Introduction to Information Security Registered Assessors Program (IRAP)

PACIFIC AEROSPACE
CONSULTING

We'd like to begin by acknowledging the Traditional Owners of Country throughout Australia and recognising the continuing connection to lands, waters and communities. We pay our respect to Aboriginal and Torres Strait Islander cultures; and to Elders past and present.

PACIFIC AEROSPACE CONSULTING

Agenda

- Who we are
- Background
- Framework
- Purpose
- Methodology
- FAQs
- Q&A

PACIFIC AEROSPACE CONSULTING

Outcomes

- The purpose of an IRAP Assessment
- Government policy relating to IRAP
- Organisations requiring IRAP Assessment
- How requirements of the PSPF may affect DISP organisations
- What is the Information Security Manual and Essential Eight
- The IRAP Assessment lifecycle
- What an organisation should expect from an IRAP assessor
- How to prepare for an IRAP Assessment
- Post-IRAP actions

About PAC

Pacific Aerospace Consulting (PAC) is a veteran-owned SME comprised of two independent companies headquartered in Australia and the USA, providing core capabilities for Defence and commercial clients.

Core services

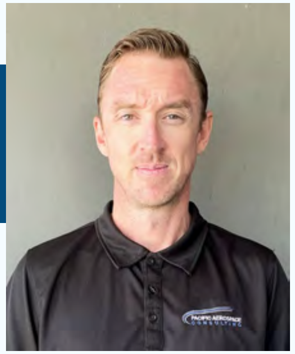
- Cyber Security
- Information Domain Exchange
- Mission Systems
- Training and Simulation

PACIFIC AEROSPACE CONSULTING

Cyber Security

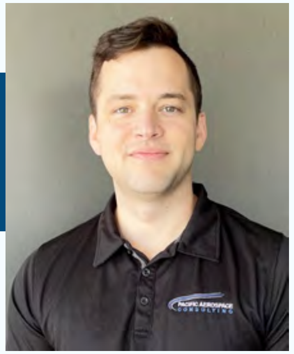
- IRAP Assessment
- Certification and Accreditation Assistance
- DISP Readiness
- ISO 27001 Audit
- Design and Remediation (E8, ISM, NIST)
- Security and Administrative Personnel
- Education, Awareness and Training

Meet the Presenters



BRAD LYNCH
(MCYBERSEC – CISM – CISA – CMMC RP)

- Cyber Security Architect
- ASD-endorsed IRAP assessor



STEFAN MARTINS
(MCYBERSEC – CISSP – CRISC – CMMC RP)

- Cyber Security Architect
- ASD-endorsed IRAP assessor

Government Policy

Cyber and information security

Cyber intrusions on government systems, critical infrastructure, and other information networks

IRAP is a key initiative

Australian Cyber Security Centre (ACSC)

National authority on cybersecurity across Australia.

- Threat Advice
- Incident Response
- Vulnerability Management
- Cybersecurity Education and Awareness
- Information Sharing
- Cyber security framework

Australian Cyber Security Centre (2023), About Us, www.cyber.gov.au/about-us

Introduction to the Information Security Manual (ISM)

Outlines a cyber security framework for organisations.

Written for:

- CISOs
- Cyber professionals
- IT managers

Australian Cyber Security Centre (2023), Using the Information Security Manual, https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/using-information-security-manual

Introduction to the Information Security Manual (ISM)

CYBERSECURITY PRINCIPLES

- Strategic guidance
- Govern, protect, detect and respond

CYBERSECURITY GUIDELINES

- Practical guidelines
- Governance, physical security, personnel security, and ICT security

Australian Cyber Security Centre (2023), Using the Information Security Manual, https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-principles
Australian Cyber Security Centre (2023), Using the Information Security Manual, https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines

Introduction to Essential Eight (E8)

Recommended to implement eight essential mitigation strategies

Makes it much harder for adversaries to compromise systems

Australian Cyber Security Centre (2023), Essential Eight, https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight

E8 Mitigation Strategies

1. Application control
2. Patch applications
3. Configure Microsoft Office macro settings
4. User application hardening
5. Restrict administrative privileges
6. Patch operating systems
7. Multi-factor authentication
8. Regular backups

Australian Cyber Security Centre (2023), Essential Eight Maturity Model, https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

Importance of assessments

How do you know what you have implemented is effective?

- Conformance with Government Requirements
- Assurance of Security Controls
- Risk Management
- Improved Security Posture
- Stakeholder Confidence
- Incident Response Readiness

What is IRAP?

Initiative to provide high-quality security Assessment services to the Australian Government and Industry.

Australian Cyber Security Centre (2023), Infosec Registered Assessors Program (IRAP), https://www.cyber.gov.au/resources-business-and-government/assessment-and-evaluation-programs/infosec-registered-assessors-program

PACIFIC AEROSPACE CONSULTING

What is an IRAP Assessment?

- Independent assessment of a system’s security controls.
- Assessment Report enables informed risk-based decision-making

Benefits of the program

- Enhancing cybersecurity posture
- Qualified and trusted
- Recognition and credibility

Australian Cyber Security Centre (2023), Why engage an IRAP Assessor?, https://www.cyber.gov.au/resources-business-and-government/assessment-and-evaluation-programs/infosec-registered-assessors-program/why-engage-irap-assessor

Which organisations need an IRAP Assessment?

All gateways, managed service providers, and cloud services that process, store, or communicate Australian Government information (excluding Top Secret) require an ASD-endorsed IRAP assessor Assessment.

Security assessments of Secret and below systems can be undertaken by an organisation's own assessors or IRAP Assessors.

Attorney-General's Department (2023), 'Protective Security Policy Framework - Policy 11 - Robust ICT Systems', https://www.protectivesecurity.gov.au/system/files/2023-05/pspf-policy11-robust-ict-systems.pdf

How does this affect DISP members?

