasks (ISO 27002 Section 10 Communications and operations management)			
D3	To maintain the	Documented and tested backup procedures	Moderate	Unlikely	Medium

Ref	Control Objectives	Selection of controls to achieve objectives (Control Reference)	Controlled Risk		Residual Risk
			Con-sequence	Likeli-hood	
Information Management Availability	availability of information processing	Often only certain types of systems are backed up. Organisations should ensure that ALL critical information is backed up and that effectiveness is tested on a regular basis (ISO 27002 – 10.5 Backup)			
		Capacity monitoring and forecasting Network monitoring and service delivery reports from vendors may effectively provide these controls(ISO 27002 – 10.3.1 Capacity Management)			
		Change Management All SCADA systems, applications and communications infrastructure should be subject to formal change management control (ISO 27002 – Change Management Sections10.1.2, 12.5.1, 13.2) (ITIL Change Management)			
E1 Communications & Networks Confidentiality	To protect the transmission of SCADA information broadcast over Public Networks	Encrypt transmission of SCADA information Ensure that appropriate encryption protocols are applied – (ISM Cryptography, ISO 27001 – Section 12.3 Cryptographic controls, NIST FIP Encryption Standards)	Minor	Unlikely	Low
		Perform vulnerability assessments on a periodic basis on all access points into the SCADA network Regular scenarios should be defined and tested to identify network vulnerabilities (ISO 27002 – 12.6 Technical Vulnerability Management, (ISM – Vulnerability Management)			
E2 Communications & Networks Integrity	To verify SCADA network configurations	Deploy network monitoring services to identify and localise network trouble spots	Moderate	Unlikely	Medium
E3 Communications & Networks Availability	To maintain SCADA network connectivity	For key services, route communications lines via multiple exchanges / mediums	Moderate	Unlikely	Medium
		Deploy intelligent networking devices to handle peak loads Routing devices and modern switching equipment can be tailored to meet specific load patterns and provide alerts for unusual activity			
F1 SCADA Application Software Confidentiality	To ensure that such software utilises recognised best practice security mechanisms and is able to withstand	Secure SCADA software configuration Where possible, computerised systems should be hardened to minimise the opportunity for unauthorised access. Hardening should also ensure that any vendor application software support is maintained throughout the life of the product whilst the underlying system is hardened. Access control mechanisms should also exist to ensure that centralised system access controls are	Moderate	Unlikely	Medium

Ref	Control Objectives	Selection of controls to achieve objectives (Control Reference)	Controlled Risk		Residual Risk
			Con-sequence	Likeli-hood	
	unauthorised access attempts.	protected in accordance with corporate password and account usage policies.			
		Minimisation of user access rights Users should only be granted the minimum access required in order to perform their duties. Such access, and the functionality assigned to SCADA system roles, should also be regularly reviewed and updated. (ISO 27002 Section Access Control)			
		Logging of access attempts and user actions - All access attempts, whether they are successful or not, should be logged to a protected audit trail. The audit trail should be regularly backed up and kept as long term evidence (12mths) to prevent erasure or tampering of evidence. In addition, significant activities (such as the changing of state of SCADA devices and updates to access lists) should also be logged. (ISO 27002 Section 10.10 Monitoring) The audit trail should be periodically reviewed for suspicious activity. It is desirable that suspicious activity be alerted to operational personnel in near real-time.			
F2 SCADA Application Software Integrity	To maintain the correct operation of the software over time.	Implement patch management process – (DSD 35 Mitigations, ISO 27001 – Section 12.6 Technical vulnerability management, ISM - Vulnerability Management)	Major	Unlikely	Medium
		Vendor support arrangements Contractual arrangements should be in place with the software vendor to ensure that: Software patches are made available in a timely manner Support arrangements such as subcontracting and off-shoring do not occur without the agreement of all contracted parties The customer is to be notified of any takeover or merger activities that may affect the level or manner in which the vendor support arrangements are provided (ISO 27002 Section 6.2 External Parties)			
		Critical software escrow arrangements Where a SCADA system comprises a vendor-specific software package, an escrow agreement should be entered into with the vendor to ensure product availability should the vendor organisation fail to be able to support the product into the future. (ISO 27002 Section 10.8.2 Exchange agreements)			
F3 SCADA Application Software		Capacity planning SCADA systems should be designed to provide scalability for future growth and information storage requirements. Collection and retention of audit trails should also be addressed. (ISO 27002 Section 10.3.1 Capacity Management)	Major	Unlikely	Medium

