Deloitte.

Department of Defence

Gatekeeper Audit of the Defence Public Key Infrastructure (PKI)

5 May 2016

Contents

Inherent Limitations

The Services provided are advisory in nature and have not been conducted in accordance with the standards issued by the Australian Auditing and Assurance Standards Board and consequently no opinions or conclusions under these standards are expressed.

Recommendations and suggestions for improvement should be assessed by management for their full commercial impact before they are implemented.

We believe that the statements made in this report are accurate, but no warranty of completeness, accuracy, or reliability is given in relation to the statements and representations made by, and the information and documentation provided by Department of Defence personnel. We have not attempted to verify these sources independently unless otherwise noted within the report.

Limitation of Use

This report is intended solely for the information and internal use of Department of Defence in accordance with our Work Order CIOG487/15 and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely, in any manner, or for any purpose, on this report. We do not accept or assume responsibility to anyone other than Department of Defence for our work, for this report, or for any reliance which may be placed on this report by any party other than Department of Defence.

Confidential - this document and the information contained in it are confidential and should not be used or disclosed in any way without our prior consent.

Executive Summary

The Gatekeeper Public Key Infrastructure (PKI) Framework governs the use of digital keys and certificates used to assure the identity of subscribers to authentication services operated within Australian Government. The Gatekeeper Framework sets out the accreditation requirements for organisations PKI-based authentication and technology to issue digital keys and certificates used to provide assurance of the identity of subscribers, which can include individual users, organisations and non-human devices. It is against this Framework that the Australian Department of Defence (Defence) PKI is seeking an Information Security Registered Assessor Program (IRAP) assessment for compliances against the Gatekeeper core requirements.

Like most modern organisations seeking to achieve its business and operational outcomes, Defence has a strong reliance on electronic information exchanges and transactions throughout the Defence Information Environment (DIE). Operating out the Certificate and Directory Management Centre (CDMC), Defence leverages the assurance of the identity associated with the issued certificates to create a level of confidence and trust in these electronic transactions. This includes confidence in the confidentiality and integrity of the data as well as confidence in the authentication and non-repudiation of the users actions.

As part of the Gatekeeper IRAP assessment, a total of 228 controls were assessed. These controls are categorised under the requirement areas of: Documentation (78 controls), Physical (51 controls), Logical (89 controls) and Personnel (10 controls). Of these requirement areas, the Defence PKI was deemed compliant with 65 Documentation controls, 51 (all) Physical controls, 72 Logical controls and 9 Personnel controls.

Within the Gatekeeper Framework, non-compliance with a control is rated at one of four levels and increasing with severity: Minor, Partial, Major and Critical. In total, 31 controls were deemed non-compliant with the delineation being:

- Of the 13 Documentation controls deemed non-compliant, 4 had a severity rating of Minor, 6 had a severity rating of Partial, and 3 had a severity rating of Major
- Of the 17 Logical controls deemed non-compliant, 16 had a severity rating of Partial and one (1) had a severity rating of Major
- The single Personnel control deemed non-compliant had a severity rating of Partial.

While there was 31 controls deemed non-compliant but with none rated critical, it is the opinion of the IRAP Assessor that the functions of the Defence PKI are still sufficiently compliant with the Gatekeeper Framework that the Defence PKI environment should retain its Gatekeeper Accreditation.

However, significant changes are currently being planned for the Defence PKI environment, including the relocation of one of the operations centres and upgrades to DIE computing platforms. For these reasons, it is recommended that Gatekeeper Accreditation be granted for ***only*** 12 months to ensure that Defence revisit Gatekeeper Accreditation at the completion of these activities.

1 Glossary

Throughout this document, unless otherwise indicated, the following references apply. These references act to clarify this report and are not intended to be authoritative.

Reference	Description
ACP	Allied Communications Publication
ACSI	Australian Communications-Electronic Security Instruction
AD-CPS	Australian Defence Certificate Practice Statement
ADF	Australian Defence Force
ADOCA	Australian Defence Organisation Certification Authority
AGIMO	Australian Government Information Management Office
AKR	Authorised Key Retriever
ASD	Australian Signals Directorate
BOC	Backup Operations Centre
CA	Certification Authority
CAO	CA Operator
CCA	Cross-Certification Agreement
CDMA	Certificate and Directory Management Centre
CJM3IEM	Combined Joint Multilateral Master Military Information Exchange Memorandum of Understanding
CMS	Card Management System
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSA	Certificate Status Authority
DIE	Defence Information Environment
DIOCA	Defence Interoperability CA
DN	Distinguished Name
DPKIPB	Defence Public Key Infrastructure Policy Board
DRBCP	Disaster Recovery and Business Continuity Plan
DRCA	Defence Root Certificate Authority
DRCAO	Defence Root Certificate Authority Operator
DRN	Defence RESTRICTED Network
DSA	Defence Security Agency
DSM	Defence Security Manual
DSN	Defence SECRET Network

Reference	Description
EAL	Evaluated Assurance Level
EBDb	Everybody Database
eDSM	Electronic Defence Security Manual
eNAR	electronic Network Access Request
EOI	Evidence of Identity
EPL	Evaluated Products List
HDSA	Head Defence Security Authority
HSM	Hardware Security Module
I&A	Identification and Authentication
ICTSP	Information Communication Technology Security Plan
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISA	Information Systems Assurance
ISM	(Australian Government) Information Security Manual
ISO	International Standards Organisation
ITSEC	Information Technology Security Evaluation Criteria
KAO	Key Archive Operator
KAS	Key Archive Server
KMP	Key Management Plan
LOA	Level of Assurance
LTSK	Long Term Storage Key
NCA	National Cryptographic Authority
NPE	Non-Person Entity
OCSP	Online Certificate Status Protocol
ODS	Other Defence Support
OID	Object Identifier
PED	Pin Entry Device
PIN	Personal Identification Number
PIV	Personal Identification Verification
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
POC	Primary Operations Centre
PSE	Personal Secure Environment
RA	Registration Authority
RAA	Registration Authority Auditor
RAO	Registration Authority Operator
RC	Resource Custodian

Reference	Description
RFC	Request For Comment
RO	Registration Officer
SCEP	Simple Certificate Enrolment Protocol
SCVP	Server-based Certificate Validation Protocol
SO	Security Officer
SRMP	Security Risk Management Plan
SSL	Secure Sockets Layer
SSP	System Security Plan
SubCA	Subordinate Certificate Authority
SubCAO	Subordinate Certificate Authority Operator
TLS	Transport Layer Security
TSA	Timestamp Authority
TSS	Timestamp Server
UPS	Uninterruptible Power Supplier
URI	Uniform Resource Identifier
UTC	Coordinated Universal Time
UUID	Universally Unique Identifier
VA	Validation Authority

2 Documentation Review Controls

As part of the Gatekeeper IRAP assessment, a total of 78 Documentation controls were assessed, with the Defence PKI deemed compliant with 65 of those 78 Documentation controls. Thirteen (13) Documentation controls were deemed non-compliant, non-compliance with a control is rated at one of four levels and increasing with severity: Minor, Partial, Major and Critical. Four non-compliant Documentation controls have a severity rating of Minor, six have a severity rating of Partial, and three have a severity rating of Major.

2.1 Service Provider Governance

No	**Source**	**Control**	**Applicability**	**Framework sections**
No: 1	**Source:** GK	**Control:** GK	**Applicability:** RA, CA, VA	**Framework sections:** 6.3
Service Providers MUST be registered with the Australian Business Register and maintain a current Australian Business Number.				
Compliance	**Compliant**	**Rationale**	The Department of Defence have a current Australian Business Number (ABN 68 706 814 312) and is registered within the Australian Business Register.	
No: 2	**Source:** GK	**Control:** GK	**Applicability:** RA, CA, VA	**Framework sections:** 6.3
Service Providers MUST be physically located within Australia and provide services from within Australia. Any remote connections to the PKI environment MUST also occur from within Australia.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	The CA is physically located within Australia (Deakin Offices and HMAS Harman) and all connections for PKI operational activities, i.e. those that directly impact the operation of the PKI infrastructure, occur within Australia.	
No: 3	**Source:** ISM	**Control:** 1071	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.5
Each system MUST have a system owner who is responsible for the operation of the system.				
Compliance	**Compliant**	**Rationale**	The system owner for the Defence Gatekeeper PKI is the CIO, with the Chair of the Defence PKI Board responsible on a day-to-day basis. The overall governance of operations and approval of policies is undertaken by the Defence PKI Policy Board. The everyday operation of the Defence PKI is the responsibility of the PKI Operations Manager.	
No: 4	**Source:** ISM, PSPF	**Control:** 1229, GOV2	**Applicability:** RA, CA, VA	**Framework sections:** 7, 9.2, 9.5
A Service Provider's Accreditation Authority MUST be at least a senior executive with an appropriate level of understanding of the security risks they are accepting on behalf of the Service Provider.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	The Defence PKI Policy Board is the decision point for all activities that occur within the Defence PKI environment. The Defence PKI Policy Board is chaired by the Director General ICT Strategy, Plan and Policy (DGICTSPP) from within the Chief Technology Officer Division (CTOD). The Secretariat of the DPKIPB is undertaken by the Deputy Director Identity Projects Military and Security Program Delivery (MSPD) Chief Information Officer Group (CIOG) with the PKI Operations Manager and an Independent Advisor complting the DPKIPB.	
No: 5	**Source:** ISM, PSPF	**Control:** 768, GOV3	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.5
Service Providers MUST appoint at least one expert, commonly referred to as an ITSA (or an equivalent position), in administering and configuring a broad range of systems as well as analysing and reporting on information security issues.				
Compliance	**Compliant**	**Rationale**	The CDMC Security Officer (SO) is used to enforce policies as defined by the operational documentation, Defence security policy and governmental guidelines. The CDMC SO is also responsible for the initial investigation and reporting of incidents.	
No: 6	**Source:** ISM, PSPF	**Control:** 741, GOV2	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK2), 9.2, 9.5
Service Providers MUST appoint at least one executive, commonly referred to as an ITSM (or an equivalent position), to manage the day-to-day operations of information security within the Service Provider, in line with the strategic directions provided by the CISO or equivalent.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	The CDMC SO is mandated to enforce policies as defined by the operational documentation, Defence security policy and governmental guidelines. Those duties are defined within the PKI Operations Manual, the Defence PKI Certificate Practice Statement (CPS) and Defence PKI Standard Operating Procedures (SOPs).	
No: 7	**Source:** ISM	**Control:** 7	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5
Service Providers undertaking system design activities for in-house or out-sourced projects MUST use the latest release of the ISM for security requirements.				
Compliance	**Compliant**	**Rationale**	At the time of design, the latest version of the ISM was in use. Future planned activities, primarily the relocation of the CDMC infrastructure and support mechanisms is being project managed and designed in accordance with Defence requirements, including the use of the latest version of the ISM in the event that underlining infrastructure is expected to change.	
No: 8	**Source:** ISM	**Control:** 710	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.8, 10.3

No	Source	Control	Applicability	Framework sections
Service Providers seeking approval for non-compliance with any control MUST document: • the justification for non-compliance, • a security risk assessment, • the alternative mitigation measures to be implemented, if any.				
Compliance	**Compliant**	**Rationale**	All previous decisions, particularly around the use of SHA1 have been documented in each of the policy documents and include a statement of risk. The expectation is that this will continue with any non-compliances identified within this assessment report.	
Recommendation 1: That any identified and accepted non-compliance with controls identified within this report be justified in writing and validated with a risk assessment and any mitigation measures listed.				
No: 9	**Source:** ISM, GK	**Control:** 3, GK	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.8, 10.3
Service Providers MUST retain a copy of decisions to grant non-compliance with any Gatekeeper specific control from the ISM.				
Compliance	**Compliant**	**Rationale**	All previous decisions have been documented in the relevant policy documents and include a statement of risk. The expectation is that this will continue with any non-compliances identified within this assessment report.	
Recommendation 2: That any identified and accepted non-compliance with controls be retained as evidence for the next Gatekeeper assessment.				
No: 10	**Source:** ISM	**Control:** 876	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.8, 10.3

No	Source	Control	Applicability	Framework sections
Service Providers MUST review decisions to grant non-compliance with any control, including the justification, any mitigation measures and security risks, at least annually or when significant changes occur to ensure its continuing relevance, adequacy and effectiveness.				
Compliance	**Compliant**	**Rationale**	The review process includes the approval by the Defence PKI Policy Board. Significant events are ratified with the Gatekeeper Competent Authority.	
No: 11	**Source:** PSPF	**Control:** GOV10	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK6)
Service Providers MUST adhere to any provisions concerning the security of people, information and assets contained in multilateral or bilateral agreements and arrangements to which Australia is a party.				
Compliance	**Compliant**	**Rationale**	The Defence PKI is a key partner in the multilateral agreement as specified in ACP 185, Public Key Infrastructures (PKI) Cross-Certification Between Combined Communications-Electronics Board (CCEB) Nations and adheres to its provisions.	
No: 12	**Source:** GK	**Control:** GK	**Applicability:** RA, CA, VA	**Framework sections:** 6.3
Service Providers MUST document their compliance with Gatekeeper Core Obligations in their legal documents such as the CPS, CP, Subscriber and Relying Party Agreements (where relevant), or into other Approved Documents submitted for approval by the Gatekeeper Competent Authority.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	The Gatekeeper Core Obligations are referenced within the relevant PKI CPS and CPs. Note: The Defence PKI Subscriber Agreement does not reference the core obligations.	
No: 13	**Source:** ISM	**Control:** 137	**Applicability:** RA, CA, VA	**Framework sections:** 9.9
Service Providers considering allowing intrusion activity to continue under controlled conditions for the purpose of seeking further information or evidence MUST seek legal advice.				
Compliance	**Compliant**	**Rationale**	The decision on allowing an identified intrusion to continue would be at the insistence of ADFCERT and ASD. It is therefore expected that any legal decisions or position regarding this purpose would be instigated by either of those two entities and not the CDMC.	

