Office of the Auditor General
Serving the Public Interest

Report 24: 2022-23 | 14 June 2023

BETTER PRACTICE GUIDE

Security Basics for Protecting Critical Infrastructure from Cyber Threats

Office of the Auditor General
Western Australia

Audit team:
Aloha Morrissey
Kamran Aslam
Fareed Bakhsh

National Relay Service TTY: 133 677
(to assist people with hearing and voice impairment)

We can deliver this report in an alternative format for
those with visual impairment.

ISSN: 2200-1913 (print)
ISSN: 2200-1921 (online)

The Office of the Auditor General acknowledges the traditional custodians throughout Western Australia and their continuing connection to the land, waters and community. We pay our respects to all members of the Aboriginal communities and their cultures, and to Elders both past and present.

Image credit: Panimoni/shutterstock.com

WESTERN AUSTRALIAN AUDITOR GENERAL’S REPORT

Security Basics for Protecting Critical Infrastructure from Cyber Threats

Report 24: 2022-23
14 June 2023

This page is intentionally left blank

THE PRESIDENT
LEGISLATIVE COUNCIL

THE SPEAKER
LEGISLATIVE ASSEMBLY

SECURITY BASICS FOR PROTECTING CRITICAL INFRASTRUCTURE FROM CYBER THREATS

This report has been prepared for submission to Parliament under the provisions of section 23(2) and 24(1) of the *Auditor General Act 2006*.

This better practice guide aims to help Western Australian public sector entities better manage cyber security threats to their critical infrastructure. The guide focuses on better practice principles to safeguard critical operational technology and has been informed by this Office's recent audit work on this topic.

CAROLINE SPENCER
AUDITOR GENERAL
14 June 2023

Contents

Auditor General's overview

Cyber security is a critical concern across all industries as threats continue to evolve and pose significant threats. Australian organisations have seen an increase in successful cyber attacks in recent years. Of increasing concern, cyber criminals and nation states are also targeting critical infrastructure including power grids, water delivery systems, transport networks and communication systems.

These attacks pose a significant risk to our national security where consequences can impact health and safety, essential services and result in severe economic damage. As threats continue to grow in sophistication, effective strategies with multiple layers of defence over cyber and information security, supply chain, physical security and operational technology is required.

In response to growing cyber threats, governments worldwide are taking steps to improve cyber security measures and resilience of critical infrastructure. The Australian Government's amendments to the *Security of Critical Infrastructure Act 2018* is one such example.

Connectivity between IT and OT continues to blur network boundaries, it is therefore important to keep an eye on risks and defend against threats. Entities should remain vigilant, adapt to changing threat landscapes and collaborate to protect critical infrastructure. Security of critical infrastructure has been a key focus for my Office, and based on recent audit work in this area, this better practice guide aims to help entities manage cyber threats to their critical systems and infrastructure. Other public sector entities are also encouraged to use this guide to enhance their cyber resilience.

Part 1: Introduction

1.1 About this guide

This better practice guide aims to help Western Australian (WA) public sector entities better manage cyber security threats to their critical infrastructure[1]. The guide focuses on better practice principles to safeguard critical operational technology (OT) and has been informed by this Office's recent audit work on this topic.

This is not intended to be an exhaustive document. Further guidance is available from the Cyber and Infrastructure Security Centre[2] and relevant standards. Some security standards are referred to in the Security of Critical Infrastructure Rules[3] and include the:

- Australian Standard for Information Security AS ISO/IEC 27001:2015
- Essential Eight[4] controls developed by the Australian Signals Directorate
- National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity
- Cybersecurity Capability Maturity Model by the Department of Energy of the United States of America
- 2020-21 AESCSF Framework Core by the Australian Energy Market Operator.

1.2 Who should use this guide

Entities who operate critical infrastructure, including those in the energy, water, transport, health sectors, and those responsible for maintaining critical communication infrastructure are encouraged to engage with the principles and practices in this guide. Other public sector entities are also encouraged to apply the principles as required to ensure the continuity and reliability of essential services.

1.3 Background

Every day, millions of Western Australians rely on critical infrastructure to access a range of essential services including public transport, clinical health services and the provision of water, gas and power to their homes and businesses.