Ref	Control Objectives	Selection of controls to achieve objectives (Control Reference)	Controlled Risk		Residual Risk
			Con-sequence	Likeli-hood	
Availability		Capacity monitoring SCADA functionality should include a function to allow for potential bottlenecks such as CPU, memory, disk and communications usage to be monitored and analysed. (ISO 27002 Section 10.3.1 Capacity Management)			
		Acceptance testing Acceptance testing procedures and criteria should be developed for all changes to SCADA software. These procedures should encompass software updates, bug fixes and security patches. In cases where emergency security patching is required, Business Continuity Plans should allow for the implementation of such patches and the recovery from failed operational implementations. (ISO 27002 Section 10.3.2 System Acceptance)			
		Use of open architectures and protocols Where possible, open architectures and protocols should be adopted to prevent vendor-specific architectures and protocols from potentially 'hiding' security issues and constraining system scalability and interoperability.			
G1 SCADA Hardware including operating System Confidentiality	To ensure that the SCADA computing platform is resilient against unauthorised access attempts.	Security hardening of the computing platform Computer platforms should be hardened to remove unnecessary services, accounts and software packages. Vendor support agreements should allow for basic hardening of supported computer platforms. (ISM - Software Security Standard Operating Environments) (ISO 27002 Section 12 Information systems acquisition, development and maintenance) (DHS Procurement Guidelines)	Moderate	Unlikely	Medium
		Operating System access controls OS access controls should be implemented to ensure that sensitive information is protected from unnecessary and unauthorised disclosure Unnecessary user accounts should also be removed and default account passwords changed. (ISO 27002 Section 11 Access control)			
		Vendor support arrangements Vendor support arrangements should ensure that system hardening measures do not void support arrangements and that measures such as timely security patching of systems are supported.			
G2 SCADA	To ensure that the configuration of the	Formal configuration management and control procedures There should be measures in place to ensure that the SCADA system is in a known and approved	Moderate	Unlikely	Medium

Ref	Control Objectives	Selection of controls to achieve objectives (Control Reference)	Controlled Risk		Residual Risk
			Con-sequence	Likeli-hood	
Hardware including operating System Integrity	SCADA computing platform is in a known and approved state.	state, and that changes are appropriately analysed, tested and authorised.			
		Vendor support arrangements Contractual support arrangements should be in place with the SCADA software vendor to ensure that timely installation of security patches to supported hardware and OS is possible.			
G3 SCADA Hardware including operating System Availability	To ensure that the SCADA computing platform is reliable in the event of component failure, environmental disturbance, or attempted malicious disruption.	System redundancy Critical system components should be designed to withstand single points of failure. Business Continuity Plans (and/or if necessary, Disaster Recovery Plans) should be updated and tested to ensure that systems are able to withstand loss of single physical, personnel and procedural dependencies.	Moderate	Possible	High
		Spares holdings Adequate spares should be held (or covered by vendor support arrangements) for timely recovery from component failures.			
		Protection against malware Antivirus measures should be implemented on SCADA networks as they would with other corporate IT environments. Malware protection should be applied and updated in a timely manner on SCADA server, FEP, field device and workstation platforms. NOTE: it is becoming increasingly common to find field devices operating via well-known operating systems. Any virus attack on the system can therefore also have major repercussions on field devices and they should therefore be brought into the corporate AV regime. ISO 27002 – Section 10.4 Protection against malicious and mobile code			
		Capacity planning and monitoring Measures should be in place to monitor and manage SCADA system capacity and address potential bottlenecks in advance of them impacting on system operations. – (ISO 27002 – Section 10.3.1 Capacity Management)			
		Business Continuity Plans BCPs and associated DRPs should be in place and tested to ensure that the SCADA system can cope with the loss of components (and potentially sites) and that the system can be restored to normal operations as faults are rectified. – (ISO 27002 – Section 14 Business Continuity, HB 292 – A			