2.2 Information Security Documentation

2.2.1 Information Security Policy

No	Source	Control	Applicability	Framework sections
No: 14	**Source:** ISM, PSPF	**Control:** 39, GOV5, INFOSEC 1	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK3), 9.2

No	Source	Control	Applicability	Framework sections
Service Providers MUST have an Information Security Policy which covers the PKI environment.				
Compliance	**Compliant**	**Rationale**	While this control has been identified as Compliant as the DPKI environment is covered by the PKI ICTSP, it is noted that the PKI ICTSP needs to include detail about the accreditation process to be compliant with associated ISM 0890 control.	
Recommendation 3: That the DPKI ICTSP be updated to include a description of this Gatekeeper and Defence's Accreditation processes.				

2.2.2 Protective Security Risk Review

No	Source	Control	Applicability	Framework sections
No: 15	**Source:** GK	**Control:** GK	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4
Threats to PKI services, assets and business processes MUST be outlined in the Protective Security Risk Review and Security Risk Management Plan documents as part of the Service Provider's Information Security Documents.				
Compliance	**Non-Compliant**	**Rationale**	While an extensive risk assessment and management plan exists with the DPKI SRMP, there is currently no Protective Security Risk Review for the DPKI environment.	
Recommendation 4: That the CDMC adapt the existing DPKI SRMP to include the requirements of the Protective Security Risk Review. Recommendation 5: That the CDMC undertake and document a Protective Security Risk Review as a separate artefact.				

2.2.3 Security Risk Management Plan

No	Source	Control	Applicability	Framework sections
No: 16	**Source:** ISM, PSPF	**Control:** 40, GOV4, 5 & 6, INFOSEC 2	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK3 & 4), 9.4
All systems MUST be covered by a Security Risk Management Plan.				
Compliance	**Compliant**	**Rationale**	All nominated PKI Systems and the day-to-day operations are covered by the SRMP. This includes the threats and risk faced by the Defence Root Certification Authority and Sub Certification Authorities and associated operations undertaken within the Defence PKI facilities.	
No: 17	**Source:** ISM	**Control:** 1208	**Applicability:** RA, CA, VA	**Framework sections:** 9.4
Service Providers MUST document identified information security risks, as well as the evaluation of those risks and mitigation strategies, in their Security Risk Management Plan.				
Compliance	**Compliant**	**Rationale**	A comprehensive analysis is undertaken within the risk assessment which clearly identifies those risks the CDMC face in the day-to-day operation of the PKI environment, which is then documented.	

No	Source	Control	Applicability	Framework sections
No: 18	**Source:** ISM	**Control:** 1203	**Applicability:** RA, CA, VA	**Framework sections:** 9.4
Service Providers MUST identify and analyse security risks to their information and systems.				
Compliance	**Compliant**	**Rationale**	A comprehensive analysis is undertaken during this risk assessment which clearly identifies those risks the CDMC face in the day-to-day operation of the PKI environment.	
No: 19	**Source:** ISM	**Control:** 1204	**Applicability:** RA, CA, VA	**Framework sections:** 9.4
Security risks deemed unacceptable MUST be treated.				
Compliance	**Compliant**	**Rationale**	Identified risks have in some ways all been treated. A realistic risk assessment process within the SRMP enables some of the controls to only be reduce in a slight manner, however all risks have been treated.	
No: 20	**Source:** GK	**Control:** GK	**Applicability:** RA, CA, VA	**Framework sections:** 9.4
Assets to be protected MUST be identified in the Risk Assessment.				
Compliance	**Compliant**	**Rationale**	Assets are defined within the Scope section of the Defence PKI SRMP. Primarily, these include the relevant elements such as the Defence Root CA, the associated SubCAs, the facilities, hardware and software used in the operation of the Defence PKI as well as the staff that operate the Defence PKI.	

No	Source	Control	Applicability	Framework sections
No: 21	**Source:** ISM	**Control:** 1205	**Applicability:** RA, CA, VA	**Framework sections:** 9.4
Service Providers MUST incorporate the relevant controls contained in the current version of the ISM in their security risk management processes. The relevant controls are those listed in this IRAP Guide.				
Compliance	**Non-Compliant**	**Rationale**	No explicit or implied referencing to the ISM Controls occurs within the SRMP review. It does imply servitude to the ISM but does not categorically meet this control.	
Recommendation 6: That the Controls listed within the SRMP be referenced against the ISM categories listed within the ISM. Recommendation 7: That future iterations of the SRMP specify which Controls within the ISM are relevant to the controls of SRMP.				
No: 22	**Source:** ISM, PSPF	**Control:** 1354, GOV5 & GOV6, INFOSEC 2	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK3 & 4), 9.4, 9.8, 10.3
Service Providers MUST adopt a risk–management approach and implement alternative security controls for: • technologies which lack available software to enforce the mandatory controls; and • scenarios or circumstances which prevent enforcement of the mandatory Top 4 Strategies.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	While the Top4 has not been included explicitly within the SRMP, especially as the current environment relies on non-supported software (WindowsXP), software that cannot natively enforce application whitelisting, alternative risk mitigations are in place. For example, while no native support for Windows XP from Microsoft exists, given the limited exposure of the Defence PKI environment due to the other existing logical and physical controls, the risk of exploitation of those vulnerabilities is greatly reduced.	
Recommendation 8: That the CDMC ensure that any delays in the implementation away from Windows XP is reflected within the SRMP and that alternative controls are investigated if the delay is to impact the next assessment period.				
No: 23	**Source:** ISM	**Control:** 282	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.10, 10.3
Service Providers MUST NOT use unevaluated products, unless the risks have been appropriately accepted and documented.				
Compliance	**Compliant**	**Rationale**	The use of the unevaluated products has been documented within the PKI SRMP and is included as part of the Moderated Risks that need to be accepted.	
No: 24	**Source:** ISM	**Control:** 291	**Applicability:** RA, CA, VA	**Framework sections:** 9.4, 9.8, 10.3

No	Source	Control	Applicability	Framework sections
Service Providers wishing to use an evaluated product in an unevaluated configuration MUST undertake a security risk assessment including: • the necessity of the unevaluated configuration; • testing of the unevaluated configuration in the Service Provider's environment; and • new vulnerabilities introduced due to the product being used outside of its evaluated configuration.				
Compliance	**Compliant**	**Rationale**	The use of the unevaluated configurations for evaluated products has been documented within the PKI SRMP and is included as part of the Moderated Risks that need to be accepted.	
No: 25	**Source:** GK	**Control:** GK	**Applicability:** RA, CA, VA	**Framework sections:** 9.4
Security risks deemed acceptable by a Service Provider MUST be formally accepted by the System Owner.				
Compliance	**Compliant**	**Rationale**	The process of accreditation includes the formal submission of the SRMP in the first instance the Defence PKI Policy Board, then the Service Owner and then the GKCA. The submission of the SRMP from Defence to the GKCA is deemed as an acceptance of the document.	

2.2.4 System Security Plan

No	Source	Control	Applicability	Framework sections
No: 26	**Source:** ISM	**Control:** 41	**Applicability:** RA, CA, VA	**Framework sections:** 9.5

No	Source	Control	Applicability	Framework sections
All systems MUST be covered by a System Security Plan.				
Compliance	**Compliant**	**Rationale**	The Australian Department of Defence Public Key Infrastructure System Security Plan (SSP) reviewed during this assessment indicated that all systems that are identified within the boundaries of the Gatekeeper Assessment and for Gatekeeper Accreditation are included within the DPKI SSP.	
No: 27	**Source:** ISM, PSPF	**Control:** 895, INFOSEC 5 & 6	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK 3 & 4), 9.5
Service Providers MUST select controls from the current version of the ISM to be included in the SSP based on the scope of the system with additional system specific controls being included as a result of the associated SRMP.				
Compliance	**Compliant**	**Rationale**	While the DPKI SSP does not explicitly list the specific ISM controls, the DPKI SSP refers to the ISM for stipulating the exact requirements.	
No: 28	**Source:** ISM	**Control:** 432	**Applicability:** RA, CA, VA	**Framework sections:** 9.5
Service Providers MUST specify in the SSP any authorisations, security clearances and briefings necessary for system access.				
Compliance	**Compliant**	**Rationale**	The DPKI SSP dictates these requirements under the *System Users* section.	

No	Source	Control	Applicability	Framework sections
No: 29	**Source:** GK	**Control:** GK	**Applicability:** RA, CA, VA	**Framework sections:** 9.5,
All server and workstation security objectives and mechanisms MUST be documented in the relevant SSP.				
Compliance	**Non-Compliant**	**Rationale**	The current *Security Objectives* section listed in the DPKI SSP does not specifically address server and workstation security objectives, as it relates to the objectives of securing the DPKI and CDMC as a whole.	
Recommendation 9: That the CDMC update the Security Objectives section of the DPKI SSP to include the objectives for the Workstations and Servers.				
No: 30	**Source:** ISM	**Control:** 580	**Applicability:** RA, CA, VA	**Framework sections:** 9.5
Service Providers MUST develop an event log strategy covering: • logging facilities including availability requirements and the reliable delivery of event logs to logging facilities; • the list of events associated with a system or software component to be logged; and • Event log protection and archival requirements.				
Compliance	**Non-Compliant**	**Rationale**	The level of detailed required by this Control is not explicitly stated within the current DPKI SSP. The list of events is specified within the *Audit/Accountability* section of the DPKI SSP with a description of nightly archival but no real description of protection.	
Recommendation 10: That the CDMC update the Audit/Accountability section of the DPKI SSP to include the ability to protect the logs. Recommendation 11: That the CDMC update the Audit/Accountability section of the DPKI SSP to include availability.				

No	Source	Control	Applicability	Framework sections
No: 31	**Source:** ISM	**Control:** 586	**Applicability:** RA, CA, VA	**Framework sections:** 9.5
Event logs MUST be protected from modification and unauthorised access, and whole or partial loss within the defined retention period.				
Compliance	**Compliant**	**Rationale**	The *Audit/Accountability* section (Page 25) of the DPKI SSP defines the retention period and that the logs must be protected.	
No: 32	**Source:** ISM	**Control:** 1405	**Applicability:** RA, CA, VA	**Framework sections:** 9.5
Service Providers MUST implement a secure centralised logging facility.				
Compliance	**Non-Compliant**	**Rationale**	The DPKI SSP does not specify or describe a centralised logging capability, nor is one implemented.	
Recommendation 12: That the CDMC initiate the planning phase to centralise the logging of events.				
No: 33	**Source:** ISM	**Control:** 1344	**Applicability:** RA, CA, VA	**Framework sections:** 9.5
Service Providers MUST ensure systems are configured to save event logs to the secure centralised logging facility.				
Compliance	**Non-Compliant**	**Rationale**	See Rationale for Control number 32.	
Recommendation 13: That once the CDMC implement a centralised logging capability, a reference that all systems will log to this location must be included within the DPKI SSP.				

2.2.5 Standard Operating Procedures

No	Source	Control	Applicability	Framework sections
No: 34	**Source:** ISM	**Control:** 123, 130, GK	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.9
Standard Operating Procedures for all personnel with access to systems MUST include the requirement to notify the ITSM: • of any cyber security incident as soon as possible after the cyber security incident is discovered, and • access to any data that they are not authorised to access.				
Compliance	**Non-Compliant**	**Rationale**	While policies such as the DPKI SSP and CDMC ICTSP state this, there was no specification of this requirement within the initial SOPs examined.	
Recommendation 14: That the CDMC draft a standard statement to be inserted into all current and future SOPs that specifies that users report all suspicious events to the CDMC Security Officer.				
No: 35	**Source:** ISM	**Control:** 322	**Applicability:** RA, CA, VA	**Framework sections:** 9.5
Service Providers MUST document SOPs for the reclassification and declassification of media and equipment.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology destruction, classification and registration of events including; Australian Communications-Electronic Security Instruction (ACSI) 24, ACSI 40 and ACSI 51.	
No: 36	**Source:** ISM	**Control:** 348	**Applicability:** RA, CA, VA	**Framework sections:** 9.5

No	Source	Control	Applicability	Framework sections
Service Providers MUST document SOPs for the sanitisation of media and equipment.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology destruction, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	
No: 37	**Source:** ISM	**Control:** 363	**Applicability:** RA, CA, VA	**Framework sections:** 9.5
Service Providers MUST document SOPs for the destruction of media and equipment.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology destruction, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	
No: 38	**Source:** ISM	**Control:** 313	**Applicability:** RA, CA, VA	**Framework sections:** 9.5
Service Providers MUST have a documented process for the disposal of media and equipment.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology destruction, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	

No	Source	Control	Applicability	Framework sections
No: 39	**Source:** ISM	**Control:** 374	**Applicability:** RA, CA, VA	**Framework sections:** 9.5
Service Providers MUST document SOPs for the disposal of media and equipment				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology destruction, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	
No: 40	**Source:** ISM	**Control:** 1082	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6
Service Providers MUST develop a policy governing the use of mobile devices.				
Compliance	**Compliant**	**Rationale**	Compliant – Mobile devices is covered from within the CDMC ICTSP for excluding devices brought into the facility. The policy for the use of mobile devices, particularly laptop devices, is covered within general Defence guidelines and does not require further specification for use within the Defence PKI environment.	

2.2.6 Physical & Environmental Security Plan

No	Source	Control	Applicability	Framework sections

No	Source	Control	Applicability	Framework sections
No: 41	**Source:** PSPF	**Control:** PHYSEC3	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK11), 9.6
Service Providers MUST prepare a Physical & Environmental Security Plan.				
Compliance	**Compliant**	**Rationale**	Each facility that operates and stores Defence PKI equipment is covered through a wider facility plans for that location. For example, the Defence PKI environment that is operated out of Defence Network Operations Centre (DNOC), is covered within the Physical & Environmental Security Plan for the DNOC and the wider HMAS Harman.	

2.2.7 Personnel Security Plan

No	Source	Control	Applicability	Framework sections
No: 42	**Source:** GK	**Control:** GK	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK), 9.7
Service Providers MUST implement a Personnel Security Plan.				
Compliance	**Compliant**	**Rationale**	Personnel Security is covered in-depth through a series of governance documents endorsed by general Defence and used to support staff actions within the Defence PKI environment.	