- Not a requirement for DISP Cyber Entry Level
- But it depends on the complexity of a system
- Working Securely with Defence Guide (2020)
- Products and services provided to Defence may be subject to an IRAP assessment
- Can allow for faster integration

Stages of an IRAP assessment

1 PLAN AND PREPARE

2 DEFINE THE SCOPE

3 ASSESS SECURITY CONTROLS

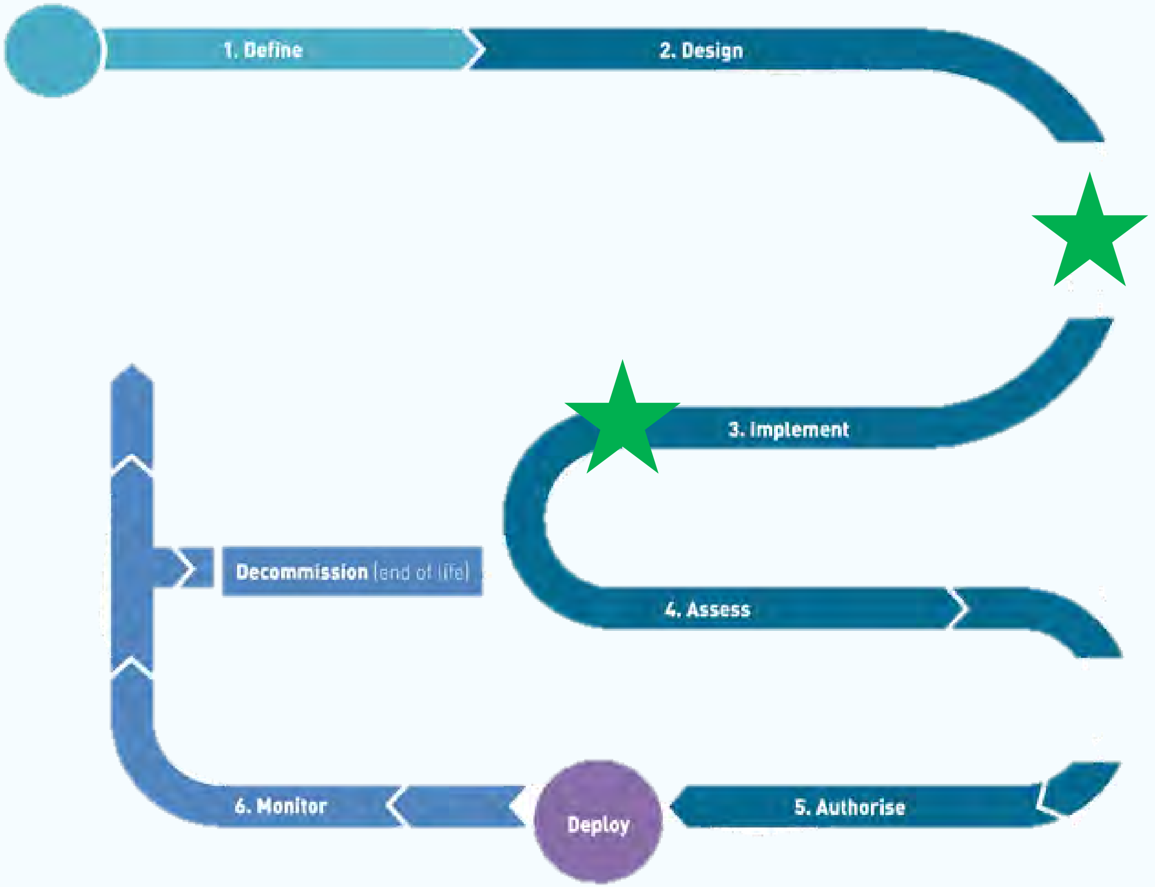
4 PRODUCE ASSESSMENT REPORT

Australian Cyber Security Centre (2023), 'IRAP Assessment Process Guide', https://www.cyber.gov.au/sites/default/files/2023-03/IRAP-Assessment-Process-Guide-06-July-2022.pdf

System lifecycle vs. IRAP Assessment

Assessment takes place immediately after the implementation phase

The engagement starts as early as the definition and design phases



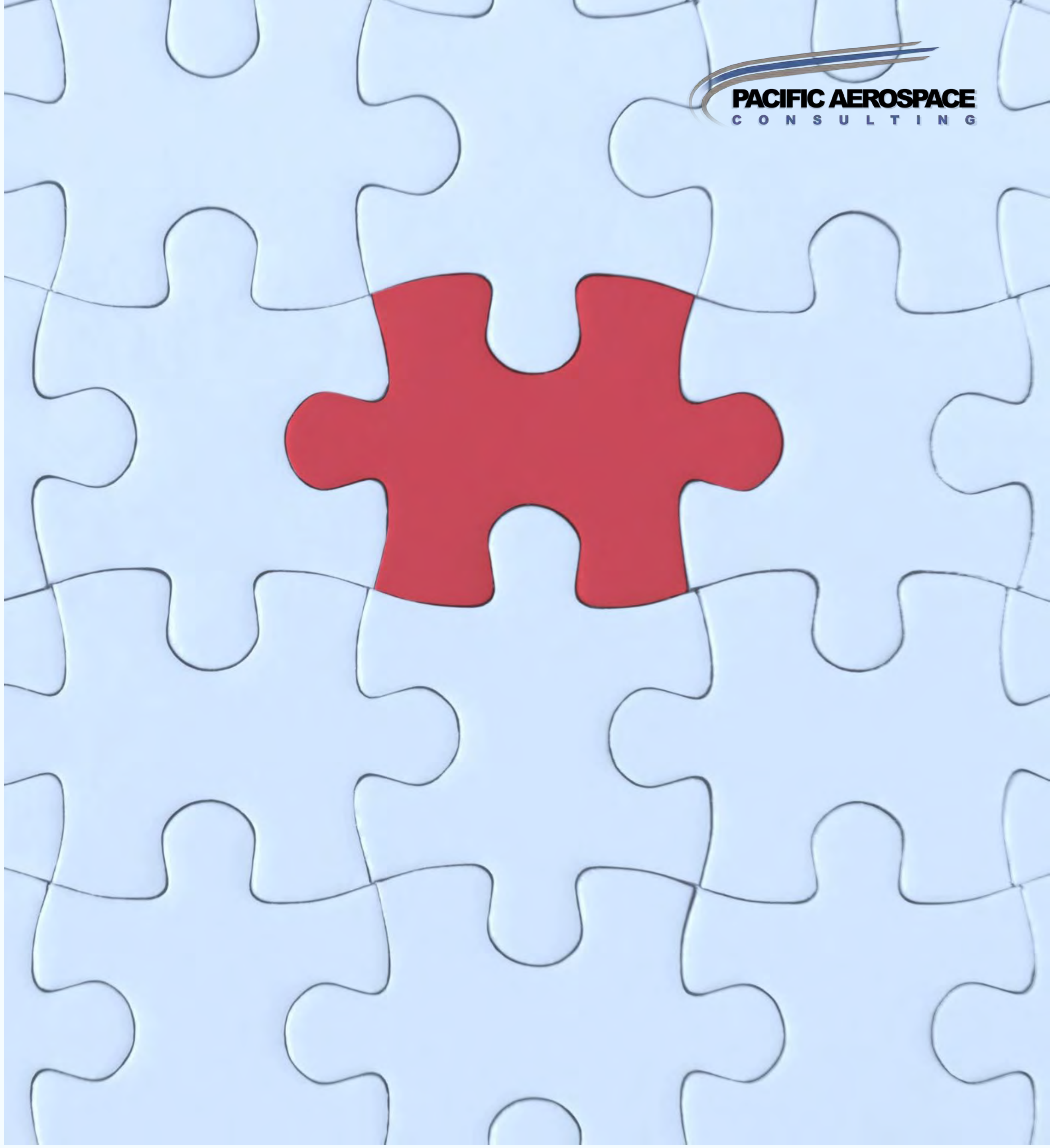
Attorney-General's Department (2023), 'Protective Security Policy Framework - Policy 11 - Robust ICT Systems', https://www.protectivesecurity.gov.au/system/files/2023-05/pspf-policy11-robust-ict-systems.pdf