Ref	Control Objectives	Selection of controls to achieve objectives (Control Reference)	Controlled Risk		Residual Risk
			Con-sequence	Likeli-hood	
		Practitioners Guide to Business Continuity Management, ISM Business Continuity and Disaster Recovery)			
H1 SCADA Field Devices Confidentiality	To prevent unauthorised monitoring and control of these devices.	Encrypted data communications Where communications with field devices occurs over a communications line susceptible to external interception and / or compromise, information should be encrypted to minimise the opportunity for external parties to compromise the communications channel. – (ISO 27002 – Section 12.3 Cryptographic Controls, ISM – Section Cryptography, NIST FIPS encryption standards)	Moderate	Unlikely	Medium
		Deactivation of default configuration accounts – where technically feasible default configuration accounts should be deactivated			
		Private communications channels Where possible, sensitive communications with field devices should be performed over dedicated leased-line services rather than using a public communications infrastructure.			
H2 SCADA Field Devices Integrity	To ensure that these devices are in a stable and known state	Periodic device polling Field devices should be periodically polled to ensure that their status is verified to the central control system and, if necessary, that discrepancies are investigated and verified.	Minor	Unlikely	Low
H3 SCADA Field Devices Availability	To ensure that these devices can be monitored and controlled as required.	Device maintenance A maintenance regime should be in place to ensure that all peripheral devices are regularly tested	Moderate	Unlikely	Medium
		Alternate communications channels Critical field establishments and devices should be connected to the SCADA system via redundant communications channels. The central control station should also be configured such that it has control over the communications channel(s) available to the field device. – (ISO 27002 – 9.2.2 Supporting utilities)			
I1 Supporting Utilities Confidentiality	To ensure that power failures do not lead to a security compromise of the SCADA system.	Backup power source Critical system components should be fed through both mains and backup power supplies. (ISO 27002 – 9.2.2 Supporting utilities)	Minor	Rare	Low
I2 Supporting	To ensure that SCADA systems operate as	Backup power source A medium-to-long term power supply alternative (such as a long term diesel power unit) should be	Moderate	Unlikely	Medium

Ref	Control Objectives	Selection of controls to achieve objectives (Control Reference)	Controlled Risk		Residual Risk
			Con-sequence	Likeli-hood	
Utilities Integrity	expected during power supply disruptions.	available to power critical SCADA system components during power interruptions. Should core SCADA components be installed in dedicated control environments, power supply should also be capable of powering support environments such as air conditioning and fire detection. (ISO 27002 – 9.2.2 Supporting utilities)			
		Power conditioning System-critical devices should be connected to a conditioned and uninterruptible power supply.(ISO 27002 – 9.2.2 Supporting utilities)			
I3 Supporting Utilities Availability	To prevent disruption to SCADA operations during power failure conditions.	Backup power source Critical system components should be fed through both mains and backup power supplies.(ISO 27002 – 9.2.2 Supporting utilities)	Major	Unlikely	Medium
		Redundant control centres There should be redundancy built into centralised control sites to mitigate against damage to, or loss of availability of, critical establishments.(ISO 27001 – Section 14 Business Continuity)			
		Contingency planning Contingency plans should ensure that centralised services can be transitioned to alternative arrangements during such interruptions and be able to be transitioned back into service once central sites are restored to normal operations. (ISO 27001 – Section 14 Business Continuity)			
		Disaster recovery testing Contingency plans should be tested periodically. Where a physical failover test is not able to be performed, formal scenario testing should be undertaken, with results and lessons learned documented, analysed and actioned as appropriate. (ISO 27001 – Section 14 Business Continuity)			

8 Presentation of Results to Senior Management

8.1 Overview

8.1.1 Whilst the detailed analysis and documentation contained within an organisation's full SCADA risk management plan is likely to form a significant report, it is suggested that measures be undertaken to summarise the plan for presentation to senior management.

8.1.2 Whilst detailed documentation is available to senior management personnel, a summarised report is more often an effective format to communicate the results to such an audience.

8.1.3 A number of organisations already use a 'traffic light' approach to present such data to senior management, where each risk is assigned a green, amber or red status depending on the current health of risk management measures.

8.1.4 The following subsection presents the use of a 'radar chart' to display risk management status to an organisation's senior management. It can be a highly effective mechanism in cases where identified SCADA process enablers are not overly complex and it has a number of advantages as follows:

- The entire risk management story is presented via a single graphic diagram
- It is easy to explain and intuitive to understand
- It can be used to show risk management progress over time by including historical data to demonstrate the organisation's risk profile over time.