2.2.8 Vulnerability Management

No	Source	Control	Applicability	Framework sections
No: 43	**Source:** ISM	**Control:** 112	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.8
Service Providers MUST analyse any vulnerabilities to determine their potential impact on their PKI operations and determine appropriate mitigations or other treatments. Evidence of these mitigations and treatments MUST appear in the Service Provider's Information Security Documentation.				
Compliance	**Non-Compliant**	**Rationale**	The vulnerability assessment procedures or criteria is not demonstrated in the documentation for the control of risk in the environment. However, during a site visit, it was demonstrated the active Nagios scanning that is undertaken on the environment and the environment is regularly scanned as part of the DIE.	

No	Source	Control	Applicability	Framework sections
Recommendation 15: That the CDMC draft a SOP that incorporates the Nagios scanning that is undertaken within the environment as well as any external to DPKI testing that occurs.				
No: 44	**Source:** ISM	**Control:** 113	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.8
Service Providers MUST mitigate or otherwise treat identified vulnerabilities as soon as possible.				
Compliance	**Non-Compliant**	**Rationale**	Without the relevant controls and methods as specified within control 43, the enforcement of this control (44) cannot occur.	
Recommendation 15: That the CDMC draft a SOP that incorporates the Nagios scanning that is undertaken within the environment as well as any external to DPKI testing that occurs.				

2.2.9 Incident Response Plan

No	Source	Control	Applicability	Framework sections
No: 45	**Source:** ISM, PSPF	**Control:** 43, PHYSEC7	**Applicability:** RA, CA, VA	**Framework sections:** 7(GK12), 9.9
Service Providers MUST develop, maintain and implement an Incident Response Plan and supporting procedures.				
Compliance	**Non-Compliant**	**Rationale**	While Incident Response has been categorised into the Disaster Recovery and Business Continuity Plan (DRBCP), the DRAFT PKI Incident Response Plan (IRP) is an explicit plan and is inclusive enough of incident response to provide sufficient coverage as specified within later Gatekeeper requirements.	

No	Source	Control	Applicability	Framework sections
Recommendation 16: That at the conclusion of the Gatekeeper Accreditation process, the DRAFT PKI IRP be accepted as final and versioned accordingly.				
No: 46	**Source:** ISM	**Control:** 58	**Applicability:** RA, CA, VA	**Framework sections:** 9.9
Service Providers MUST include, as a minimum, the following content in their IRP: • broad guidelines on what constitutes a cyber security incident • the minimum level of cyber security incident response and investigation training for users and system administrators • the authority responsible for initiating investigations of a cyber security incident • the steps necessary to ensure the integrity of evidence supporting a cyber security incident • the steps necessary to ensure that critical systems remain operational • how to formally report cyber security incidents.				
Compliance	**Compliant**	**Rationale**	While some of the categories have some coverage within the DRBCP, SSP and ICTSP, the requirements are met within the PKI IRP.	
No: 47	**Source:** ISM	**Control:** 131	**Applicability:** RA, CA, VA	**Framework sections:** 9.9
Service Providers MUST document procedures for dealing with data spills in their IRP.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	Data spills, i.e. infiltration of material from the PKI High to PKI Low are referenced within in the PKI IRP and primarily deals with the unintended exposure of Certificates on HSMs and not classified material.	
No: 48	**Source:** ISM	**Control:** 132	**Applicability:** RA, CA, VA	**Framework sections:** 9.9
Service Providers MUST treat any data spillage as an cyber security incident, and follow the IRP to mitigate the incident.				
Compliance	**Compliant**	**Rationale**	Data spills are referenced within the PKI IRP.	
No: 49	**Source:** ISM	**Control:** 129	**Applicability:** RA, CA, VA	**Framework sections:** 9.9
When a data spill occurs Service Providers MUST assume that the information has been compromised and report the details of the data spill to ASD.				
Compliance	**Compliant**	**Rationale**	Data spills are referenced within the PKI IRP.	
No: 50	**Source:** ISM	**Control:** 133	**Applicability:** RA, CA, VA	**Framework sections:** 9.9
When a data spill occurs, Service Providers MUST report the details of the data spill to the information owner.				
Compliance	**Compliant**	**Rationale**	Data spills are referenced within the PKI IRP.	

No	Source	Control	Applicability	Framework sections
No: 51	**Source:** ISM	**Control:** 139, GK	**Applicability:** RA, CA, VA	**Framework sections:** 9.9
Service Providers MUST report cyber security incidents to ASD and the Gatekeeper Competent Authority.				
Compliance	**Non-Compliant**	**Rationale**	While the DRBCP does reference reporting to DSD under the ISIDRAS scheme, listing the old agency name and old reporting mechanism, it does not reference reporting to the Gatekeeper Competent Authority.	
Recommendation 17: That the CDMC updates the DRBCP to reference the ASD Cyber Security Incident Reporting (CSIR) reporting mechanism. Recommendation 18: That the CDMC updates the DRBCP to reference reporting cyber security events to the Gatekeeper Competent Authority. Recommendation 19: That the CDMC ensures that the new IRP reference the ASD CSIR reporting mechanism and the Gatekeeper Competent Authority.				
No: 52	**Source:** ISM	**Control:** 142	**Applicability:** RA, CA, VA	**Framework sections:** 9.9, 9.10
Service Providers MUST notify all communications security custodians of any suspected loss or compromise of keying material.				
Compliance	**Compliant**	**Rationale**	It is expected that central PKI authorities within the Defence PKI trust chain, such as RA and sub-ordinate CAs, would be notified of events when they occur. Relying parties would be communicated through CRL and OCSP revocation information. It is also clearly documented within the CPs and CPS.	

No	Source	Control	Applicability	Framework sections
No: 53	**Source:** ISM	**Control:** 141	**Applicability:** RA, CA, VA	**Framework sections:** 9.9
Service Providers that outsource their ICT services and functions to a third party MUST ensure that the third party consults with them when a cyber security incident occurs.				
Compliance	**Non-Compliant**	**Rationale**	Due to the DRAFT IRP, there is no indication of notifications from the Defence vendors that support not just the PKI environment but those vendors that support the Defence Information Environment (DIE).	
Recommendation 20: That the created CDMC IRP reference the notification process of vendors to the CDMC of detected or suspected vulnerabilities within the CDMC networks and equipment.				

2.2.10 Cryptographic Key Management Plan

No	Source	Control	Applicability	Framework sections
No: 54	**Source:** ISM, GK	**Control:** 511, GK	**Applicability:** RA, CA, VA	**Framework sections:** 9.9
The Cryptographic Key Management Plan MUST be consistent with the criticality and classification of the information to be protected.				
Compliance	**Compliant**	**Rationale**	The KMP is commensurate with the level of information protected by the Defence PKI.	

No	Source	Control	Applicability	Framework sections
No: 55	**Source:** ISM	**Control:** 504	**Applicability:** RA, CA, VA	**Framework sections:** 9.9
Service Providers MUST conduct an inventory of cryptographic system material: • on handover/takeover of administrative responsibility for the cryptographic system • on change of personnel with access to the cryptographic system • at least annually.				
Compliance	**Compliant**	**Rationale**	The *Accounting* section of the PKI KMP covers the requirements for inventory inspection and review. The guidance for meeting this requirement is governed by the SSP, including the requirements for media and associated event accounting.	
No: 56	**Source:** GK	**Control:** GK	**Applicability:** RA, CA, VA	**Framework sections:** 9.10, 10.3
Service Providers MUST use accredited PKI software and hardware products that have undergone a security evaluation through an ASD recognised evaluation program.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use Verizon Business software UniCERT 5.3.4.1 which has undergone Common Criteria certification to the level of EAL 4.	

No	Source	Control	Applicability	Framework sections
No: 57	**Source:** ISM	**Control:** 280	**Applicability:** RA, CA, VA	**Framework sections:** 9.4, 9.10
Service Providers MUST select PKI software and hardware products with the required security functionality that has completed an ASD approved Protection Profile evaluation in preference to one that has completed an EAL–based evaluation. If Service Providers select a PKI software and hardware products that has not completed an evaluation, documenting this decision, assessing the security risks and accepting these risks ensures the decision is appropriate for an Service Provider's business requirements and risk profile.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use Verizon Business software UniCERT 5.3.4.1 which has undergone Common Criteria certification to the level of EAL 4, however this was not to a Protection Profile.	
No: 58	**Source:** ISM	**Control:** 463	**Applicability:** RA, CA, VA	**Framework sections:** 9.10, 10.3
Service Providers MUST check PKI software and hardware product evaluation documentation, where available, to determine any product specific requirements.				
Compliance	**Compliant**	**Rationale**	All product specific requirements have been met.	
No: 59	**Source:** ISM	**Control:** 464	**Applicability:** RA, CA, VA	**Framework sections:** 9.10, 10.3
Service Providers MUST comply with all PKI software and hardware product specific requirements outlined in product evaluation documentation.				
Compliance	**Compliant**	**Rationale**	The incorporation of the evaluated HSM increases the security profile of the solution.	

No	Source	Control	Applicability	Framework sections
No: 60	**Source:** ISM	**Control:** 503	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers MUST be able to readily account for all transactions relating to cryptographic system material, including identifying hardware and software that was issued with the cryptographic equipment and materials, when they were issued and where they were issued.				
Compliance	**Compliant**	**Rationale**	All transactions for the various elements within the PKI environment are logged and signed for protection.	
No: 61	**Source:** ISM	**Control:** 455	**Applicability:** CA	**Framework sections:** 6.4, 9.10
Where practical, cryptographic products MUST provide a means of data recovery to allow for circumstances where the encryption key is unavailable due to loss, damage or failure.				
Compliance	**Compliant**	**Rationale**	The Key Archive Server (KAS), as described within the PKI KMP, is the primary source for the secure archival purpose of users private keys.	

2.2.11 Change Management

No	Source	Control	Applicability	Framework sections
No: 62	**Source:** ISM, GK	**Control:** 1211, GK	**Applicability:** RA, CA, VA	**Framework sections:** 9.11
Service Providers MUST have a formal change management process in place.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	A formal change process is in place with the PKI Configuration Control Board and the Defence Information Environment CAB being listed as the relevant authorities.	
No: 63	**Source:** ISM	**Control:** 117	**Applicability:** RA, CA, VA	**Framework sections:** 9.11
The change management process MUST define appropriate actions to be followed before and after urgent or emergency changes are implemented.				
Compliance	**Non-Compliant**	**Rationale**	Urgent or emergency changes are not referenced within the *Configuration and Change Control* section of the CDMC ICTSP nor the *Configuration Management* section of the PKI SSP.	
Recommendation 21: That the CDMC ICTSP and the PKI SSP be updated to include a specific reference to the emergency change management procedures.				
No: 64	**Source:** ISM	**Control:** 115	**Applicability:** RA, CA, VA	**Framework sections:** 9.1, 9.3, 9.4, 9.5, 9.6, 9.11
Service Providers MUST ensure that for routine and urgent changes: • the change management process is followed; • the proposed change is approved by the relevant authority; • any proposed change that could impact the security of a system is submitted to the accreditation authority for approval; and • all relevant Information Security Documentation is updated to reflect the change.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	The documented process specifies that change management is followed, that approval exists, accreditation status is considered and that the relevant documents be examined for impact and updating.	
No: 65	**Source:** ISM, GK	**Control:** 809, GK	**Applicability:** RA, CA, VA	**Framework sections:** 5.6, 9.3, 9.4, 9.5, 9.11
When a configuration change impacts the security of a system, and is subsequently assessed as having changed the overall security risk for the system, the system MUST undergo reaccreditation.				
Compliance	**Compliant**	**Rationale**	Multiple documentation sources, such as the CDMC SSP, the CDMC ICTSP and the DPKI SRMP refer to this requirement to notify the user of this requirement.	

2.2.12 Disaster Recovery and Business Continuity Plan

No	Source	Control	Applicability	Framework sections
No: 66	**Source:** PSPF, GK	**Control:** GOV11, GK	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK5), 9.12
Service Providers MUST develop a Disaster Recovery Business Continuity Plan.				
Compliance	**Compliant**	**Rationale**	A Disaster Recovery and Business Continuity Plan have been developed for the Defence PKI.	

No	Source	Control	Applicability	Framework sections
No: 67	**Source:** ISM, PSPF	**Control:** 0118, GOV11	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK7), 9.12
Service Providers MUST determine availability requirements for their systems and implement appropriate security measures to support these requirements.				
Compliance	**Compliant**	**Rationale**	It has been sufficiently demonstrated that availability identified as a strong requirement for the PKI facility and therefor has been deployed in a manner that ensures the ongoing availability of the system.	

2.3 Certification Practice Statement and Certificate Policies

No	Source	Control	Applicability	Framework sections
No: 68	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 6.4
The Certification Practice Statement and Certificate Policy MUST conform to the document framework as described in RFC3647.				
Compliance	**Compliant**	**Rationale**	All reviewed Certificate Policies and the Certification Practice Statement was reviewed and is considered in compliance with the framework as described in RFC3647.	

No	Source	Control	Applicability	Framework sections
No: 69	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 6.4
Security objectives identified in the Security Policy MUST be reflected in the Certification Practice Statement and as appropriate all Certificate Policies.				
Compliance	**Compliant**	**Rationale**	The security objectives of the DPKI Certification Practice Statement meet the Security Policy.	
No: 70	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 6.4
The PKI MUST perform its operations to manage the life cycle of the certificates it issues in compliance with its CPS.				
Compliance	**Compliant**	**Rationale**	The management as referenced in the documentation manages the certificates in the lifecycle of the PKI.	
No: 71	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 6.4, 6.8
All certificates issued by the PKI MUST be issued in compliance with a published CP.				
Compliance	**Compliant**	**Rationale**	All certificates issued within the Defence PKI are issued with a corresponding Certificate Profile.	
No: 72	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 6.4

No	Source	Control	Applicability	Framework sections
A CA MUST ensure every Certificate Policy under which digital certificates are issued clearly specify the Level of Assurance associated with the digital certificates.				
Compliance	**Compliant**	**Rationale**	All Certificate Policies reviewed as part of this assessment clearly articulate the associated Level of Assurance with that certificate, through level of assurance, such as the Level of Assurance Mapping in Appendix D of the Defence Individual – Hardware Certificates (High Assurance).	
No: 73	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 6.4
The Certificate Revocation List MUST conform to the X.509 version 2 profile as described in RFC5280.				
Compliance	**Compliant**	**Rationale**	The Certificate Revocation List published on the Defence PKI website and examined all stipulated as being V2 under the Version field.	
No: 74	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 6.4
If supported Online Certificate Status Protocol responses MUST conform to RFC5019.				
Compliance	**Compliant**	**Rationale**	The Defence PKI utilises the Tumbleweed Validation Authority Server Version 4.11.1 which utilises RFC5019.	