Non-implementation of controls

The Information Security Manual is not a compliance framework

A risk-based approach

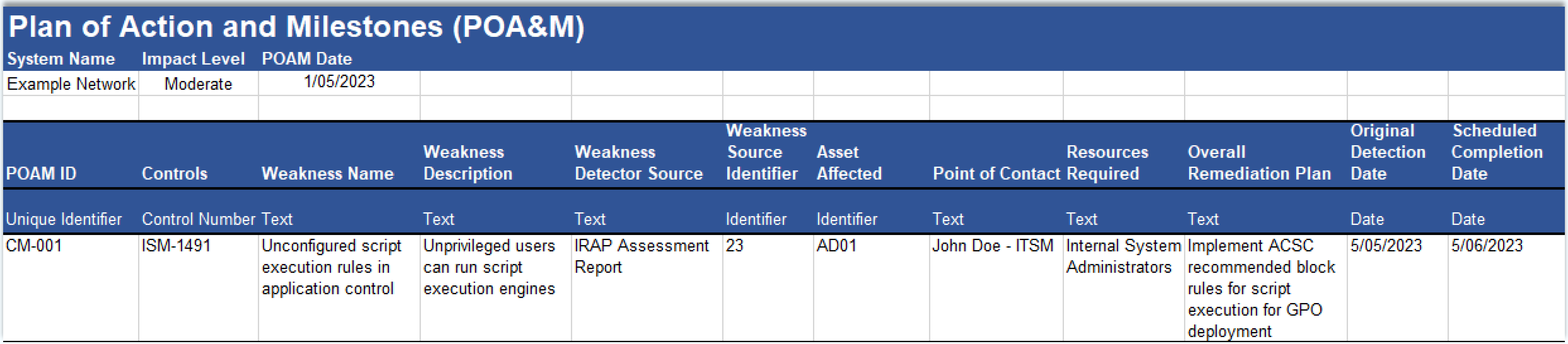
We will evaluate the application of each control



PACIFIC AEROSPACE CONSULTING

IRAP Assessment post-actions

Develop a Plan of Action and Milestones (POAM):



Plan of Action and Milestones (POA&M)

System Name	Impact Level	POAM Date
Example Network	Moderate	1/05/2023

POAM ID	Controls	Weakness Name	Weakness Description	Weakness Detector Source	Weakness Source Identifier	Asset Affected	Point of Contact	Resources Required	Overall Remediation Plan	Original Detection Date	Scheduled Completion Date
Unique Identifier	Control Number	Text	Text	Text	Identifier	Identifier	Text	Text	Text	Date	Date
CM-001	ISM-1491	Unconfigured script execution rules in application control	Unprivileged users can run script execution engines	IRAP Assessment Report	23	AD01	John Doe - ITSM	Internal System Administrators	Implement ACSC recommended block rules for script execution for GPO deployment	5/05/2023	5/06/2023

Common issues

- Misunderstanding the purpose of an IRAP assessment
- Inadequate traceability
- Availability of people, documents, or systems
- Quality of evidence
- Defining favourable assessment outcomes

FAQs

ISO 27001 or NIST frameworks

Any security framework can be applied.

Ensure that your chosen assessor is experienced in other frameworks such as NIST SP 800 series, CMMC, ISO27001 or COBIT.

How long does it take?

PACIFIC AEROSPACE
CONSULTING

Allow at least three months .

Comprehensive IRAP questionnaire can ensure quotations are accurate and estimated timelines are correct.

Is IRAP a certification or authority to operate?

🚫

IRAP does not certify a system or provide an "authority to operate".

✓

independent Assessment

provides a high confidence level

enables risk owner to make informed decisions.

Australian Cyber Security Centre (Oct 2022), IRAP Policy and Procedures , https://www.cyber.gov.au/sites/default/files/2023-03/IRAP%20Policy%20and%20Procedures.pdf

24 months or more overdue Assessment

Generally, a reassessment will only include changes since the previous one.

This may include new or amended controls, architecture, or risks.