8.1.4.1 The radar chart is a standard Microsoft charting option. Applications such as PowerPoint or Visio can be used to create the background colour scheme onto which the chart can be overlayed for presentation purposes.

8.2 Sample Radar Chart

8.2.1 Figure 8-1 provides a sample radar chart based on the enablers identified in this report and arbitrary treated risk exposure data.

8.2.2 It shows on the one diagram:

- The health of risk management against each of the identified enablers; and
- The current (May 11) risk management profile in comparison to the profile 12 months previous (May 10).

8.3 Sample Executive Summary Risk Status Table

8.3.1 Table 8-1 provides a sample executive risk status obtained by taking the highest likelihood and consequence from each enabler as a high level overview

- It should be noted that the colour in the current columns refer to the current level of risk described in section 3.10.2 Conventions – Risk Assessment
- The colour in the controlled columns refers to the effective implementation of controls documented – see section 3.10.3 Conventions – Risk Treatment Plan.

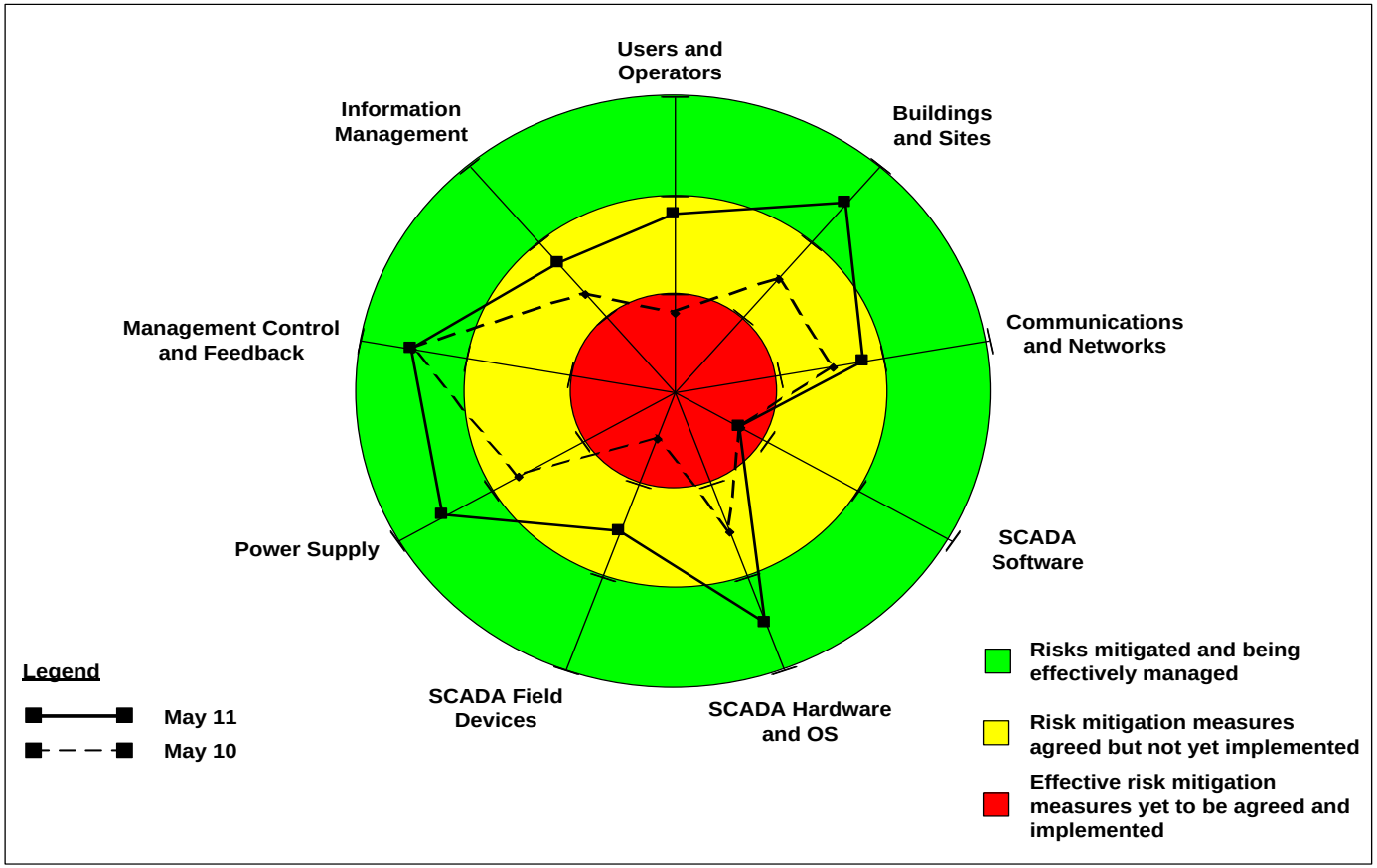

Figure 8-1 Sample Radar Chart Presentation of Risk Management

Asset	Current Risk				Controlled Risk		
	Consequence	Likelihood	Risk Rating	Treatment Option	Consequence	Likelihood	Risk Rating
Pe.1 - People	Moderate	Almost Certain	High	Reduce A1-3	Moderate	Unlikely	Medium
Pr.1 - Management Control & Feedback	Catastrophic	Likely	Extreme	Reduce B1-3	Moderate	Unlikely	Medium
P.1 - Building Site	Moderate	Possible	Medium	Reduce C1-3	Moderate	Unlikely	Medium
Pr.2 - Information Management	Moderate	Almost Certain	High	Reduce D1-3	Moderate	Unlikely	Medium
P.2 - Communication & Networks	Moderate	Almost Certain	Very High	Reduce E1-3	Moderate	Unlikely	Medium
P.3 - SCADA Application Software	Major	Likely	High	Reduce F1-3	Major	Unlikely	Medium
P.4 - SCADA Hardware including Operating System	Moderate	Almost Certain	High	Reduce G1-3	Moderate	Possible	High
P.5 - SCADA Field Devices	Moderate	Likely	High	Reduce H1-3	Moderate	Unlikely	Medium
P.6 - Supporting Utilities	Major	Likely	High	Reduce I1-3	Major	Unlikely	Medium

Table 8-1 Executive Summary Risk Status Table

9 Ongoing Monitoring and Review

9.1 Overview