Delivery of these services has increasingly moved away from historical manual processes towards reliance on information technology (IT) and OT systems working together (Figure 1). The benefits and efficiencies that arise from the use of IT and OT are numerous. They include the ability to remotely access and operate control systems used to deliver government services. For example, whenever we turn on a tap or a light, we access a

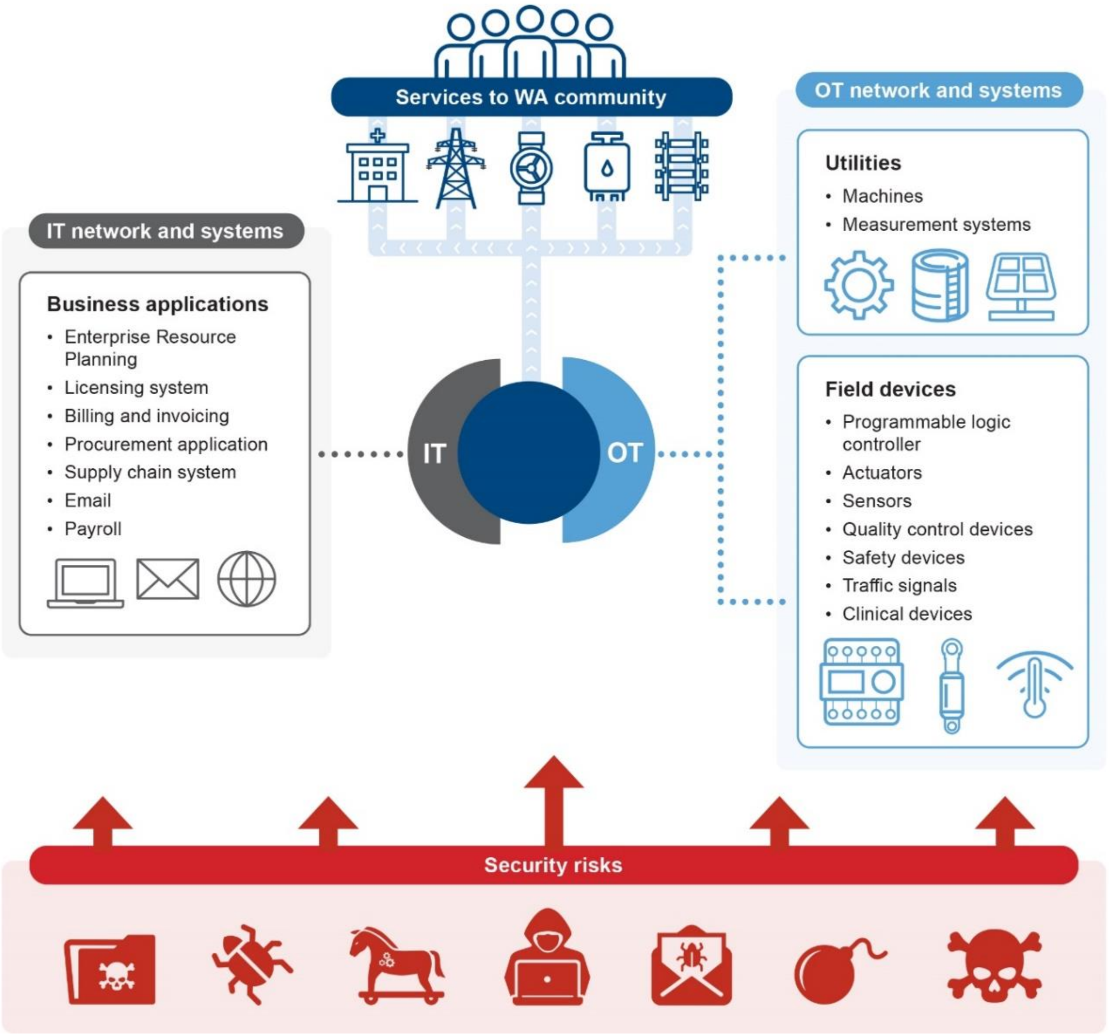
[1] Critical infrastructure is defined by the Cyber and Infrastructure Security Centre as those physical facilities, supply chains, information technologies and communication networks, which if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation, or affect Australia's ability to conduct national defence and ensure national security.

[2] Australian Government Department of Home Affairs, 'Critical Infrastructure Resilience Strategy', *Cyber and Infrastructure Security Centre,* 23 February 2023, accessed 8 June 2023.

[3] Australian Government, 'Security of Critical Infrastructure (Critical infrastructure risk management program) Rules', Federal Register of Legislation, 16 February 2023, accessed 8 June 2023.

[4] Australian Government Australian Signals Directorate, 'Essential Eight Maturity Model', *Australian Cyber Security Centre*, 24 November 2022, accessed 8 June 2023. These controls are mandated for WA State government entities by the *WA Government Cyber Security Policy*. Although not mandatory for all government trading entities, the Essential Eight represent minimum controls for cyber security and should be considered.

complicated system underpinned by OT that includes industrial control systems, and supervisory control and data acquisition (SCADA[5]) systems.