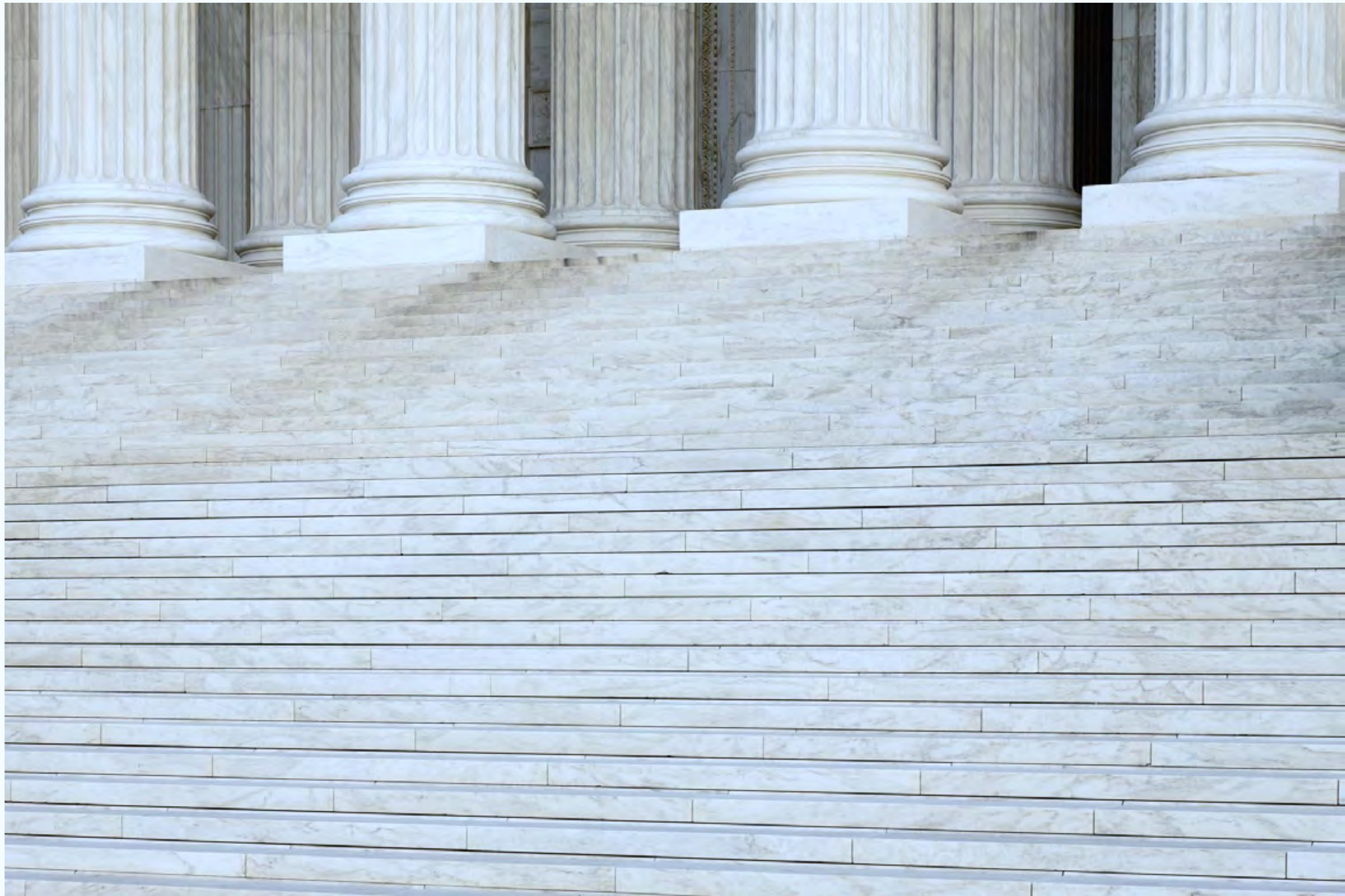
Make past audits available.

When the Certification Authority asks to engage an IRAP assessor

Support the certification and accreditation activity within Government bodies.

Ensure your chosen IRAP assessor has experience coordinating with Certification Authorities (CA) within the Government.

Additional approvals may be required for an IRAP Assessor to act as a certification consultant on behalf of a Defence CA.



Can IRAP assessors provide advice on Remediation or Design?

Yes. However, the independence of the assessor must be maintained. This may mean engaging with an additional IRAP assessor to provide the IRAP Assessment itself.