No	Source	Control	Applicability	Framework sections
No: 75	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 6.4
Where CRLs are used, new CRLs MUST be generated at regular scheduled intervals and published CRLs have a suitable validity period.				
Compliance	**Compliant**	**Rationale**	CRL's are published within the intervals as documented and specified within each of the various CPs, either with a monthly, fortnightly or weekly schedule. This was validated by the IRAP assessor by accessing over the period of the assessment the Defence PKI website (www.defence.gov.au/pki) and downloading the latest CRL's and verifying that they had been updated when it was specified the CRL would.	
No: 76	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 6.4, 6.8
CRLs MUST be published to a location that is accessible by any applications that use the certificates.				
Compliance	**Compliant**	**Rationale**	All Defence CRL's are available from the Defence PKI website: http://www.defence.gov.au/pki/	
No: 77	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 6.4
The location where certificates and CRLs are published MUST have restricted write access so that only valid certificates and CRLs issued by approved PKI entities can be published by an authorised person or process.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	After reviewing the network architecture and access controls mechanisms in place, the evidence implies that this condition is being met.	
No: 78	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 6.4, 6.8
The PKI MUST publish as much of its documented CPS as necessary to alloy a relying party to make informed decision on trust.				
Compliance	**Compliant**	**Rationale**	The full CPS is published to the Defence website to enable relying parties to determine if the security aspects of the Defence PKI are suitable for them to rely on the certificates.	

3 Physical Controls

As part of the Gatekeeper IRAP assessment, a total of 51 Physical controls were assessed, with the Defence PKI deemed compliant with all 51 Physical controls.

3.1 Facilities

No	Source	Control	Applicability	Framework sections
No: 79	**Source:** ISM, PSPF	**Control:** 865, PHYSEC4 & 6	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK11), 6.3, 8.2, 9.6, 10.4
Service Providers MUST ensure that any facility containing a PKI system, (including a mobile device or removable media as the case may be for remote RAs) meet the requirements in the Australian Government Physical Security Management Protocol.				
Compliance	**Compliant**	**Rationale**	Existing certifications are not to the specifications as listed in the Australian Government Physical Security Management Protocol. However, as per DSM Part 2:60.67 and Table 2:60-3, as both facilities are Accredited Secure Areas with no significant environmental change occurring, the areas are classed now as Zone 4. The CDMC SO validates the security of Canberra centric RAs and has a roaming schedule of interstate visits to validate the physical security of RAs.	

No	Source	Control	Applicability	Framework sections
Recommendation 22: That once CDMC PKI POC is relocated to its new facility, the CDMC must engage Defence Security and Vetting Service to assess and rate the facility under the current Australian Government Physical Security Management Protocol if the new facility has not been already physically accredited. Recommendation 23: That the CDMC PKI engage Defence Security and Vetting Service to assess and rate the BOC facility within HMAS Harman under the current Australian Government Physical Security Management Protocol or validate that the BOC facility is covered by an existing physical accreditation to the new protocol. Recommendation 24: That on the Defence Security and Vetting Service assessing the POC and BOC facility under the current Australian Government Physical Security Management Protocol, the CDCM SSP be updated to include the new physical certifications.				
No: 80	**Source:** PSPF, GK	**Control:** PHYSEC6, GK	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK11), 8.2, 9.2, 9.6, 10.4
PKI servers MUST be housed within a secure data centre and have restrictive physical access controls to ensure only authorized and trained PKI administrator have access.				
Compliance	**Compliant**	**Rationale**	Multiple barriers prevent access to the PKI facility, such as guarded entrance, CCTV coverage of hallways and work areas, multiple controlled entrances and no lone zones are enforced.	
No: 81	**Source:** ISM	**Control:** 813	**Applicability:** RA, CA, VA	**Framework sections:** 9.4, 9.5, 9.6
Service Providers MUST NOT leave server rooms, communications rooms and security containers or rooms in an unsecured state.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	No evidence was every observed that this was the case and existing controls and procedures, such as those contained within the DSM Part2:4 *Facilities and ICT Systems Security Accreditation* determine the likelihood of this occurring as being low.	
No: 82	**Source:** ISM	**Control:** 1074	**Applicability:** RA, CA, VA	**Framework sections:** 9.4, 9.5, 9.6
Service Providers MUST ensure that keys or equivalent access mechanisms to server rooms, communications rooms and security containers or rooms are appropriately controlled and audited.				
Compliance	**Compliant**	**Rationale**	Access is recorded through the use of swipe keys with guests registered in the Visitors Register. As equipment is stored within a No Lone Zone, access is restricted to at least two individuals at any one time. Access to the environment also requires the removal of smart and mobile devices, including phones. Cameras are also not permitted within the server areas.	
No: 83	**Source:** ISM	**Control:** 150	**Applicability:** RA, CA, VA	**Framework sections:** 9.6, 10.4
Where a Service Provider uses a NLZ, this area MUST: • be suitably sign-posted; and • have all entry and exit points appropriately secured.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	The NLZ within the CDMC Deakin facility is enforced through sufficient physical and logical controls and the single entry point is sign posted to the fact that the area is a NLZ.	
No: 84	**Source:** ISM, PSPF	**Control:** 1053, INFOSEC 6, & 7, PHYSEC 6	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5, 7, 10.4
Service Providers MUST ensure that servers and network devices are secured in either security containers or rooms as specified in the Australian Government Physical Security Management Protocol.				
Compliance	**Compliant**	**Rationale**	While it is noted that the servers and network devices are secured with a specifically dedicated room that is accessed through a No-Lone-Zone, the specification of the server room has not been validated under the current Australian Government Physical Security Management Protocol. However, as per DSM Part 2:60.67 and Table 2:60-3, as both facilities are Accredited Secure Areas with no significant environmental change occurring, the areas are classed now as Zone 4.	
Recommendation 25: That once CDMC PKI POC is relocated to its new facility, the CDMC must engage Defence Security and Vetting Service to assess and rate the facility under the current Australian Government Physical Security Management Protocol. Recommendation 26: That the CDMC PKI engage Defence Security and Vetting Service to assess and rate the BOC facility within HMAS Harman under the current Australian Government Physical Security Management Protocol or validate that the BOC facility is covered by an existing physical accreditation to the new protocol.				

3.2 Infrastructure

No	Source	Control	Applicability	Framework sections
No: 85	**Source:** ISM	**Control:** 1304	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5, 9.7
Default network device accounts MUST be disabled, renamed or have their passphrase changed.				
Compliance	**Compliant**	**Rationale**	The *ICT System Access Controls* section of the CDMC ICTSP specifies the requirements around default or privileged access accounts.	
No: 86	**Source:** ISM	**Control:** 1383	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5, 9.6, 9.7
Service Providers MUST ensure that all administrative infrastructure including, but not limited to, privileged workstations and jump boxes are hardened appropriately.				
Compliance	**Compliant**	**Rationale**	All administrative computing infrastructure is built from predefined and approved Defence sourced images that are appropriately hardened.	
No: 87	**Source:** ISM	**Control:** 1388	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5, 9.6, 9.7

No	Source	Control	Applicability	Framework sections
Service Providers MUST ensure that jump boxes are prevented from communicating to assets and sending and receiving traffic not related to administrative purposes.				
Compliance	**Compliant**	**Rationale**	Jump boxes are only used for the purpose of communicating to the relevant CDMC device and cannot be used for non-administrative activities.	
No: 88	**Source:** ISM	**Control:** 1296	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5, 9.6, 10.4
Adequate physical measures MUST be provided to protect network devices, especially those in public areas, from physical damage or unauthorised access.				
Compliance	**Compliant**	**Rationale**	No network devices exist in public locations due to the facilities that house the service.	
No: 89	**Source:** GK	**Control:** GK	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5, 9.6, 9.10
Service Providers MUST use a firewall as part of their traffic flow filter.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	Firewalls are in place (Common Criteria EAL4 rated) to ensure communication paths are secured. The Defence PKI environment is also a segment within the Defence Information Environment (DIE) that is protected by the Defence High Availability Internet Gateway Service (HAIGS).	
No: 90	**Source:** ISM	**Control:** 639	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5, 9.6, 9.10
Service Providers MUST use a firewall between networks of different security domains.				
Compliance	**Compliant**	**Rationale**	Common Criteria EAL4 rated firewalls are in place however it is used as a delineation point between inside and external to the PKI environment as both environments are the same classification.	
No: 91	**Source:** ISM	**Control:** 1194	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5, 9.6
The requirement to use a firewall as part of gateway infrastructure MUST be met by both parties independently; shared equipment does not satisfy the requirements of both parties.				
Compliance	**Compliant**	**Rationale**	The gateway environment only services one environment and is not dependent on multiple parties.	

3.3 Equipment & Media

No	Source	Control	Applicability	Framework sections
No: 92	**Source:** ISM	**Control:** 337	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5, 9.6
Service Providers MUST NOT use media with a system that is not accredited to process, store or communicate the information on the media.				
Compliance	**Compliant**	**Rationale**	All media is classified at the correct level to be used within the relevant system.	
No: 93	**Source:** ISM, PSPF	**Control:** 294, INFOSEC 6 & 7	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK 10), 9.4, 9.5, 9.6
Service Providers MUST clearly label all ICT equipment capable of storing information, with the exception of High Assurance products, with the appropriate protective marking.				
Compliance	**Compliant**	**Rationale**	IAW the *Physical Security* section of the CDMC ICTSP, all hardware will be labelled with the relevant security classification.	
No: 94	**Source:** ISM, PSPF	**Control:** 323, INFOSEC 6 & 7	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK10), 9.3, 9.4, 9.5, 9.6
Service Providers MUST classify media to the highest classification stored on the media since any previous reclassification.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	All media is classified to the required level of the system that is connected to and will be reclassified to a higher classification in the event that this occurs.	
No: 95	**Source:** ISM, PSPF	**Control:** 325, INFOSEC 6 & 7	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK10), 9.3, 9.4, 9.5, 9.6
Service Providers MUST classify any media connected to a system the same sensitivity or classification as the system, unless either: • the media is read-only • the media is inserted into a read-only device • the system has a mechanism through which read-only access can be assured.				
Compliance	**Compliant**	**Rationale**	All media is classified to the required level of the system that is connected to.	
No: 96	**Source:** ISM	**Control:** 333	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6
Service Providers MUST ensure that classification of all media is easily visually identifiable.				
Compliance	**Compliant**	**Rationale**	IAW the *Physical Security* section of the CDMC ICTSP, all media is clearly labelled with the relevant security classification.	

No	Source	Control	Applicability	Framework sections
No: 97	**Source:** ISM, PSPF	**Control:** 334	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6, 9.7
When using non-textual protective markings for media due to operational security reasons, Service Providers MUST document the labelling scheme and train personnel appropriately.				
Compliance	**Compliant**	**Rationale**	IAW the *Physical Security* section of the CDMC ICTSP, all media is clearly labelled with the relevant security classification and does not implement non-textual protective marking.	
No: 98	**Source:** ISM, PSPF	**Control:** 161, INFOSEC 6 & 7	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK 10), 9.4, 9.5, 9.6, 10.4
Service Providers MUST ensure that ICT equipment and media with sensitive or classified information is secured in accordance with the requirements for storing sensitive or classified information in the Australian Government Physical Security Management Protocol.				
Compliance	**Compliant**	**Rationale**	While it is noted that the servers and network devices are secured with a specifically dedicated room that is accessed through a No-Lone-Zone, the specification of the server room has not been validated under the current Australian Government Physical Security Management Protocol. However, as per DSM Part 2:60.67 and Table 2:60-3, as both facilities are Accredited Secure Areas with no significant environmental change occurring, the areas are classed now as Zone 4.	

No	Source	Control	Applicability	Framework sections
Recommendation 25: That once CDMC PKI POC is relocated to its new facility, the CDMC must engage Defence Security and Vetting Service to assess and rate the facility under the current Australian Government Physical Security Management Protocol. Recommendation 26: That the CDMC PKI engage Defence Security and Vetting Service to assess and rate the BOC facility within HMAS Harman under the current Australian Government Physical Security Management Protocol or validate that the BOC facility is covered by an existing physical accreditation to the new protocol.				
No: 99	**Source:** ISM	**Control:** 832	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers MUST encrypt media with at least an ASD Approved Cryptographic Algorithm if it is to be transferred through an area not certified and accredited to process the sensitivity or classification of the information on the media.				
Compliance	**Compliant**	**Rationale**	All media to be transferred that is required to be encrypted is done so with an AACA.	
No: 100	**Source:** ISM	**Control:** 418	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5
Authentication information MUST be stored separately to a system to which it grants access.				
Compliance	**Compliant**	**Rationale**	Authentication information includes the identity that is contained within the administrators SmartCard is authenticated via a separate AD structure.	