Source: OAG

Figure 1: High level view of IT and OT convergence and risks

The interconnection of IT and OT exposes the control systems and the essential services they deliver to increased cyber risks. OT infrastructure is particularly targeted and protecting it presents unique challenges. OT software generally requires support from specialist suppliers, is often not secure by design and many traditional security controls cannot be applied to them. Unique and industry specific protocols (Appendix 1) drive OT networks, although common IT communication protocols are also used.

Inadequate security of OT systems can cause physical harm to people and damage to equipment that can lead to significant disruption and financial loss. For example, a cyber attack on a power grid could result in a widespread blackout, or a compromised industrial control system could cause a chemical plant to release hazardous substances. In comparison, a compromise of an IT business application could result in exposure of sensitive information or loss of information for decision making. Further examples of compromised IT and OT systems are listed below in Table 1.

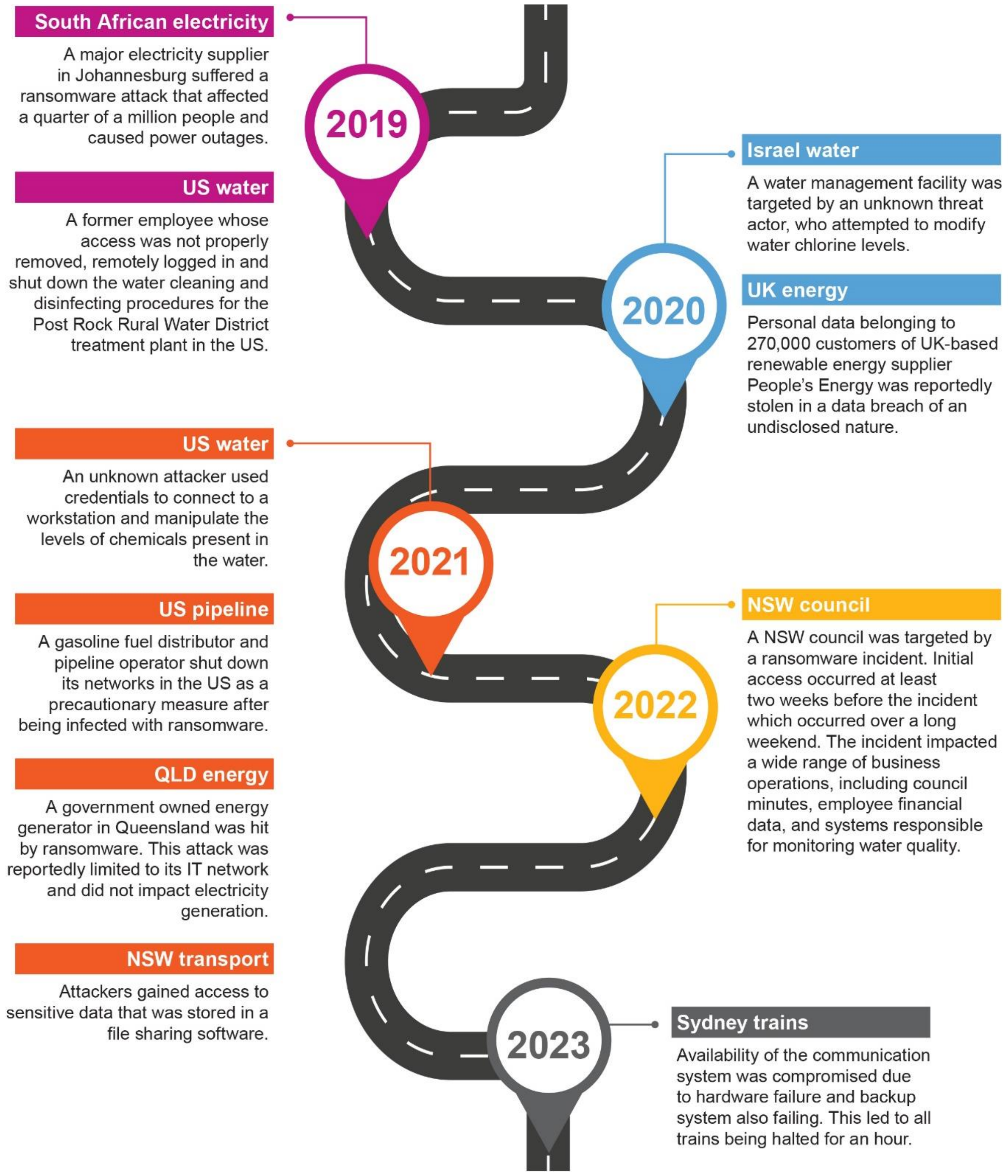
[5] SCADA collectively refers to software and hardware (sensors, controllers, machines and computers) working together to deliver essential services.