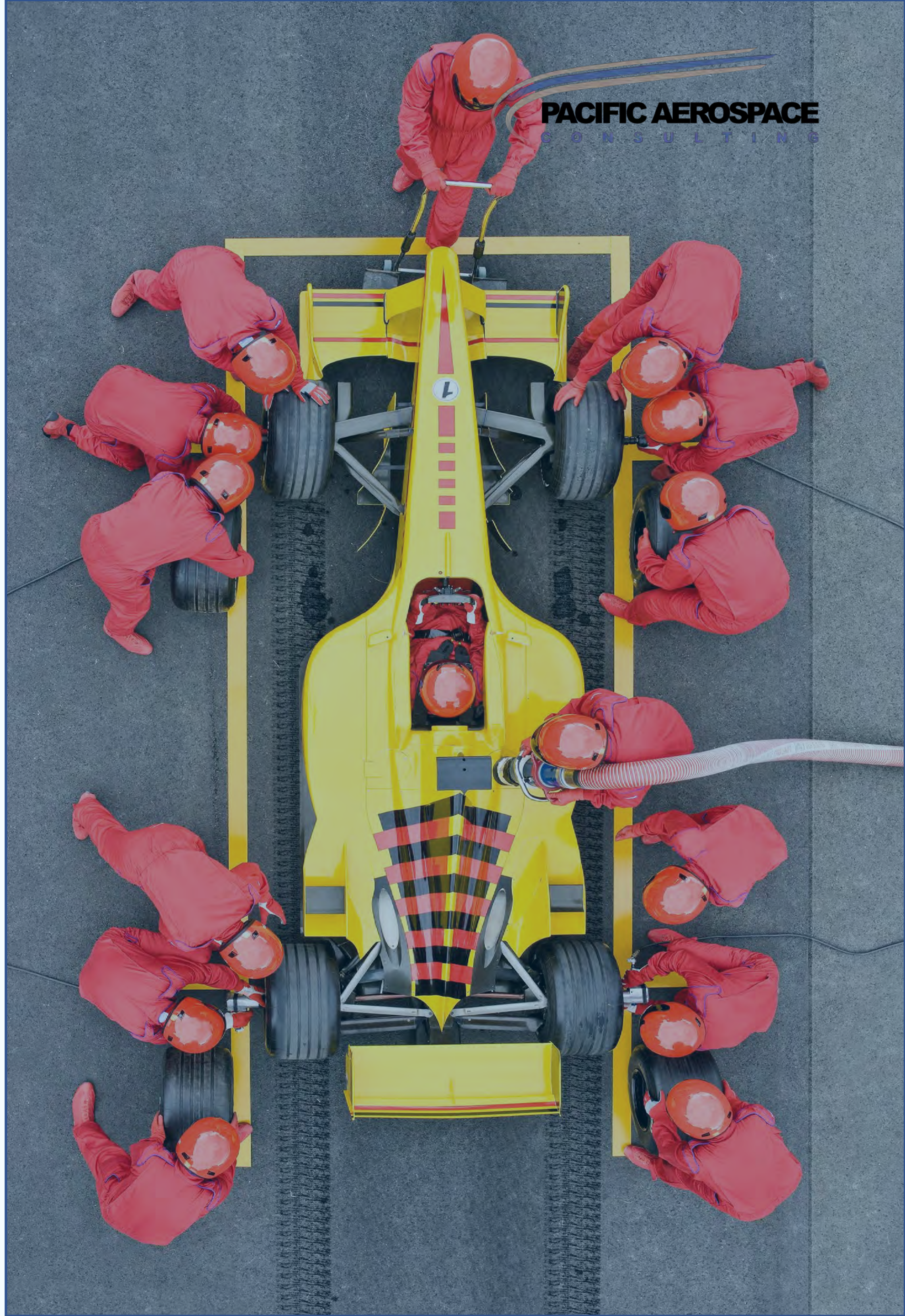
Australian Cyber Security Centre (Oct 2022), IRAP Policy and Procedures , https://www.cyber.gov.au/sites/default/files/2023-03/IRAP%20Policy%20and%20Procedures.pdf

How much it costs?

The cost of an Assessment is based on the scope and ability to obtain and assess the implementation of security controls.

Where else can an IRAP help?

1. Endorsed third-party
2. Independent assessment for informed security decisions
3. Faster integration with authorised systems
4. Prioritise security in technology design to avoid costly remediation



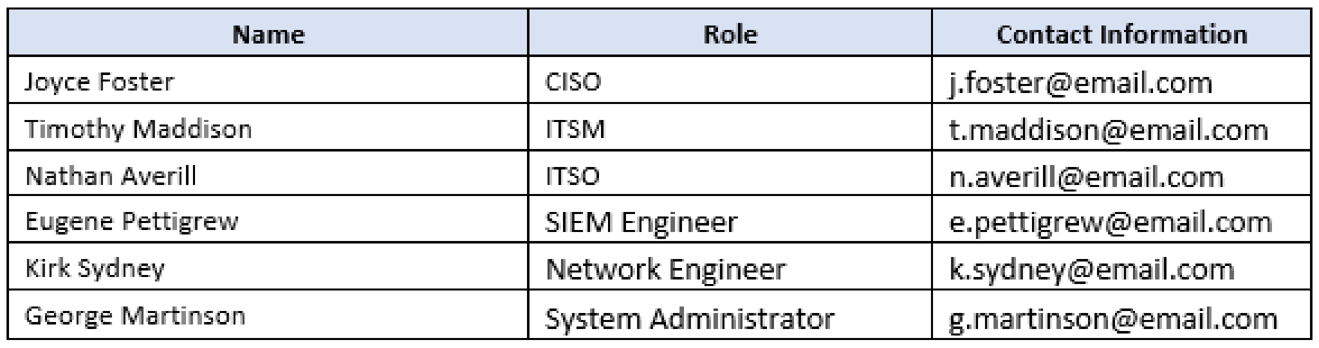
What deliverables can you expect from an IRAP assessor?

PACIFIC AEROSPACE CONSULTING

- Scoping Assessment Report
- Security Assessment Plan
- Design Effectiveness Summary Report
- Operational Effectiveness Assessment Plan
- Security Assessment Report
- Security Controls Matrix