No	Source	Control	Applicability	Framework sections
No: 101	**Source:** ISM	**Control:** 1402	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5
Authentication information stored on a system MUST be protected.				
Compliance	**Compliant**	**Rationale**	Information on authentication systems is protected through network separation mechanisms.	
No: 102	**Source:** ISM	**Control:** 462	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6, 9.10
When a user authenticates to ICT equipment storing encrypted information, it MUST be treated in accordance with the original sensitivity or classification of the equipment.				
Compliance	**Compliant**	**Rationale**	The systems are replicated through the two classifications to ensure that elements on the Defence PKI High are treated as a SECRET system and the Defence PKI Low classified system is held in accordance with its classification.	
No: 103	**Source:** ISM, PSPF	**Control:** 159, INFOSEC 6 & 7	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK 10), 9.4, 9.5, 9.6
Service Providers MUST account for all sensitive and classified ICT equipment and media.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	All equipment is accounted for through the application of musters that are undertaken by the CDMC SO.	
No: 104	**Source:** ISM, PSPF	**Control:** 293, INFOSEC 3 & 7	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK 10), 9.4, 9.5, 9.6
Service Providers MUST classify ICT equipment based on the sensitivity or classification of information for which the equipment and any associated media in the equipment are approved for processing, storing or communicating.				
Compliance	**Compliant**	**Rationale**	The Defence PKI environment has been separated into two separate domains to explicitly handle the two different classifications that the service operates in.	
No: 105	**Source:** ISM	**Control:** 306	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5, 9.6, 9.7
If an uncleared technician is used to undertake maintenance or repairs of ICT equipment, the technician MUST be escorted by someone who: • is appropriately cleared and briefed; • takes due care to ensure that sensitive or classified information is not disclosed; • takes all responsible measures to ensure the integrity of the equipment; and, • has the authority to direct the technician.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	All Defence PKI repairs are undertaken under the supervision of a suitably skilled staff member who understands the elements of activity being undertaken.	
No: 106	**Source:** ISM	**Control:** 310	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6
Service Providers having ICT equipment maintained or repaired off-site MUST ensure that the physical transfer, processing and storage requirements are appropriate for the sensitivity or classification of the equipment and that procedures are complied with at all times.				
Compliance	**Compliant**	**Rationale**	The *Maintenance and Disposal* section of the PKI SSP specifies the requirements in the event of off-site maintenance that meet this control.	
No: 107	**Source:** ISM, PSPF	**Control:** 329, INFOSEC 6 & 7	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK10), 9.3, 9.4, 9.5, 9.6
Service Providers declassifying media MUST ensure that: • the media has been reclassified to an unclassified level either through an administrative decision, sanitisation or destruction • a formal administrative decision is made to release the unclassified media, or its waste, into the public domain.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology destruction, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	

No	Source	Control	Applicability	Framework sections
No: 108	**Source:** ISM, PSPF	**Control:** 330, INFOSEC 6 & 7	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK10), 9.3, 9.4, 9.5, 9.6
Service Providers wishing to reclassify media to a lower classification MUST ensure that: • the reclassification of all information on the media has been approved by the originator, or the media has been appropriately sanitised or destroyed. • a formal administrative decision is made to reclassify the media.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology destruction, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	
No: 109	**Source:** ISM, PSPF	**Control:** 331, INFOSEC 6 & 7	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK10), 9.3, 9.4, 9.5, 9.6
Media MUST be reclassified if: • information copied onto the media is of a higher classification than the sensitivity or classification of the information already on the media; and • information contained on the media is subjected to a classification upgrade.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology destruction, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	

No	Source	Control	Applicability	Framework sections
No: 110	**Source:** ISM	**Control:** 375	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6
Service Providers MUST declassify all media prior to disposing of it into the public domain.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology destruction, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	
No: 111	**Source:** ISM, PSPF	**Control:** 311, INFOSEC 6 & 7	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK10), 9.3, 9.4, 9.5, 9.6
Service Providers MUST, when disposing of ICT equipment containing classified media, sanitise the equipment by either: • sanitising the media within the equipment; • removing the media from the equipment and disposing of it separately; or • destroying the equipment in its entirety.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology destruction, sanitisation, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	

No	Source	Control	Applicability	Framework sections
No: 112	**Source:** ISM	**Control:** 350	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6
Service Providers MUST destroy the following media types prior to disposal, as they cannot be sanitised: • microform (i.e. microfiche and microfilm) • optical discs • printer ribbons and the impact surface facing the platen • programmable read-only memory • read-only memory • faulty or other types of media that cannot be successfully sanitised.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology destruction, sanitisation, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	
No: 113	**Source:** ISM	**Control:** 364	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6
To destroy media, Service Providers MUST either: • break up the media • heat the media until it has either burnt to ash or melted • degauss the media.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology destruction, sanitisation, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	
No: 114	**Source:** ISM	**Control:** 1217	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6
When disposing of ICT equipment, Service Providers MUST remove labels and markings indicating the classification, code words, caveats, owner, system or network name, or any other marking that can associate the equipment with its original use.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology disposal, destruction, sanitisation, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	
No: 115	**Source:** ISM	**Control:** 1347	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6
Where volatile media has undergone sanitisation but sensitive or classified information persists on the media, Service Providers MUST destroy the media, and handle the media at the sensitivity or classification of the information it contains until it is destroyed.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology disposal, destruction, sanitisation, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	

No	Source	Control	Applicability	Framework sections
No: 116	**Source:** ISM, PSPF	**Control:** 370, PERSEC 1, PERSEC 4, INFOSEC 6	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK8 & 10), 9.3, 9.4, 9.5, 9.6
Service Providers MUST perform the destruction of media under the supervision of at least one person cleared to the classification of the media being destroyed.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology disposal, destruction, sanitisation, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	
No: 117	**Source:** ISM, PSPF	**Control:** 371, PERSEC 1, PERSEC 4, INFOSEC 6	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK8 & 10), 9.3, 9.4, 9.5, 9.6
The person supervising the destruction of the media MUST: • supervise the handling of the material to the point of destruction; and • ensures that the destruction is successfully completed.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology disposal, destruction, sanitisation, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	
No: 118	**Source:** ISM	**Control:** 378	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6

No	Source	Control	Applicability	Framework sections
Service Providers MUST dispose of media in a manner that does not draw undue attention to its previous sensitivity or classification.				
Compliance	**Compliant**	**Rationale**	The Defence PKI facility use a combination of Defence instructions for the coverage of media and technology disposal, destruction, sanitisation, classification and registration of events including; ACSI 24, ACSI 40 and ACSI 51.	
No: 119	**Source:** ISM, GK	**Control:** 336, GK	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6
Service Providers MUST register all removable media with a unique identifier in an appropriate register (e.g. removable media register).				
Compliance	**Compliant**	**Rationale**	All removable media is assigned a unique identifier (with a physical form completed) and is itemised in a register (a physical hardcopy listing) stored within the POC Operations room. [Sited during the site visit that occurred on the 23rd February 2016]	
Recommendation 27: That the CDMC PKI operations team complete a copy of the Register (not the individual physical forms) for storage within the BOC for the purpose of remediation in case of loss of the POC. Recommendation 28: That the CDMC PKI operations team investigate creating an electronic register for such items, such as database register, that is retained in a centralised location that could be accessed from either the POC or BOC.				

3.4 Mobile Devices[1]

No	Source	Control	Applicability	Framework sections
No: 120	**Source:** ISM	**Control:** 864	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5, 9.7
Service Providers MUST prevent personnel from disabling security functions on a mobile device once provisioned.				
Compliance	**Compliant**	**Rationale**	Security controls prevent the ability of personnel from disabling any functions that are required for the service of that mobile device.	
No: 121	**Source:** ISM	**Control:** 1085	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5, 9.6
Service Providers using mobile devices to communicate sensitive or classified information over public network infrastructure MUST use encryption approved for communicating such information over public network infrastructure.				
Compliance	**Compliant**	**Rationale**	Suitable encryption methods are used over the relevant WAN environments to enforce this control, with applied protocols used to separate PKI information from the network traffic.	
No: 122	**Source:** ISM	**Control:** 870	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6

[1] The context for this section is two-fold; 1) the use of mobile devices by a Service Provider and, 2) Registration Authorities that support mobile identity proofing capabilities

No	Source	Control	Applicability	Framework sections
Service Providers MUST ensure mobile devices are carried in a secured state when not being actively used.				
Compliance	**Compliant**	**Rationale**	All Defence devices are transported in a secure manner as per Defence policy, dependant on the classification of the system involved.	
No: 123	**Source:** ISM	**Control:** 1087	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5, 9.6
When travelling with mobile devices and media, personnel MUST retain control over them at all times, this includes not placing them in checked-in luggage or leaving them unattended for any period of time.				
Compliance	**Compliant**	**Rationale**	All Defence devices are transported in a secure manner as per Defence policy, dependant on the classification of the system involved.	
No: 124	**Source:** ISM	**Control:** 871	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6
When in use mobile devices MUST be kept under continual direct supervision.				
Compliance	**Compliant**	**Rationale**	Mobile devices are assigned to the relevant user.	

No	Source	Control	Applicability	Framework sections
No: 125	**Source:** ISM	**Control:** 693	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6
Service Providers permitting personnel to access or store sensitive information using non-Service Provider owned mobile devices MUST implement technical controls to enforce the separation of sensitive information from personnel information.				
Compliance	**Compliant**	**Rationale**	Non-Service Provider devices are not allowed.	
No: 126	**Source:** ISM	**Control:** 1200	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6
If using Bluetooth on a mobile device, Service Providers MUST ensure both pairing devices uses Bluetooth version 2.1 or later.				
Compliance	**Compliant**	**Rationale**	Bluetooth is not enabled.	

4 Logical Controls

As part of the Gatekeeper IRAP assessment, a total of 89 Logical controls were assessed, with the Defence PKI deemed compliant with 72 of those 89 Logical controls. Seventeen (17) Logical controls were deemed non-compliant, with sixteen having a severity rating of Partial and one having a severity rating of Major.

4.1 Strategies to Mitigate Targeted Cyber Intrusions (Top 4)[2]

No	Source	Control	Applicability	Framework sections
No: 127	**Source:** ISM, PSPF, GK	**Control:** 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Service Providers, at a minimum, MUST implement the controls indicated in the following table on all PKI-related systems. Note: Some controls are duplicated between 'patch applications' and 'patch operating system' as they satisfy both strategies.				
Compliance	**Non-Compliant**	**Rationale**	The management console operating system, Windows XP, is no longer a supported platform. Defence however has initiated additional vendor support from Microsoft to continue. However, this software should still be considered not supported, as vulnerabilities within the application layer may have no applicable patches that are provided to prevent presently discovered vulnerabilities within the operating systems.	

[2] For Linux based systems use the ASD publication *The Top 4 in a Linux Environment*

No	Source	Control	Applicability	Framework sections
Recommendation 29: That the CDMC PKI support infrastructure be an immediate candidate for the replacement of Windows XP. Recommendation 30: That the CDMC be allowed to implement their own updated SOE to upgrade PKI support infrastructure independent of the replacement of Windows XP project.				

TOP 4 CONTROLS	
Mitigation strategy	**ISM Control numbers**
Application whitelisting	0843, 0846, 0955, 1391, 1392
Patch applications	0300, 0303, 0304, 0940, 0941, 1143, 1144,
Patch operating systems	0300, 0303, 0304, 0940, 0941, 1143, 1144,
Restrict administrative privileges	0405, 0445, 0985, 1175

4.1.1 Application Whitelisting

No	Source	Control	Applicability	Framework sections
No: 128	**Source:** ISM, PSPF	**Control:** 843, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Service Providers MUST use an application whitelisting solution within the Standard Operating Environments to restrict the execution of programs and Dynamic Link Libraries to an approved set.				

No	Source	Control	Applicability	Framework sections
Compliance	**Non-Compliant**	**Rationale**	Windows XP does not have a native ability to apply Application Whitelisting.	
Recommendation 29: That the CDMC PKI support infrastructure be an immediate candidate for the replacement of Windows XP. Recommendation 30: That the CDMC be allowed to implement their own updated SOE to upgrade PKI support infrastructure independent of the replacement of Windows XP project.				
No: 129	**Source:** ISM, PSPF	**Control:** 846, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Service Providers MUST ensure that users and system administrators cannot temporarily or permanently disable, bypass or be exempt from application whitelisting mechanisms.				
Compliance	**Non-Compliant**	**Rationale**	As White Listing is not applied, this control cannot also be enforced.	
Recommendation 29: That the CDMC PKI support infrastructure be an immediate candidate for the replacement of Windows XP. Recommendation 30: That the CDMC be allowed to implement their own updated SOE to upgrade PKI support infrastructure independent of the replacement of Windows XP project.				
No: 130	**Source:** ISM, PSPF	**Control:** 955, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6

No	Source	Control	Applicability	Framework sections
Service Providers MUST implement application whitelisting using at least one of the following methods: • cryptographic hashes, • publisher certificates, • absolute paths, or • parent folders.				
Compliance	**Non-Compliant**	**Rationale**	As White Listing is not applied, this control cannot also be applied.	
Recommendation 29: That the CDMC PKI support infrastructure be an immediate candidate for the replacement of Windows XP. Recommendation 30: That the CDMC be allowed to implement their own updated SOE to upgrade PKI support infrastructure independent of the replacement of Windows XP project.				
No: 131	**Source:** ISM, PSPF	**Control:** 1391, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
When implementing application whitelisting using parent folder rules, file system permissions MUST be configured to prevent users and system administrators from adding or modifying files in authorised parent folders.				
Compliance	**Non-Compliant**	**Rationale**	As White Listing is not applied, this control cannot also be applied.	
Recommendation 29: That the CDMC PKI support infrastructure be an immediate candidate for the replacement of Windows XP. Recommendation 30: That the CDMC be allowed to implement their own updated SOE to upgrade PKI support infrastructure independent of the replacement of Windows XP project.				

No	Source	Control	Applicability	Framework sections
No: 132	**Source:** ISM, PSPF	**Control:** 1392, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
When implementing application whitelisting using absolute path rules, file system permissions MUST be configured to prevent users and system administrators from modifying files that are permitted to run.				
Compliance	**Non-Compliant**	**Rationale**	As White Listing is not applied, this control cannot also be applied.	
Recommendation 29: That the CDMC PKI support infrastructure be an immediate candidate for the replacement of Windows XP. Recommendation 30: That the CDMC be allowed to implement their own updated SOE to upgrade PKI support infrastructure independent of the replacement of Windows XP project.				

4.1.2 Patch applications

No	Source	Control	Applicability	Framework sections
No: 133	**Source:** ISM, PSPF	**Control:** 300, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
High Assurance products MUST only be patched by ASD approved patches using methods and timeframes prescribed by ASD				
Compliance	**Compliant**	**Rationale**	This element is covered through standard Defence procedures and policy.	