Impact in OT environment	Impact in IT environment
Rail and road traffic signals may be compromised and result in crashes	A website which provides road congestion information may become unavailable
Power and water services to the public may not be delivered	Systems may not be available to establish new customer accounts, or prepare and process customer invoices
Loss of clinical health systems that support human life	Unavailability, theft or disclosure of private medical records
Systems that regulate the quantity of chemicals used to treat water may be disrupted	Systems may not generate and issue water bills to customers
Surgical systems and screens may not work during surgery	A medical appointment booking website may not be accessible

Source: OAG

Table 1: Examples of potential impacts of cyber incidents in IT and OT environments

Figure 2 provides examples of global incidents in the utilities sector from the last five years, highlighting the need for effective strategies to deter threats to critical infrastructure. Strategies should cover, but are not limited to, risk management, OT, people, supply chains, cyber and information security, and physical infrastructure.



2019

South African electricity

A major electricity supplier in Johannesburg suffered a ransomware attack that affected a quarter of a million people and caused power outages.

US water

A former employee whose access was not properly removed, remotely logged in and shut down the water cleaning and disinfecting procedures for the Post Rock Rural Water District treatment plant in the US.

2020

Israel water

A water management facility was targeted by an unknown threat actor, who attempted to modify water chlorine levels.

UK energy

Personal data belonging to 270,000 customers of UK-based renewable energy supplier People's Energy was reportedly stolen in a data breach of an undisclosed nature.

2021

US water

An unknown attacker used credentials to connect to a workstation and manipulate the levels of chemicals present in the water.

US pipeline

A gasoline fuel distributor and pipeline operator shut down its networks in the US as a precautionary measure after being infected with ransomware.

QLD energy

A government owned energy generator in Queensland was hit by ransomware. This attack was reportedly limited to its IT network and did not impact electricity generation.

NSW transport

Attackers gained access to sensitive data that was stored in a file sharing software.

2022

NSW council

A NSW council was targeted by a ransomware incident. Initial access occurred at least two weeks before the incident which occurred over a long weekend. The incident impacted a wide range of business operations, including council minutes, employee financial data, and systems responsible for monitoring water quality.

2023

Sydney trains

Availability of the communication system was compromised due to hardware failure and backup system also failing. This led to all trains being halted for an hour.

Source: OAG based on publicly available information

Figure 2: Examples of critical infrastructure security breaches

In response to growing cyber threats to critical infrastructure, the Australian Government amended the *Security of Critical Infrastructure Act 2018* (SOCI) to strengthen the security posture of critical infrastructure entities. Changes to the SOCI took effect in early 2022 and include:

- increased coverage of sectors (water, gas, power, health and many others)
- mandating entities to report cyber incidents
- obligations on entities to maintain their risk management program for cyber, people, supply chain and physical security
- entities including WA public sector are obliged to report critical asset information to the Cyber and Infrastructure Security Centre.

Part 2: How to protect critical infrastructure from threats

Entities require effective risk management policies, procedures and governance to mitigate threats to their critical infrastructure. This guide is not exhaustive and highlights areas that require attention including asset management, insider threats, supply chain, and cyber and physical security risks.

2.1 Identify and maintain an accurate inventory of important IT and OT assets

Identification and management of critical assets helps protect them against cyber and physical threats. Security of OT assets requires a different approach to IT assets.

Identify critical assets

Identify assets critical to the delivery of services. This includes sites, buildings and technology such as sensors, actuators, programmable logical controllers, servers, engineering workstations and applications.

Identify and manage asset risks

Understand the purpose of assets and relevant risks. Treat these risks with a view to minimise them as much as possible.

Get to know critical assets

Document critical asset details including their location, importance, software and firmware information and supporting vendor, where applicable. Access to this information should be granted on a need-to-know basis.

Maintain an inventory

Keep the register of critical assets current. Update it when changes are made or assets are disposed. Periodically confirm the register's accuracy.

Securely dispose assets when they are no longer required or reach their end-of-life. Any information including configurations should be erased prior to disposal.

Source: OAG

Figure 3: Better practice areas for asset management

2.2 Develop a culture of security

Supporting staff through training and appropriate policies is paramount to building secure operations and a security culture. Without this, staff may not know what good security behaviours look like or how to practice them. Security programs should be tailored to roles to help develop staff understanding of risks.

Develop specific training

Develop specific and regular training for staff and contractors with access to critical sites and systems. General cyber security training usually focuses on IT security, this is not sufficient.