Security Assessment Plan

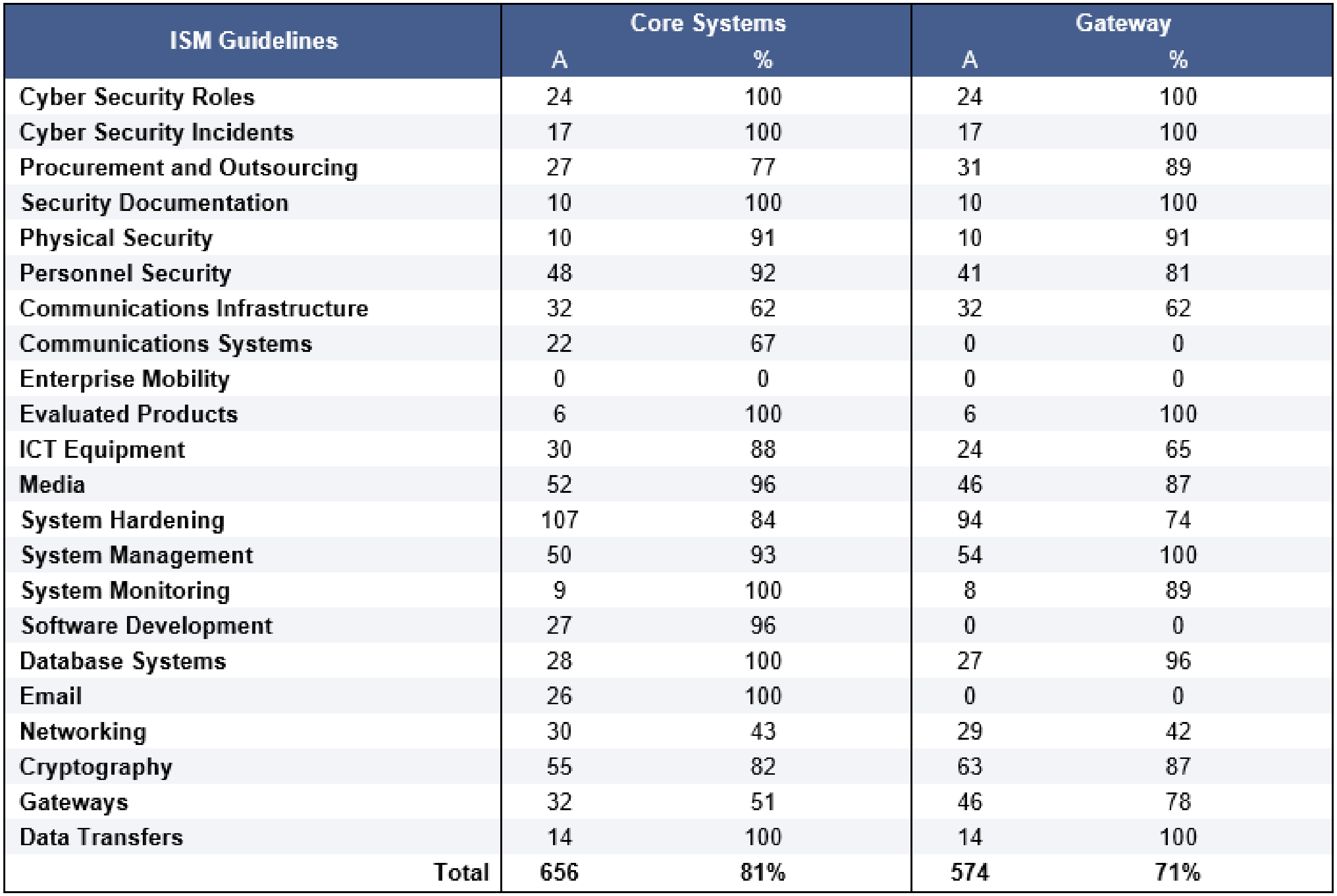
- Assessment timelines
- Scope and assessment boundary
- Assessment objectives
- Version of the ISM used
- Define assessment methodologies



Name	Role	Contact Information
Joyce Foster	CISO	j.foster@email.com
Timothy Maddison	ITSM	t.maddison@email.com
Nathan Averill	ITSO	n.averill@email.com
Eugene Pettigrew	SIEM Engineer	e.pettigrew@email.com
Kirk Sydney	Network Engineer	k.sydney@email.com
George Martinson	System Administrator	g.martinson@email.com

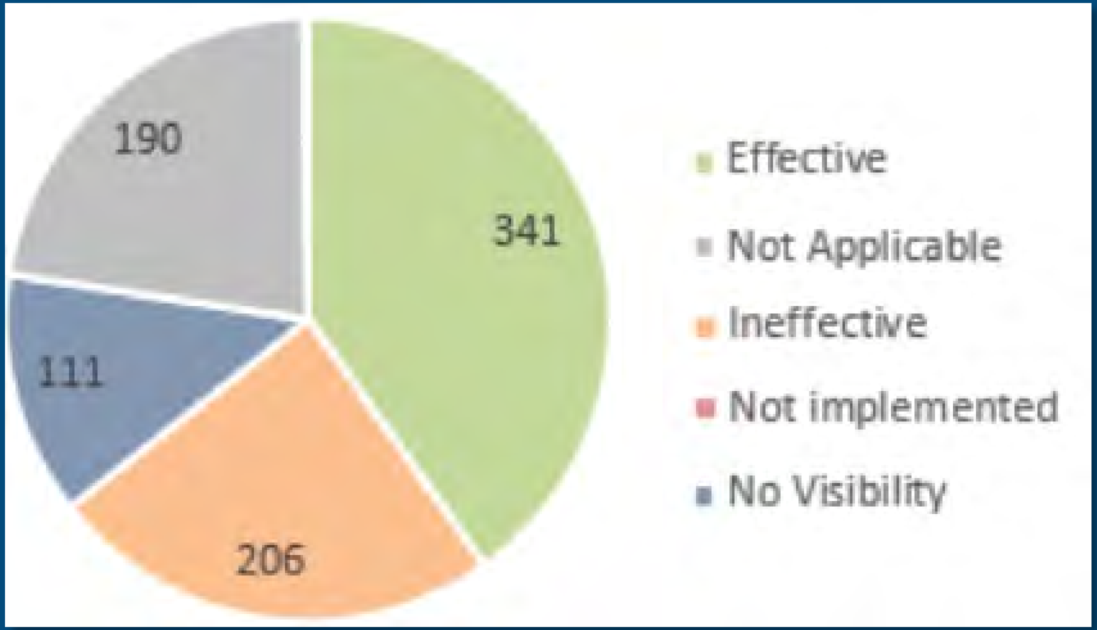
Scoping Assessment Report

- Define the scope
- Ensure accuracy
- Invaluable in high-complexity scenarios
- Same understanding



ISM Guidelines	Core Systems		Gateway	
	A	%	A	%
Cyber Security Roles	24	100	24	100
Cyber Security Incidents	17	100	17	100
Procurement and Outsourcing	27	77	31	89
Security Documentation	10	100	10	100
Physical Security	10	91	10	91
Personnel Security	48	92	41	81
Communications Infrastructure	32	62	32	62
Communications Systems	22	67	0	0
Enterprise Mobility	0	0	0	0
Evaluated Products	6	100	6	100
ICT Equipment	30	88	24	65
Media	52	96	46	87
System Hardening	107	84	94	74
System Management	50	93	54	100
System Monitoring	9	100	8	89
Software Development	27	96	0	0
Database Systems	28	100	27	96
Email	26	100	0	0
Networking	30	43	29	42
Cryptography	55	82	63	87
Gateways	32	51	46	78
Data Transfers	14	100	14	100
Total	656	81%	574	71%