No	Source	Control	Applicability	Framework sections
No: 134	**Source:** ISM, PSPF	**Control:** 303, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Service Providers MUST use an approach for patching operating systems, applications, drivers and hardware devices that ensures the integrity and authenticity of patches as well as the processes used to apply them.				
Compliance	**Non-Compliant**	**Rationale**	Patches are not applied as they are not available for the operating systems the software runs on.	
Recommendation 29: That the CDMC PKI support infrastructure be an immediate candidate for the replacement of Windows XP. Recommendation 30: That the CDMC be allowed to implement their own updated SOE to upgrade PKI support infrastructure independent of the replacement of Windows XP project.				
No: 135	**Source:** ISM, PSPF	**Control:** 304, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Operating systems, applications and hardware devices that are no longer supported by their vendors MUST be updated to a vendor supported version or replaced with an alternative vendor supported version.				
Compliance	**Non-Compliant**	**Rationale**	Initial examination of software used within the environment includes software no longer supported (Windows XP and Windows Server 2003).	
Recommendation 29: That the CDMC PKI support infrastructure be an immediate candidate for the replacement of Windows XP. Recommendation 30: That the CDMC be allowed to implement their own updated SOE to upgrade PKI support infrastructure independent of the replacement of Windows XP project.				

No	Source	Control	Applicability	Framework sections
No: 136	**Source:** ISM, PSPF	**Control:** 940, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Service Providers MUST apply all security patches as soon as possible.				
Compliance	**Non-Compliant**	**Rationale**	Patches are not applied as they are not available for the operating systems the PKI management console software runs on.	
Recommendation 29: That the CDMC PKI support infrastructure be an immediate candidate for the replacement of Windows XP. Recommendation 30: That the CDMC be allowed to implement their own updated SOE to upgrade PKI support infrastructure independent of the replacement of Windows XP project.				

No	Source	Control	Applicability	Framework sections
No: 137	**Source:** ISM, PSPF	**Control:** 941, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6

When patches are not available for vulnerabilities, one or more of the following approaches must be implemented:

- resolve the vulnerability by either:
  - disabling the functionality associated with the vulnerability
  - asking the vendor for an alternative method of managing the vulnerability
  - moving to a different product with a more responsive vendor
  - engaging a software developer to resolve the vulnerability.
- prevent exploitation of the vulnerability by either:
  - applying external input sanitisation (if an input triggers the exploit)
  - applying filtering or verification on output (if the exploit relates to an information disclosure)
  - applying additional access controls that prevent access to the vulnerability
  - configuring firewall rules to limit access to the vulnerability.
- contain exploitation of the vulnerability by either:
  - applying firewall rules limiting outward traffic that is likely in the event of an exploitation
  - applying mandatory access control preventing the execution of exploitation code
  - setting file system permissions preventing exploitation code from being written to disk.
- detect exploitation of the vulnerability by either:
  - deploying an intrusion detection system
  - monitoring logging alerts
  - using other mechanisms for the detection of exploits using the known vulnerability.

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	Due to the small environment that contains the Defence PKI infrastructure and supporting systems, alternative strategies can be and are implemented. There is also a reduced program base to track vulnerabilities that could present vulnerabilities.	
No: 138	**Source:** ISM, PSPF	**Control:** 1143, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Service Providers MUST develop and implement a patch management strategy covering the patching of vulnerabilities in operating systems, applications, drivers and hardware devices.				
Compliance	**Non-Compliant**	**Rationale**	No Patch Management policy is clearly documented in a single location or implemented.	
Recommendation 31: That the CDMC draft a single policy or procedures around patch management.				
No: 139	**Source:** ISM, PSPF	**Control:** 1144, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Vulnerabilities in operating systems, applications, drivers and hardware devices assessed as extreme risk MUST be patched or mitigated within two days.				
Compliance	**Compliant**	**Rationale**	Where identified, patches are applied or alternative strategies put in place, such as upgrades and replacements.	

4.1.3 Patch operating systems

No	Source	Control	Applicability	Framework sections
No: 140	**Source:** ISM, PSPF	**Control:** 300, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
High Assurance products MUST only be patched by ASD approved patches using methods and timeframes prescribed by ASD				
Compliance	**Compliant**	**Rationale**	High Assurance products are patched in accordance with ASD prescribed timeframes.	
No: 141	**Source:** ISM, PSPF	**Control:** 303, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Service Providers MUST use an approach for patching operating systems, applications, drivers and hardware devices that ensures the integrity and authenticity of patches as well as the processes used to apply them.				
Compliance	**Compliant**	**Rationale**	Patches are obtained from reputable sources and validated using relevant procedures, such as checksums.	
No: 142	**Source:** ISM, PSPF	**Control:** 304, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Operating systems, applications and hardware devices that are no longer supported by their vendors MUST be updated to a vendor supported version or replaced with an alternative vendor supported version.				

No	Source	Control	Applicability	Framework sections
Compliance	**Non-Compliant**	**Rationale**	The Defence PKI environment is currently Non-Compliant with the ASD Top4 as Windows XP SOE is no longer a supported platform. As it is not supported, there is no applicable patches that are provided to prevent presently discovered vulnerabilities within the operating systems.	
Recommendation 142a: That the CDMC PKI support infrastructure be an immediate candidate for the implementation of the EUC CP project. Recommendation 142b: That the CDMC be allowed to implement their own updated SOE to upgrade PKI support infrastructure independently of the EUC CP project.				
No: 143	**Source:** ISM, PSPF	**Control:** 940, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Vulnerabilities in operating systems, applications, drivers and hardware devices assessed as below extreme risk MUST be patched or mitigated as soon as possible.				
Compliance	**Non-Compliant**	**Rationale**	The Defence PKI environment is currently Non-Compliant with the ASD Top4 as Windows XP SOE is no longer a supported platform. As it is not supported, there is no applicable patches that are provided to prevent presently discovered vulnerabilities within the operating systems.	
Recommendation 29: That the CDMC PKI support infrastructure be an immediate candidate for the replacement of Windows XP. Recommendation 30: That the CDMC be allowed to implement their own updated SOE to upgrade PKI support infrastructure independent of the replacement of Windows XP project.				

No	Source	Control	Applicability	Framework sections
No: 144	**Source:** ISM, PSPF	**Control:** 941, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6

When patches are not available for vulnerabilities, one or more of the following approaches must be implemented:

- resolve the vulnerability by either:
  - disabling the functionality associated with the vulnerability
  - asking the vendor for an alternative method of managing the vulnerability
  - moving to a different product with a more responsive vendor
  - engaging a software developer to resolve the vulnerability.
- prevent exploitation of the vulnerability by either:
  - applying external input sanitisation (if an input triggers the exploit)
  - applying filtering or verification on output (if the exploit relates to an information disclosure)
  - applying additional access controls that prevent access to the vulnerability
  - configuring firewall rules to limit access to the vulnerability.
- contain exploitation of the vulnerability by either:
  - applying firewall rules limiting outward traffic that is likely in the event of an exploitation
  - applying mandatory access control preventing the execution of exploitation code
  - setting file system permissions preventing exploitation code from being written to disk.
- detect exploitation of the vulnerability by either:
  - deploying an intrusion detection system
  - monitoring logging alerts
  - using other mechanisms for the detection of exploits using the known vulnerability.

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	Due to the small environment that contains the Defence PKI infrastructure and supporting systems, alternative strategies can be implemented.	
No: 145	**Source:** ISM, PSPF	**Control:** 1143, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Service Providers MUST have a patch management strategy covering the patching or upgrade of applications and operating systems to address security vulnerabilities.				
Compliance	**Non-Compliant**	**Rationale**	No Patch Management strategy seems to be in place or implemented on a consistent basis by either the Defence PKI staff or supporting infrastructure staff.	
Recommendation 32: That the CDMC draft a single policy or procedure around patch management and ensure it is implemented.				
No: 146	**Source:** ISM, PSPF	**Control:** 1144, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
For security vulnerabilities assessed as 'extreme risk', Service Providers MUST, within two days: • apply the security patch, or • mitigate the vulnerability if there is no patch available.				
Compliance	**Compliant**	**Rationale**	Where identified, patches are applied or alternative strategies put in place, such as upgrades and replacements.	

4.1.4 Restrict administrative privileges

No	Source	Control	Applicability	Framework sections
No: 147	**Source:** ISM, PSPF	**Control:** 0405, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Service Providers MUST: • limit system access on a need-to-know basis • have any requests for access to a system authorised by the person's manager • provide personnel with the least amount of privileges needed to undertake their duties • review system access and privileges at least annually and when personnel change roles • when reviewing access, ensure a response from the person's manager confirming the need to access the system is still valid, otherwise access will be removed.				
Compliance	**Compliant**	**Rationale**	Only authorised users and administrators can access the elements of the CDMC infrastructure.	

No	Source	Control	Applicability	Framework sections
No: 148	**Source:** ISM, PSPF	**Control:** 445, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Service Providers MUST restrict the use of privileged accounts by ensuring that: • the use of privileged accounts is controlled and auditable; • system administrators are assigned a dedicated account to be used solely for the performance of their administration tasks; • privileged accounts are kept to a minimum; • privileged accounts are used for administrative work only; • passphrases for privileged accounts are regularly audited to check the same passphrase is not being reused over time or for multiple accounts (particularly between privileged and unprivileged accounts); and • privileges allocated to privileged accounts are regularly reviewed.				
Compliance	**Compliant**	**Rationale**	All accounts are controlled and auditable and are physically restricted in their ability to implemented changes due to dedicated infrastructure points being located within no-lone-zones. Only administrative work is allowed as connectivity is limited to operations using administration accounts.	
No: 149	**Source:** ISM, PSPF	**Control:** 985, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Service Providers MUST conduct remote administration of systems, including the use of privileged accounts, over a secure communications medium from secure devices.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	Remote connections, if required, are enabled through secure communications.	
No: 150	**Source:** ISM, PSPF	**Control:** 1175, 1353, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Service Providers MUST prevent users from using privileged accounts access to access the Internet and email.				
Compliance	**Compliant**	**Rationale**	Access using the dedicated accounts and terminals restrict the functionality to access this capability from within the PKI management environment.	

4.2 Access Controls

No	Source	Control	Applicability	Framework sections
No: 151	**Source:** ISM	**Control:** 414	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5
Service Providers MUST ensure that all users are: • uniquely identifiable • authenticated on each occasion that access is granted to a system.				
Compliance	**Compliant**	**Rationale**	All users are uniquely identifiable and must authenticate on each access.	

No	Source	Control	Applicability	Framework sections
No: 152	**Source:** ISM	**Control:** 1173	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5
Service Providers MUST use multi-factor authentication for: • system administrators, • database administrators, • privileged users, • positions of trust, and • remote access.				
Compliance	**Compliant**	**Rationale**	Multifactor authentication is under taken through the provision of High Assurance smart cards.	
No: 153	**Source:** ISM	**Control:** 1384	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5
Service Providers MUST ensure that all privileged actions have passed through at least one multi-factor authentication process.				
Compliance	**Compliant**	**Rationale**	Multifactor authentication is under taken through the provision of High Assurance smart cards.	

No	Source	Control	Applicability	Framework sections
No: 154	**Source:** ISM	**Control:** 1381	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5, 9.7
Service Providers MUST ensure that dedicated workstations used for privileged tasks are prevented from communicating to assets and sending and receiving traffic not related to administrative purposes.				
Compliance	**Compliant**	**Rationale**	Privileged workstations used for the administration of the Defence PKI environment are not able to operate additional features either through operating system or network control.	
No: 155	**Source:** ISM, PSPF	**Control:** 856, PERSEC 1, INFOSEC 5	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK8 & 9), 9.2, 9.3, 9.4, 9.5, 9.7
Users authorisations MUST be enforced by access controls.				
Compliance	**Compliant**	**Rationale**	All authorisations/activities must be authorised and attributable to a user's account, with access controls enabling roles and responsibilities.	
No: 156	**Source:** ISM	**Control:** 382	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6
Service Providers MUST ensure that users do not have the ability to install, uninstall or disable software.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	*General* users of the Defence PKI environment do not have this capability. Only authorised and approved administrators, with the permission for that role, can install, uninstall and disable software.	
No: 157	**Source:** ISM	**Control:** 845	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5
Service Providers MUST restrict a user's rights in order to permit them to only execute a specific set of predefined executables as required for them to complete their duties.				
Compliance	**Compliant**	**Rationale**	Users rights are enforced through directory permissions as well as the administration rights the user holds (if any) to undertake PKI specific administration tasks.	

4.3 User Accounts

No	Source	Control	Applicability	Framework sections
No: 158	**Source:** ISM	**Control:** 383	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5
Service Providers MUST ensure that default operating system accounts are disabled, renamed or have their passphrase changed.				
Compliance	**Compliant**	**Rationale**	Access to the Administrator accounts on Windows devices is deactivated and the passphrase changed. All other access is undertaken through 2 factor privileged access.	

No	Source	Control	Applicability	Framework sections
No: 159	**Source:** GK	**Control:** GK	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5, 9.7
PKI administrative rights MUST be removed when no longer required by the user, or when the user leaves the company/Service Provider.				
Compliance	**Compliant**	**Rationale**	The physical removal of the CDMC smartcards used in the operation of the PKI environment prevents the reciprocal account from being used. Account permissions are review on a regular basis.	
No: 160	**Source:** ISM	**Control:** 421	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5
Service Providers using passphrases as the sole method of authentication MUST enforce the following passphrase policy: • a minimum length of 13 alphabetic characters with no complexity requirement; or • a minimum length of 10 characters, consisting of at least three of the following character sets: – lowercase alphabetic characters (a–z) – uppercase alphabetic characters (A–Z) – numeric characters (0–9) – special characters.				
Compliance	**Compliant**	**Rationale**	All passphrases used within the PKI environment comply with Defence requirements.	