Maintain relevant policies

Keep workforce development and security policies and processes updated following incidents or changes in environments (e.g. regulatory, organisational, or technology). Promptly communicate updates to all staff and contractors.

Perform adequate background checks

Vet all staff and contractors before granting access to critical systems and sites.

Based on positions, background checks should go beyond basic national police clearances and include checks that cover national security[6] to minimise the risk of foreign interference and espionage. Include similar requirements in contracts with third party suppliers and check they comply.

Manage health and safety risks

Develop policies and procedures to provide a safe work environment for staff at critical sites.

Ongoing assessments are crucial to identify potential dangers that may result in injury.

Source: OAG

Figure 4: Better practice areas for security culture

[6] Australian Government Department of Home Affairs, 'AusCheck background checking under the Security of Critical Infrastructure Act 2018', *Cyber and Infrastructure Security Centre*, 11 April 2023, accessed 8 June 2023.

2.3 Manage supply chain risks

Entities increasingly rely on third party suppliers to maintain their IT and OT infrastructure. It is therefore important to understand and protect against supplier risks. For example, a supply chain compromise could provide cyber criminals with an opportunity to insert malicious code in OT devices prior to delivery to entities, or while servicing or maintaining them.

Assess suppliers before onboarding

Third party risk assessments help identify weaknesses that may be detrimental to the delivery of important services.

Document all suppliers and identify those who have access to critical assets and those supplying OT devices.

Document security requirements in contracts

Contracts with suppliers should include security requirements based on industry better practices.

Develop processes to ensure suppliers comply with their obligations.

Regularly gain assurance

Based on supplier risk and the importance of their service, perform regular reviews or gain cyber security control assurance through independent reports.

Entities should develop a program to test OT devices before deploying them and follow up with suppliers to fix identified issues.

Secure information exchange

Avoid direct connection to external supplier networks for information exchange or maintenance of critical systems, as this can introduce unnecessary vulnerabilities.

Source: OAG

Figure 5: Better practice areas for supply chain risks

2.4 Design a resilient network

Business functions often require access to the OT network or data to monitor and analyse. Careful consideration must be given to the network design needed to support business functions securely and the ongoing maintenance of network and associated devices throughout their life.

Separate IT and OT networks

Segment IT and OT into different networks and create a demilitarized zone[7] between them. Further segment the OT network by grouping devices based on their function and risk. Refer to the Purdue[8] model at Appendix 2 and tailor a solution that best fits needs.

Implement barriers between various OT segments to enhance resilience.

Prevent direct access to OT networks and field devices

Do not allow direct access into the OT network from IT network or remote internet access.

Use jump hosts[9] to access OT networks and devices and implement a security baseline for devices that connect to the network.

Exceptions must be risk assessed and continuously monitored.

Periodically review configurations

Regularly review the configuration of security appliances that protect and segregate the network.

Secure and protect administration interfaces and ports against common attacks.

Maintain backups

Where possible, implement high availability or have offline hardware on standby to continue operations in the event of an incident.

Keep offline and secure backups of configurations, builds, operational data and manuals to use during an incident.

Source: OAG

Figure 6: Better practice areas for network security

[7] A demilitarized zone (DMZ) prevents direct access to OT assets and acts as a layer of protection.

[8] An architecture model developed at Purdue University to manage business and industrial control networks. The model has been further expanded by various organisations to suit their needs.

[9] A jump host is an intermediary computer used for access between two network zones.

2.5 Implement effective access management procedures

Effective access management is essential to securing IT and OT environments against cyber threats. All users and devices should be identified, authenticated and authorised before being granted access to systems and information. Unauthorised users and devices should be prevented at all levels in the network.

Separate access management systems

Separate IT and OT access control systems (e.g. domain controllers) and do not create trusts between the IT and OT access systems.

If systems have built-in remote maintenance capability, disable or closely monitor it.

Use multi-factor authentication (MFA)

Make MFA mandatory for access to jump hosts, critical systems, security appliances and networks.

Govern and review privileged access

Accounts should be granted access using the principle of least privilege. Only assign super privileges where a role requires it.

Where appropriate, use just-in-time[10] access to avoid ongoing privileged access. Monitor the use of privileged activity such as provisioning of new access or changes to OT configurations.

Implement a lifecycle approach to manage access accounts

Ensure all accounts (e.g. staff, contractors and service providers) are assessed before granting access to critical systems, and promptly terminate when not needed.

Keep access levels in line with role responsibilities.

Source: OAG

Figure 7: Better practice areas for access management

[10] Just-in-time access provides privileges for a predetermined time on a needs basis to troubleshoot, upgrade or patch applications and systems.