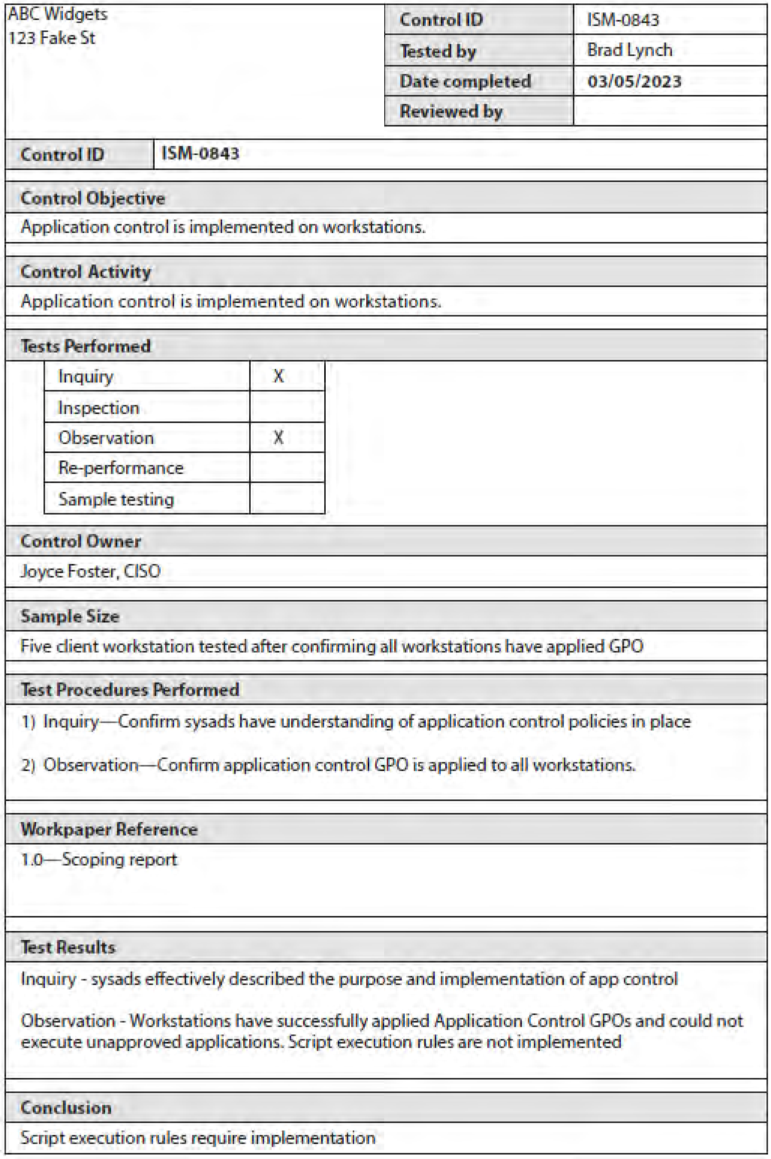
Design Effectiveness Summary Report



- Summary of observations and recommendations
- Implementation status of security controls from a design perspective.
- Analysis of system documentation suite

Operational Effectiveness Assessment Plan

- Detail methodology of assessment
- Assessment priorities
- Defines control test activities are used to control implementation and effectiveness
- Evidence gathering (Inquiry, Observation, Re-performance)



ABC Widgets
123 Fake St

Control ID	ISM-0843
Tested by	Brad Lynch
Date completed	03/05/2023
Reviewed by	

Control ID	ISM-0843

Control Objective

Application control is implemented on workstations.

Control Activity

Application control is implemented on workstations.

Tests Performed

Inquiry	X
Inspection	
Observation	X
Re-performance	
Sample testing	

Control Owner

Joyce Foster, CISO

Sample Size

Five client workstation tested after confirming all workstations have applied GPO

Test Procedures Performed

1) Inquiry—Confirm sysads have understanding of application control policies in place

2) Observation—Confirm application control GPO is applied to all workstations.

Workpaper Reference

1.0—Scoping report

Test Results

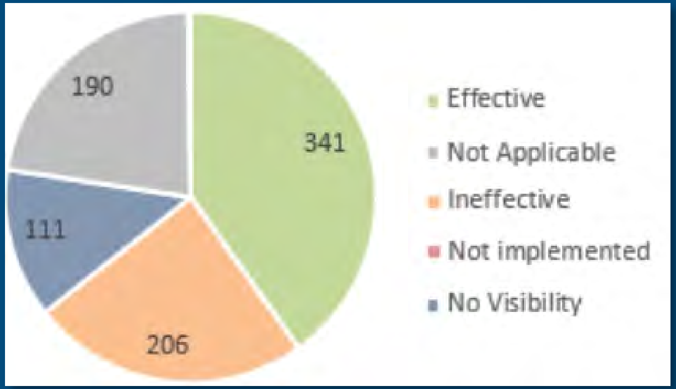
Inquiry - sysads effectively described the purpose and implementation of app control

Observation - Workstations have successfully applied Application Control GPOs and could not execute unapproved applications. Script execution rules are not implemented

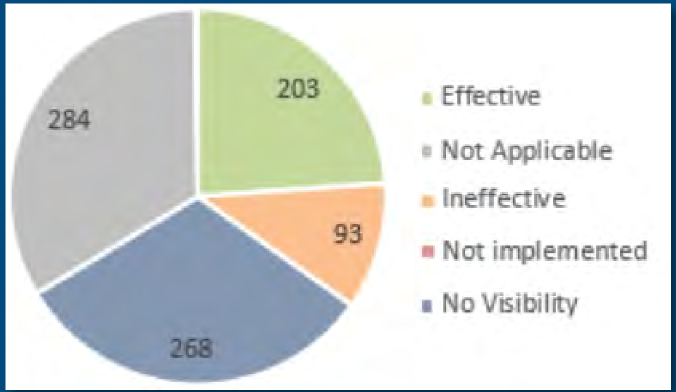
Conclusion

Script execution rules require implementation

Security Assessment Report



Assessment results for Design Effectiveness



Assessment results for Operational Effectiveness

Culmination of previous assessment activities. At a high level:

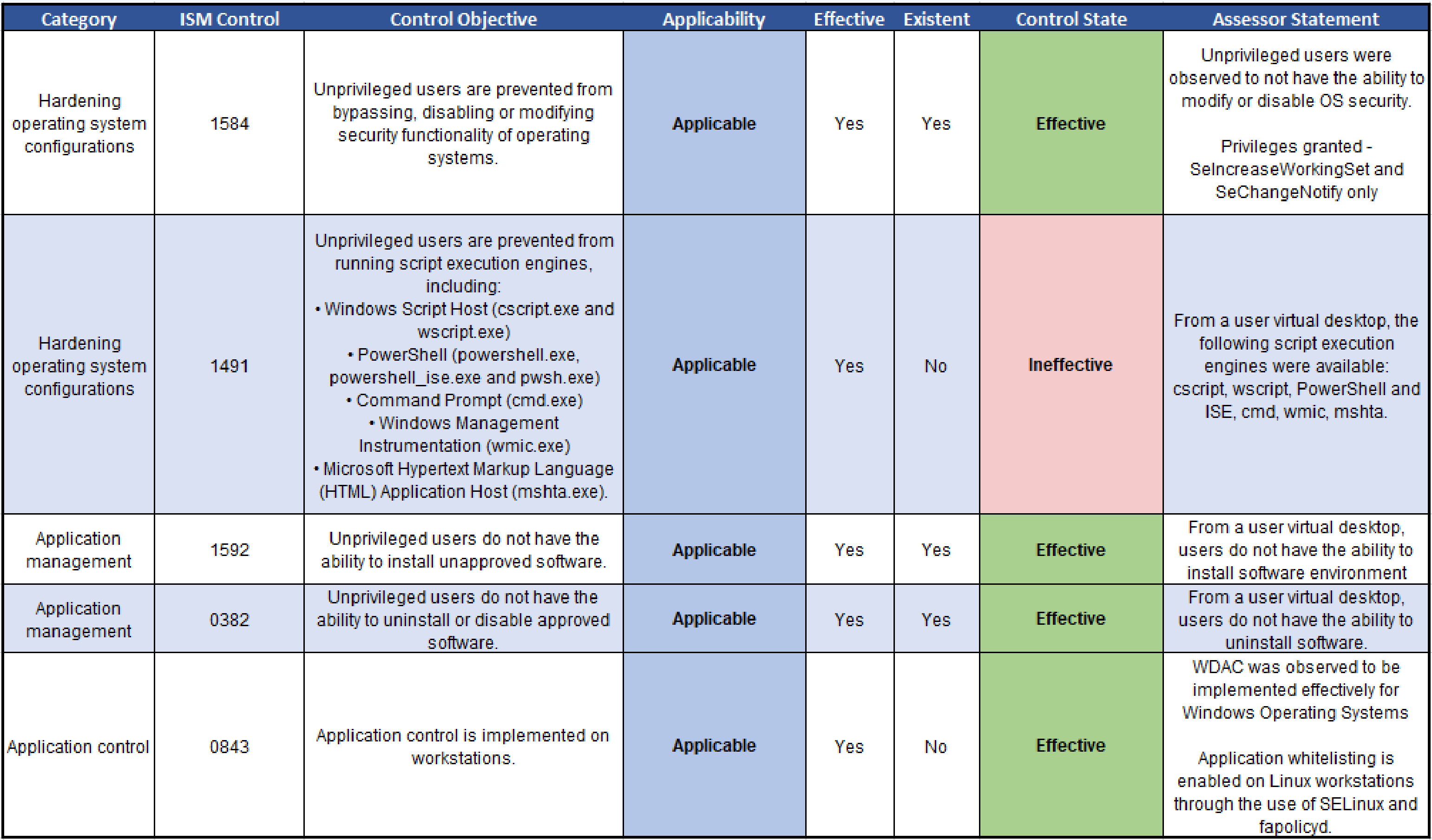
- Assessment scope
- Effectiveness of security controls
- Identified security risks
- Any recommendations identified during assessments
- Quality of Evidence

Security Controls Matrix

Provided as part of the Security Assessment Report.

Observations against each ISM control:

- Applicability
- Control state
- Effectiveness
- Recommendations



Category	ISM Control	Control Objective	Applicability	Effective	Existent	Control State	Assessor Statement
Hardening operating system configurations	1584	Unprivileged users are prevented from bypassing, disabling or modifying security functionality of operating systems.	Applicable	Yes	Yes	Effective	Unprivileged users were observed to not have the ability to modify or disable OS security. Privileges granted - SeIncreaseWorkingSet and SeChangeNotify only
Hardening operating system configurations	1491	Unprivileged users are prevented from running script execution engines, including: • Windows Script Host (cscript.exe and wscript.exe) • PowerShell (powershell.exe, powershell_ise.exe and pwsh.exe) • Command Prompt (cmd.exe) • Windows Management Instrumentation (wmic.exe) • Microsoft Hypertext Markup Language (HTML) Application Host (mshta.exe).	Applicable	Yes	No	Ineffective	From a user virtual desktop, the following script execution engines were available: cscript, wscript, PowerShell and ISE, cmd, wmic, mshta.
Application management	1592	Unprivileged users do not have the ability to install unapproved software.	Applicable	Yes	Yes	Effective	From a user virtual desktop, users do not have the ability to install software environment
Application management	0382	Unprivileged users do not have the ability to uninstall or disable approved software.	Applicable	Yes	Yes	Effective	From a user virtual desktop, users do not have the ability to uninstall software.
Application control	0843	Application control is implemented on workstations.	Applicable	Yes	No	Effective	WDAC was observed to be implemented effectively for Windows Operating Systems Application whitelisting is enabled on Linux workstations through the use of SELinux and fapolicyd.

Thank you

✉ brad.lynch@pacaerocon.com.au
stefan.martins@pacaerocon.com.au

☎ +61 2 4081 2887

in pacific-aerospace-consulting

f PACAeroCon

🌐 pacificaerospaceconsulting.com.au

PACIFIC AEROSPACE
CONSULTING