No	Source	Control	Applicability	Framework sections
No: 161	**Source:** ISM	**Control:** 417	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5
Service Providers MUST NOT use a numerical password (or personal identification number) as the sole method of authenticating a user.				
Compliance	**Compliant**	**Rationale**	This is not undertaken within the CDMC.	
No: 162	**Source:** ISM	**Control:** 1403	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5
Service Providers MUST ensure accounts are locked after a maximum of five failed logon attempts.				
Compliance	**Compliant**	**Rationale**	Accounts are locked out once a maximum of five attempts to log in have been made.	
No: 163	**Source:** ISM	**Control:** 430	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5
Accounts MUST be removed or suspended the same day a user no longer has a legitimate business requirement for its use. For example, changing duties or leaving the organisation.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	The *ICT Systems Access Controls* section of the CDMC ICTSP stipulates that accounts no longer required are to be suspended immediately.	
No: 164	**Source:** ISM	**Control:** 1227	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5, 9.7
Service Providers MUST ensure reset passphrases are: • random for each individual reset • not reused when resetting multiple accounts • not based on a single dictionary word • not based on another identifying factor, such as the user's name or the date.				
Compliance	**Compliant**	**Rationale**	Password resets are randomised and are not based on a replicating identifying factor.	
No: 165	**Source:** ISM	**Control:** 976	**Applicability:** RA, CA, VA	**Framework sections:** 9.4, 9.5, 9.7
Service Providers MUST ensure users provide sufficient evidence to verify their identity when requesting a passphrase reset for their system account.				
Compliance	**Compliant**	**Rationale**	Resets can incorporate up to the same level of authentication required when passphrases were issued.	

No	Source	Control	Applicability	Framework sections
No: 166	**Source:** ISM	**Control:** 419	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5
Authentication information MUST be protected when communicated across networks.				
Compliance	**Compliant**	**Rationale**	Authentication information is encrypted at all times across networks.	
No: 167	**Source:** ISM	**Control:** 416	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5
If Service Providers choose to allow shared, non user-specific accounts, another method of attributing actions undertaken by such accounts to specific personnel MUST be implemented.				
Compliance	**Compliant**	**Rationale**	Non user-specific accounts are not used within the CDMC.	

4.4 Standard Operating Environment

No	Source	Control	Applicability	Framework sections
No: 168	**Source:** ISM	**Control:** 380	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5, 9.6
Service Providers MUST remove or disable unneeded operating system accounts, software, components, services and functionality.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	A hardened SOE (gold image) is supplied by a central authority and applied to the CA hardware prior to the installation of the supporting CA software.	
No: 169	**Source:** ISM	**Control:** 1033	**Applicability:** RA, CA, VA	**Framework sections:** 9.5
Service Providers MUST ensure that antivirus or internet security software has: • signature-based detection enabled and set to a high level • heuristic-based detection enabled and set to a high level • detection signatures checked for currency and updated on at least a daily basis • automatic and regular scanning configured for all fixed disks and removable media.				
Compliance	**Compliant**	**Rationale**	The AV Virus Pattern Number is a recorded item within the Daily System Operability Test (DSOT) for PKI Operators which would also be an indicator if the updating of the product does not occur. Scanning is configured to update on a regular basis.	
No: 170	**Source:** ISM	**Control:** 1306	**Applicability:** RA, CA, VA	**Framework sections:** 9.5
Firmware for network devices MUST be kept up to date.				
Compliance	**Compliant**	**Rationale**	Firmware upgrades are undertaken as part of standard procedures by the designated network support area.	

No	Source	Control	Applicability	Framework sections
No: 171	**Source:** ISM	**Control:** 657	**Applicability:** RA, CA, VA	**Framework sections:** 9.5
Data imported to a system MUST be scanned for malicious and active content.				
Compliance	**Compliant**	**Rationale**	Data imported into the system is scanned for malicious or active content either through dedicated or network based resources.	
No: 172	**Source:** ISM	**Control:** 842	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5
When using a software-based isolation mechanism to share a physical server's hardware, Service Providers MUST ensure that: • the isolation mechanism is from a vendor that uses secure programming practices and, when vulnerabilities have been identified, the vendor has developed and distributed patches in a timely manner; • the configuration of the isolation mechanism is hardened, including removing support for unneeded functionality and restricting access to the administrative interface used to manage the isolation mechanism, with the configuration performed and reviewed by subject matter experts; • the underlying operating system running on the server is hardened; • security patches are applied to both the isolation mechanism and operating system in a timely manner; and, • integrity and log monitoring is performed for the isolation mechanism and underlying operating system in a timely manner.				
Compliance	**Compliant**	**Rationale**	Virtualisation is not used within the PKI environment with dedicated servers are used to host individual services.	

4.5 Databases

No	Source	Control	Applicability	Framework sections
No: 173	**Source:** ISM, PSPF	**Control:** 1250, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Database servers MUST use a hardened SOE.				
Compliance	**Compliant**	**Rationale**	The database platform is a standard and harden image as supplied by Defence ICT.	
No: 174	**Source:** ISM	**Control:** 1262	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5, 9.7
Database administrators MUST have unique and identifiable accounts.				
Compliance	**Compliant**	**Rationale**	In accordance with section *ICT System Access Controls* of the CDMC ICTSP, all privileged accounts must be uniquely identifiable and this would include database accounts.	
No: 175	**Source:** ISM	**Control:** 1266	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5, 9.7
Anonymous database accounts MUST be removed.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	It is Defence policy that no anonymous accounts are used within any system. It is stringently enforced within the CDMC IAW section *ICT System Access Controls* of the CDMC ICTSP.	
No: 176	**Source:** ISM	**Control:** 1260	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5, 9.7
Default database administrator accounts MUST be disabled, renamed or have their passphrases changed.				
Compliance	**Compliant**	**Rationale**	All default accounts are either disabled or renamed prior to a new passphrase being assigned.	
No: 177	**Source:** ISM	**Control:** 1263	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5, 9.7
Database administrator accounts MUST be used exclusively for administrative tasks with standard database accounts used for general purpose interactions with databases.				
Compliance	**Compliant**	**Rationale**	In accordance with para. 52 of the *ICT System Access Controls* of the CDMC ICTSP, all accounts must adhere to the least privilege principle. Administrative accounts are separated from the general purpose interactions with databases.	

No	Source	Control	Applicability	Framework sections
No: 178	**Source:** ISM, PSPF	**Control:** 1249, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
Service Providers MUST configure DBMS software to run as a separate account with the minimum privileges needed to perform its functions.				
Compliance	**Compliant**	**Rationale**	The DBMS software runs as a separate instance (Oracle) by default through the software used by the CDMC.	
No: 179	**Source:** ISM, PSPF	**Control:** 1250, INFOSEC 4	**Applicability:** RA, CA, VA	**Framework sections:** 6.3, 7 (GK10), 9.5, 9.6
The account under which DBMS software runs MUST have limited access to non-essential areas of the database server's file system.				
Compliance	**Compliant**	**Rationale**	In accordance with para. 52 of the *ICT System Access Controls* of the CDMC ICTSP, all accounts must adhere to the least privilege principle.	
No: 180	**Source:** ISM	**Control:** 1252	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6
Service Providers MUST ensure passphrases stored in databases are hashed with a strong hashing algorithm which is uniquely salted.				
Compliance	**Compliant**	**Rationale**	Database passphrases are either stored in this manner or authentication is mandated through the existing CA and RA controls, i.e. operator smartcards.	

No	Source	Control	Applicability	Framework sections
No: 181	**Source:** ISM	**Control:** 1256	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6
Service Providers MUST apply file-based access controls to database files.				
Compliance	**Compliant**	**Rationale**	Only authorised CA components of the database are able to be accessed by that CA.	
No: 182	**Source:** ISM	**Control:** 1275	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5
All queries to database systems from web applications MUST be filtered for legitimate content and correct syntax.				
Compliance	**Compliant**	**Rationale**	The current solution limits the ability to implement requests that are either illegitimate or incorrect for syntax to prevent this form of attack vector on the CA systems from occurring.	
No: 183	**Source:** ISM	**Control:** 1277	**Applicability:** RA, CA, VA	**Framework sections:** 9.2, 9.3, 9.4, 9.5, 9.10, 11.2
Sensitive or classified information communicated between database systems and web applications MUST be encrypted.				
Compliance	**Compliant**	**Rationale**	Information exchanged between webservers and databases is encrypted. However, the traffic primarily is done using SSL and not TLS.	

No	Source	Control	Applicability	Framework sections
No: 184	**Source:** ISM	**Control:** 393	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6, 9.7
Databases or their contents MUST be associated with protective markings.				
Compliance	**Compliant**	**Rationale**	Each database is held and regarded at the classification it has been assigned.	

4.6 System Monitoring

No	Source	Control	Applicability	Framework sections
No: 185	**Source:** ISM	**Control:** 859	**Applicability:** RA, CA, VA	**Framework sections:** 6.4, 9.5, 11.3
Service Providers MUST retain event logs for a minimum of 7 years after action is completed in accordance with the NAA's Administrative Functions Disposal Authority.				
Compliance	**Compliant**	**Rationale**	The PKI SSP requires that all PKI logs are retained for a period of seven years or in a accordance with the National Archives of Australia Governance.	

No	Source	Control	Applicability	Framework sections
No: 186	**Source:** ISM	**Control:** 585	**Applicability:** RA, CA, VA	**Framework sections:** 6.4, 9.5, 11.3
For each event logged, Service Providers MUST ensure that the logging facility records at least the following details: • date and time of the event; • relevant system user(s) or process; • event description; • success or failure of the event; • event source (for example application name); and • equipment location/identification.				
Compliance	**Compliant**	**Rationale**	All log files of PKI actions are not only retained by are signed by the relevant DRCA/DIOCA, SubCA, RA or KAS. In combination with the log files generated by the underlining operating system software are combined and archived on a nightly basis.	

4.7 PKI Core Elements

No	Source	Control	Applicability	Framework sections
No: 187	**Source:** ISM, GK	**Control:** 1444	**Applicability:** CA	**Framework sections:** 9.3, 9.4, 9.5, 9.6
Certificates MUST be generated using a certificate authority product or hardware security module that completed an evaluation endorsed by ASD				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	Both the certificate authority product (UniCERT) and the associated connected hardware security module (LunaCA3) have been evaluated under Common Criteria and endorsed by ASD.	
No: 188	**Source:** GK	**Control:** GK	**Applicability:** RA	**Framework sections:** 9.3, 9.4, 9.5, 9.6
RA servers are MUST be inaccessible directly from the internet.				
Compliance	**Compliant**	**Rationale**	All RAs are located within a zone known as the InnerZone, which is segmented from the internal Defence Low/High networks, which is also segmented from the Internet.	
No: 189	**Source:** GK	**Control:** GK	**Applicability:** RA	**Framework sections:** 9.5, 9.6, 9.7, 11.3
When a registration is performed, all relevant information on who performed the registration MUST is logged.				
Compliance	**Compliant**	**Rationale**	The RA logs and retains information about all the actions performed by the RAOs.	
No: 190	**Source:** GK	**Control:** GK	**Applicability:** RA	**Framework sections:** 9.7, 11.5, 11.6

No	Source	Control	Applicability	Framework sections
When very high assurance (LOA 4) is required, an in-person face to face identity proofing procedure MUST be used to ensure that there is some physical verification the registrant is who they claim to be.				
Compliance	**Compliant**	**Rationale**	Face to face identification occurs prior to the issuance of a certificate to an individual. Relevant identification material, as specified by the Gatekeeper Competent Authority is also used to verify the person identity.	
No: 191	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 9.3, 9.4, 9.5, 9.6
CA servers are MUST be inaccessible directly from the internet.				
Compliance	**Compliant**	**Rationale**	All SubCAs are located within a zone known as the InnerZone, which is segmented from the relevant internal Defence network, in which that network itself is segmented from the Internet. The RootCA is further segmented from the InnerZone, residing in its own environment.	
No: 192	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 6.4, 9.10
Service Providers MUST only archive encryption keys to enable recovery of encrypted data. Digital signature/authentication keys MUST NOT be archived.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	Only encryption keys are archived by the UniCERT Key Archive Server.	
No: 193	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 6.4, 10.4
PKI backups, including backups key escrow services and software based private keys MUST be stored in a manner at least as secure as live systems with similar restrictions on who has access and no-lone requirements.				
Compliance	**Compliant**	**Rationale**	All backups are held on the same device type as those generated for the active private key. For example, separate HSMs hold the active and back private key for the RootCAs, SubCAs, RA, KAS and TSA.	
No: 194	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 6.4, 9.4, 9.10
Private keys MUST be encrypted within the key archive store to stop attacks where the store is stolen and accessed offline.				
Compliance	**Compliant**	**Rationale**	The key archive store encrypts the private keys for confidentiality and not authentication.	

No	Source	Control	Applicability	Framework sections
No: 195	**Source:** GK	**Control:** GK	**Applicability:** CA	**Framework sections:** 6.4, 9.10
Any instances of key recovery MUST be logged, audited and alerted so they can be reviewed by the appropriate authority.				
Compliance	**Compliant**	**Rationale**	Key recovery undertaken within the dedicated Key Archive Server the KASRO can be and is audited by the KAS ROAuditor function.	

4.8 Approved Algorithms and Protocols

No	Source	Control	Applicability	Framework sections
No: 196	**Source:** GK	**Control:** GK	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers MUST use encryption products that implement ASD Approved Cryptographic Algorithms				
Compliance	**Non-Compliant**	**Rationale**	X.509 Certificate Policy for the Australian Department of Defence Timestamp Authority refers to SHA-1, no longer an approved AACA. X.509 Certificate Policy for the Australian Department of Defence Code Signing Resource Certificates refers to SHA-1, no longer an approved AACA.	
Recommendation 33: That a transition plan be compiled to ensure the successful implementation of HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512 in the environment as the XP SOE is replaced within Defence.				
No: 197	**Source:** ISM, GK	**Control:** 1446	**Applicability:** RA, CA, VA	**Framework sections:** 9.10

No	Source	Control	Applicability	Framework sections
Service Providers using elliptic curve cryptography MUST select a curve from the NIST standard, FIPS 186-4.				
Compliance	**Compliant**	**Rationale**	Not applicable, elliptic curve cryptography is not in use.	
No: 198	**Source:** ISM	**Control:** 471	**Applicability:** RA, CA, VA	**Framework sections:** 9.10, 10.3, 11.2
Service Providers using an unevaluated product that implements an AACA MUST ensure that only AACAs can be used				
Compliance	**Compliant**	**Rationale**	Only evaluated products are in use within the CDMC.	
No: 199	**Source:** ISM	**Control:** 472	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers using DH for the approved use of agreeing on encryption session keys MUST use a modulus of at least 1024 bits.				
Compliance	**Compliant**	**Rationale**	Not applicable, DH is not in use.	
No: 200	**Source:** ISM	**Control:** 1373	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers MUST NOT use anonymous DH.				
Compliance	**Compliant**	**Rationale**	Anonymous DH is not in use.	