2.6 Manage vulnerabilities and maintain vigilance

IT and OT applications, operating system software and firmware may have weaknesses that could be exploited. Processes to harden and patch these vulnerabilities will minimise the risk of exploitation.

Monitoring to detect attempted or successful security breaches is equally important. However, collecting logs is not enough. Entities should use appropriate tools to analyse logs for malicious activity. Detecting a compromise can be difficult and requires ongoing tweaks and continuous vigilance. Entities should consider emerging technologies including artificial intelligence to further support their security monitoring processes.

Understand technical vulnerabilities

Proactive vulnerability scanning in OT networks is often difficult, however this does not mean it should not be done.

Passive scanning techniques, such as creating an offline image, can identify vulnerabilities for rectification in production environments. Risk and change management processes should be followed when patching vulnerabilities.

Monitor networks and systems

Conduct assessments to identify critical logs that must be captured for IT and OT. As a minimum, industry best practice and vendor recommended logs should be captured for internet traffic, host activity, access into OT networks and phishing attempts.

Additionally, include network traffic from low level field devices such as programmable logic controllers and remote terminal units for threat monitoring.

Use logs to create alerts based on scenarios that an adversary might use to compromise systems.

Maintain situational awareness

Subscribe to and read alerts issued by the Australian Cyber Security Centre, which highlight cyber attacks on Australian and global critical infrastructure. These alerts often include techniques used by cyber criminals and indicators of compromise, which entities can use to review their own networks for potential malicious activity.

Prevent untrusted code and removeable media

Prevent execution of unapproved software, scripts, macros and other executables. Additionally, do not allow removeable media to be used on OT workstations and servers.

Where appropriate, implement application controls in IT and OT environments in line with the *Essential Eight* mitigation strategies.

Source: OAG

Figure 8: Better practice areas for vulnerability management

2.7 Implement physical security

Protecting physical sites and assets from threats is essential to entities' overall cyber security posture.

Establish perimeter protections

Limit entry points and deploy physical barriers around critical facilities such as purpose-built fences, walls and gates in metropolitan and regional locations. In addition, where appropriate, implement:

- video surveillance
- intrusion detection systems
- security guards.

Develop visitor management procedures

Effective visitor management procedures should include identification and registration. Supervised visits should be provided where access to OT and important systems is required.

Implement physical access controls

Restrict entry to sensitive areas where OT systems are located through access cards, biometric authentication or physical locks.

Do not use the same key for outer gates and rooms where OT devices are hosted. Ensure limited personal have access to master keys.

Perform ongoing site assessments

Perform ongoing security assessments on critical sites to identify deteriorations to layout, access systems, fences, lighting, alarms, signs and physical security screens.

Secure equipment during transportation

Develop procedures to minimise the risk of loss of critical assets or tampering of configuration and hardware during transportation between sites. Tamper evident seals, secure containers or trusted transportation services should be considered.

Source: OAG

Figure 9: Better practice areas for physical security

2.8 Be prepared for when things go wrong

Cyber attacks can disrupt critical systems and essential services. Entities should be prepared to manage incidents to minimise their adverse impact.

Develop achievable recovery plans

Entities should use business impact analysis to develop resilience plans. This ensures recovery objectives (RPO[11] and RTO[12]) are achievable and aligned with business objectives.

Develop OT specific playbooks

Often cyber security incident response plans are IT specific and overlook OT.

Many OT breaches originate from a compromised IT network so it is essential that OT specific playbooks are developed and tested for effective recovery.

Align resilience plans

Resilience plans and their recovery objectives should align, and dependencies should be considered and clearly noted. Dependencies may exist between processes, IT and OT networks, business units or external factors, such as service providers and supply chain networks.

Communicate with stakeholders

Plans should include processes to communicate with internal and external stakeholders affected by a breach. An effective communication plan will help to manage expectations and avoid panic.

For example, entities need to report[13] certain breaches, as required by the SOCI.