9.1.1 The effectiveness of a risk management approach is dependent not only on the methodology applied to the development of risk assessment data, but also on its continued update as influencing factors change over time.

9.1.2 Examples of such factors can include:

- Changes to business processes and / or technologies within the organisation
- Alteration to the external threat environment (e.g. the organisation may decide to undertake a project that brings it into conflict with an issue-motivated group).

9.1.3 In addition, the risk management framework itself needs to be monitored, measured and refined to ensure that it continues to provide relevant information to the organisation.

9.1.4 The subsections to follow indicate measures that are likely to contribute to the ongoing effectiveness of the SCADA Risk Management Framework.

9.2 SRMF Reviews

9.2.1 The overall SCADA Security Risk Management Framework should be reviewed over time to ensure that it functions effectively. Measures that can be undertaken to assist in this activity include, but are not necessarily limited to, the following:

- Internal process reviews
- External (independent) process reviews and audits
- Implementation of Key Performance Indicators (KPIs) designed to monitor SRMF processes.

9.2.2 Where possible, it is recommended that KPIs be chosen, and limited in number, to an easily measurable set to minimise the impact of process monitoring on normal day-to-day activities.

9.3 Communicating Risk Exposures

9.3.1 Having measured corporate risk exposures associated with the operation of the SCADA system(s), Section 8 of this document provides a suggested management reporting tool.

9.3.2 Where the organisation implements risk management at an organisation-wide level (e.g. a risk and audit committee reporting directly to their Board or senior Executives), SCADA risk exposures should also be formally reported to this risk management group to allow SCADA risk exposures to be assessed and managed at the corporate level.

9.4 Risk Assessment Updates

9.4.1 As noted, both the internal and external threat environment is likely to change over time.

9.4.2 To maintain the currency of RMF deliverable(s), a program should be put into place to:

- Trigger a refresh at defined intervals (e.g. annually).
- Allow the risk environment to be re-evaluated in response to defining changes (e.g. the introduction of new technologies or the emergence of a significant external threat source).