Source: OAG

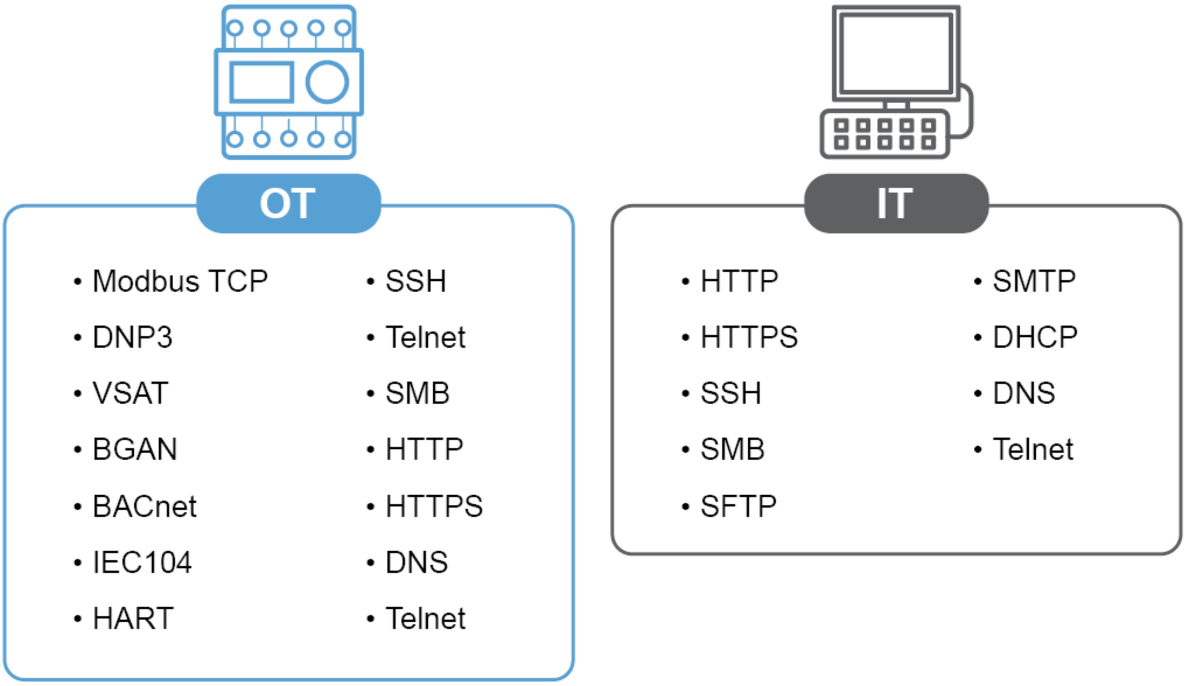
Figure 10: Better practice areas for continuity management

[11] RPO (Recovery Point Object) is the amount of data that will be lost or will need re-entering because of an incident.

[12] RTO (Recovery Time Object) is the amount of time that can pass before the disruption begins to seriously and unacceptably impede the delivery of critical services.

[13] Australian Government Department of Home Affairs, Cyber Security Incident Reporting, *Cyber and Infrastructure Security Centre,* 23 February 2023, accessed 8 June 2023.

Appendix 1: Examples of common OT and IT communication protocols



OT

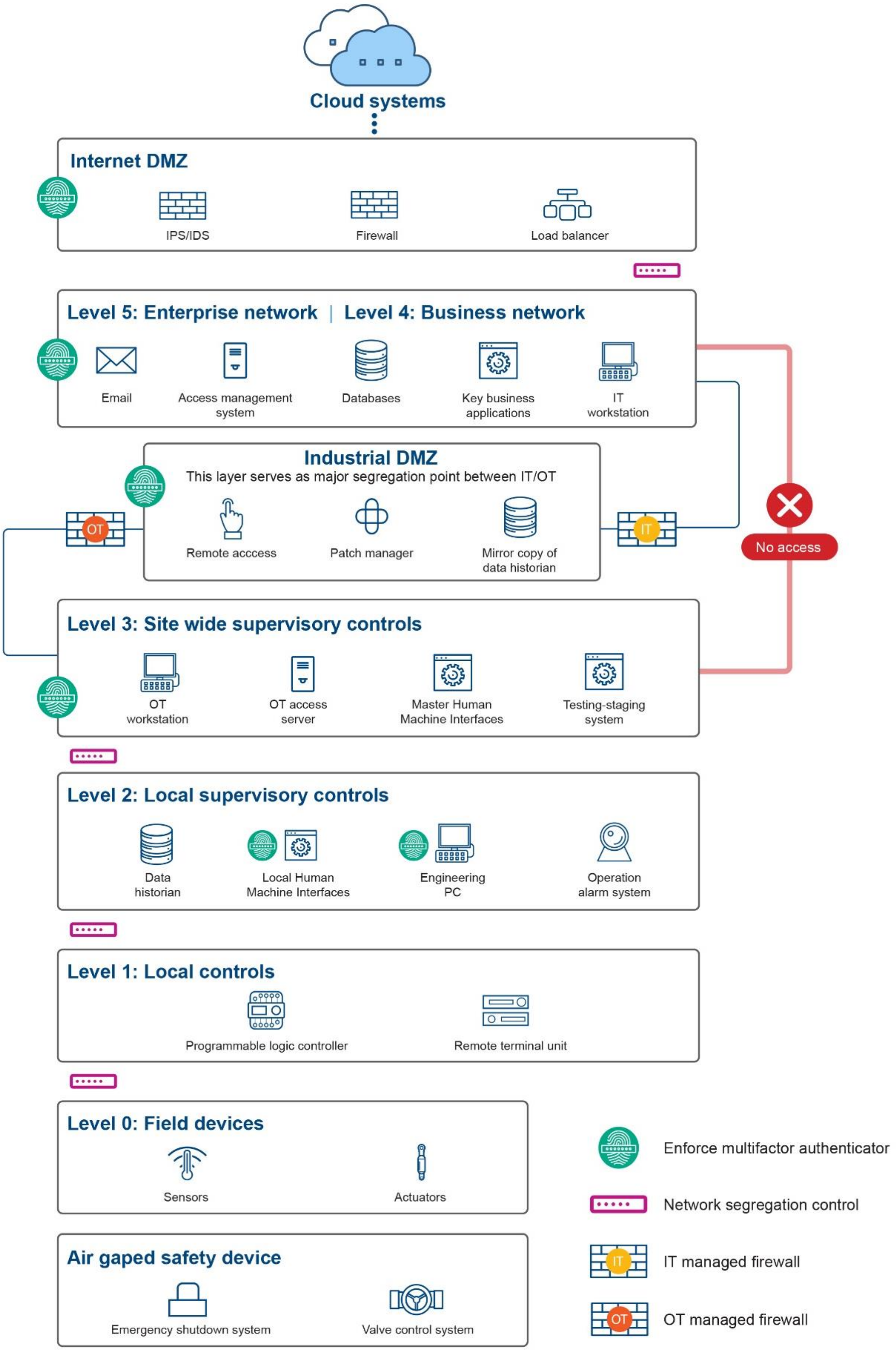
- Modbus TCP
- DNP3
- VSAT
- BGAN
- BACnet
- IEC104
- HART
- SSH
- Telnet
- SMB
- HTTP
- HTTPS
- DNS
- Telnet

IT

- HTTP
- HTTPS
- SSH
- SMB
- SFTP
- SMTP
- DHCP
- DNS
- Telnet

Source: OAG

Appendix 2: OT network segmentation – Purdue Model



Source: OAG based on the Purdue Model

Auditor General’s 2022-23 reports

Number	Title	Date tabled
23	Contractor Procurement – Data Led Learnings	14 June 2023
22	Effectiveness of Public School Reviews	24 May 2023
21	Financial Audit Results – State Government 2021-22 – Part 2: COVID-19 Impacts	3 May 2023
20	Regulation of Air-handling and Water Systems	21 April 2023
19	Information Systems Audit – Local Government 2021-22	29 March 2023
18	Opinions on Ministerial Notifications – Tourism WA’s Campaign Expenditure	27 March 2023
17	Information Systems Audit – State Government 2021-22	22 March 2023
16	Opinions on Ministerial Notifications – Triennial Reports for Griffin Coal and Premier Coal	22 March 2023
15	Opinion on Ministerial Notification – Stamp Duty on the Landgate Building, Midland	8 March 2023
14	Administration of the Perth Parking Levy	16 February 2023
13	Funding of Volunteer Emergency and Fire Services	22 December 2022
12	Financial Audit Results – State Government 2021-22	22 December 2022
11	Compliance with Mining Environmental Conditions	20 December 2022
10	Regulation of Commercial Fishing	7 December 2022
9	Management of Long Stay Patients in Public Hospitals	16 November 2022
8	Forensic Audit Results 2022	16 November 2022
7	Opinion on Ministerial Notification – Tom Price Hospital Redevelopment and Meekatharra Health Centre Business Cases	2 November 2022
6	Compliance Frameworks for Anti-Money Laundering and Counter-Terrorism Financing Obligations	19 October 2022
5	Financial Audit Results – Local Government 2020-21	17 August 2022
4	Payments to Subcontractors Working on State Government Construction Projects	11 August 2022
3	Public Trustee’s Administration of Trusts and Deceased Estates	10 August 2022
2	Financial Audit Results – Universities and TAFEs 2021	21 July 2022
1	Opinion on Ministerial Notification – Wooroloo Bushfire Inquiry	18 July 2022

Office of the Auditor General Western Australia

7th Floor Albert Facey House
469 Wellington Street, Perth

T: 08 6557 7500
E: info@audit.wa.gov.au

www.audit.wa.gov.au

@OAG_WA

Office of the Auditor General
for Western Australia