No	Source	Control	Applicability	Framework sections
No: 201	**Source:** ISM	**Control:** 474	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers using ECDH for the approved use of agreeing on encryption session keys MUST use a field/key size of at least 160 bits				
Compliance	**Compliant**	**Rationale**	Not applicable, ECDH is not in use.	
No: 202	**Source:** ISM	**Control:** 998	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers MUST use HMAC–SHA256, HMAC–SHA384 or HMAC–SHA512 as a HMAC algorithm.				
Compliance	**Non-Compliant**	**Rationale**	HMAC–SHA1 is used extensively within the environment due to the ongoing support of Windows XP SOE.	
Recommendation 33: That a transition plan be compiled to ensure the successful implementation of HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512 in the environment as the XP SOE is replaced within Defence.				
No: 203	**Source:** ISM	**Control:** 473	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers using DSA for the approved use of digital signatures MUST use a modulus of at least 1024 bits				
Compliance	**Compliant**	**Rationale**	Not applicable, DSA is not in use.	

No	Source	Control	Applicability	Framework sections
No: 204	**Source:** ISM	**Control:** 475	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers using ECDSA for the approved use of digital signatures MUST use a field/key size of at least 160 bits				
Compliance	**Compliant**	**Rationale**	Not applicable, ECDSA is not in use.	
No: 205	**Source:** ISM	**Control:** 476	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers using RSA, for both the approved use of digital signatures and passing encryption session keys or similar keys, MUST use a modulus of at least 1024 bits.				
Compliance	**Compliant**	**Rationale**	A modulus of 1024 bits is the minimum issued to operators and End Entities, with all other PKI elements issued key lengths of a minimum of 2048 bits.	
No: 206	**Source:** ISM	**Control:** 477	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers using RSA, both for the approved use of digital signatures and for passing encryption session keys or similar keys, MUST ensure that the key pair used for passing encrypted session keys is different from the key pair used for digital signatures.				
Compliance	**Compliant**	**Rationale**	There is a separation of the encryption used within the Defence PKI environment with RSA used for encryption and SHA used for digital signatures.	

No	Source	Control	Applicability	Framework sections
No: 207	**Source:** ISM	**Control:** 480	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers using 3DES MUST use either two distinct keys in the order key 1, key 2, key 1 or three distinct keys.				
Compliance	**Compliant**	**Rationale**	3DES is not listed in the CDMC KMP and therefore is not considered in use.	
No: 208	**Source:** ISM	**Control:** 1161	**Applicability:** RA, CA, VA	**Framework sections:** 9.10, 10.3, 11.2
Service Providers MUST use an encryption product that implements a AACA if they wish to reduce the storage or physical transfer requirements for ICT equipment or media that contains sensitive information to an unclassified level.				
Compliance	**Compliant**	**Rationale**	It is Defence policy that material be treated at the classification that it is generated at and transported accordingly..	
No: 209	**Source:** ISM	**Control:** 481	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers using a product that implements an AACP MUST ensure that only AACAs can be used.				
Compliance	**Compliant**	**Rationale**	Use of AACA's are applied through the CDMC use of an AACP.	
No: 210	**Source:** ISM	**Control:** 482	**Applicability:** RA, CA, VA	**Framework sections:** 9.10

No	Source	Control	Applicability	Framework sections
Service Providers MUST NOT use SSL.				
Compliance	**Non-Compliant**	**Rationale**	The PKI SSP references the links between WebRAO and RSs and the user browser and the Web Handler certificate request pages using SSL and not TLS.	
Recommendation 34: That a transition plan be compiled to remove the SSL configurations from the DIE as the XP SOE is replaced within Defence.				
No: 211	**Source:** ISM	**Control:** 1447	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers MUST use TLS.				
Compliance	**Non-Compliant**	**Rationale**	See previous example but documentation does not specify the exclusive use of TLS.	
Recommendation 35: That a transition plan be compiled to enable the implementation of TLS in the DIE as the XP SOE is replaced within Defence.				
No: 212	**Source:** ISM	**Control:** 1233	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers MUST NOT use manual keying for Key Exchange when establishing an IPsec connection.				
Compliance	**Compliant**	**Rationale**	Manual keying is not used in the Key Exchange for establishing IPsec connections.	
No: 213	**Source:** ISM	**Control:** 496	**Applicability:** RA, CA, VA	**Framework sections:** 9.10

No	Source	Control	Applicability	Framework sections
Service Providers MUST use the ESP protocol for IPsec connections.				
Compliance	**Compliant**	**Rationale**	It is standard practice that this protocol is used as part of the Defence implementation of IPsec.	
No: 214	**Source:** ISM	**Control:** 1162	**Applicability:** RA, CA, VA	**Framework sections:** 9.10, 10.3, 11.2
Service Providers MUST use an encryption product that implements a AACP if they wish to communicate sensitive information over public network infrastructure.				
Compliance	**Compliant**	**Rationale**	IPsec is the standard used in the transmission of data of lower classified information with high grade encryption used for the encryption of network traffic for the higher network classification.	
No: 215	**Source:** ISM, GK	**Control:** 457	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers MUST use a Common Criteria-evaluated encryption product that has completed a ACE if they wish to reduce the storage or physical transfer requirements for ICT equipment or media that contains classified information to an unclassified level.				
Compliance	**Compliant**	**Rationale**	The Hardware Security Modules used within the PKI environment reduce the complexity required in the event that they need to be moved.	

No	Source	Control	Applicability	Framework sections
No: 216	**Source:** ISM, GK	**Control:** 465	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers MUST use a Common Criteria-evaluated encryption product that has completed a ACE if they wish to communicate classified or sensitive information over public network infrastructure.				
Compliance	**Compliant**	**Rationale**	Evaluated network security products implementing IPsec is the standard used in the transmission of data.	
No: 217	**Source:** ISM	**Control:** 157	**Applicability:** RA, CA, VA	**Framework sections:** 9.10
Service Providers communicating sensitive or classified information over public network infrastructure or over infrastructure in unsecured spaces (Zone One security areas) MUST use encryption approved for communicating such information over public network infrastructure.				
Compliance	**Compliant**	**Rationale**	Network based encryption used for transmission across Zone One spaces is either via EPL listed products or via other encryption products endorsed by the NCA and DSA.	

4.9 Outsourced Arrangements

No	Source	Control	Applicability	Framework sections
No: 218	**Source:** ISM	**Control:** 71	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5
If information is processed, stored or communicated by a system not under a Service Provider's control, the Service Provider MUST ensure that the non-Service Provider system has appropriate security measures in place to protect the Service Provider's information.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	No Defence PKI systems are held in the control of external service providers.	

5 Personnel Controls

As part of the Gatekeeper IRAP assessment, a total of ten (10) Personnel controls were assessed, with the Defence PKI deemed compliant with nine (9) of those ten (10) Personnel controls. The single Personnel control deemed non-compliant had a severity rating of Partial.

5.1 Clearances

No	**Source**	**Control**	**Applicability**	**Framework sections**
No: 219	**Source:** ISM, PSPF	**Control:** 434, PERSEC 1, 4 & 5	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK8 & 9), 9.2, 9.3, 9.4, 9.5, 9.7
Service Providers MUST ensure that personnel undergo an appropriate employment screening, and where necessary hold an appropriate security clearance according to the requirements in the Australian Government Personnel Security Management Protocol before being granted access to a system.				
Compliance	**Compliant**	**Rationale**	All staff within the CDMC undergoes the standard clearance process of being cleared to NV2. This is required to undertake activities on the PKI High environment and is specified within the PKI SSP *System Users* section.	
No: 220	**Source:** PSPF	**Control:** PERSEC 6	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK9), 9.7
Service Providers MUST ensure that personnel holding security clearances advise AGSVA of any significant changes in personal circumstances which may impact on their continuing suitability to access security classified resources.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	It is a standard practice within Defence that the person holding the clearance brief and inform the CDMC SO (or similar) position assigned to the area, notification of any travel that is to occur. It is during this process that the user is informed of their role and responsibilities for post travel notification of events.	
No: 221	**Source:** ISM, PSPF	**Control:** 502, PERSEC 1, 4 & 5, INFOSEC 5	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK10), 9.2, 9.3, 9.4, 9.5, 9.7
Before personnel are granted communications security custodian access, Service Providers MUST ensure that they have: • a demonstrated need for access • read and agreed to comply with the relevant Cryptographic Key Management Plan for the cryptographic system they are using a security clearance at least equal to the classification of the keying material; • agreed to protect the authentication information for the cryptographic system at the sensitivity or classification of information it secures; • agreed not to share authentication information for the cryptographic system without approval; • agreed to be responsible for all actions under their accounts; and, • agreed to report all potentially security related problems to an ITSM.				
Compliance	**Compliant**	**Rationale**	CDMC PKI Staff Access Registration form, as well as additional governance instruments such as the ADF clearance process, provides sufficient and explicit direction on the expectations of the CDMC PKIK Operations staff as well as the clear acceptance of their role and requirements within the PKI environment.	

No	Source	Control	Applicability	Framework sections
No: 222	**Source:** ISM, PSPF	**Control:** 435, PERSEC 1	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK8), 9.2, 9.3, 9.4, 9.5, 9.7
Service Providers MUST ensure that personnel have received any necessary briefings before being granted access to a system.				
Compliance	**Compliant**	**Rationale**	A formal PKI Operational induction briefing is listed as required within the SSP and is described in detail within Annex A of the CDMC PKI Staff Access Registration form.	

5.2 Training

No	Source	Control	Applicability	Framework sections
No: 223	**Source:** ISM, PSPF	**Control:** 251, GOV1 & 9, INFOSEC 3, PHYSEC2	**Applicability:** RA, CA, VA	**Framework sections:** 6, 7 (GK1 & 9), 9.2, 9.4, 9.5, 9.6, 9.7
Service Providers MUST ensure that all personnel who have access to ICT systems have sufficient information awareness and training.				
Compliance	**Compliant**	**Rationale**	The *Education and Training* section PKI SSP specify the level of training and awareness that is required.	
No: 224	**Source:** ISM, PSPF	**Control:** 252, GOV1 & 9, INFOSEC 3, PHYSEC2	**Applicability:** RA, CA, VA	**Framework sections:** 6, 7 (GK1 & 9), 9.2, 9.4, 9.5, 9.6, 9.7

No	Source	Control	Applicability	Framework sections
Service Providers MUST provide ongoing ICT security training and awareness for personnel on information security policies on topics such as responsibilities, consequences of non-compliance, potential security risks and countermeasures.				
Compliance	**Compliant**	**Rationale**	The *Education and Training* section PKI SSP specifies the level of ongoing requirements as well as specifying that it is the role of the CSO to present ongoing training on PKI security issues.	

5.3 Security Awareness

No	Source	Control	Applicability	Framework sections
No: 225	**Source:** ISM, PSPF	**Control:** 413, GOV1, INFOSEC 3 & 5	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK1 & 9), 9.2, 9.4, 9.5, 9.6
Service Providers MUST develop and maintain a set of policies and procedures covering user identification, authentication, roles, responsibilities and authorisations and make users aware of, and understand the policies and procedures.				
Compliance	**Compliant**	**Rationale**	The Defence PKI publish several references to cover this requirement including the ICTSP, the SSP and other Defence wide governance documentation.	
No: 226	**Source:** ISM	**Control:** 122	**Applicability:** RA, CA, VA	**Framework sections:** 9.5, 9.6, 9.7, 9.9
Service Providers MUST detail cyber security incident responsibilities and procedures for each system in the relevant SSP, SOPs, and IRP.				

No	Source	Control	Applicability	Framework sections
Compliance	**Non-Compliant**	**Rationale**	Examined SOPs do not explicitly state what to do in the event of an incident. There is coverage within the *ICT Security Incident Response* section of the CDMC ICTSP and the *Security Administration* section of the PKI SSP however this has not been distilled into a separate Incident Response Plan.	
Recommendation 36: Update all SOPs to include a reference to report all suspicious activities.				
No: 227	**Source:** ISM, PSPF	**Control:** 1083, GOV1, INFOSEC 3 & 5	**Applicability:** RA, CA, VA	**Framework sections:** 7 (GK1 & 9), 9.2, 9.4, 9.5, 9.6, 9.7
Service Providers MUST advise personnel of the sensitivities and classifications permitted for data and voice communications when using mobile devices.				
Compliance	**Compliant**	**Rationale**	The overall Defence policy on the use of mobile devices applies to the users within the CDMC.	

5.4 Staff Responsibilities

No	Source	Control	Applicability	Framework sections
No: 228	**Source:** ISM	**Control:** 661	**Applicability:** RA, CA, VA	**Framework sections:** 9.3, 9.4, 9.5, 9.6, 9.7
Service Providers MUST ensure that system users transferring data to and from a system are held accountable for the data they transfer.				

No	Source	Control	Applicability	Framework sections
Compliance	**Compliant**	**Rationale**	All transfers are logged and recorded, with those logs signed by the relevant certificate.	

6 Recommendations

The following is a consolidated listing of the thirty six (36) Recommendations drawn from the review of the previous Documentation, Physical, Logical and Personnel Controls sections. The listing is consolidated as a particular recommendation could apply to multiple Controls. Recommendations also do not exclusively apply to Non-Compliant controls and are included to improve the operations of the Defence PKI environment.

Recommendation 1 (Control 8): That any identified and accepted non-compliance with controls identified within this report be justified in writing and validated with a risk assessment and any mitigation measures listed.

Recommendation 2 (Control 9): That any identified and accepted non-compliance with controls be retained as evidence for the next Gatekeeper assessment.

Recommendation 3 (Control 14): That the DPKI ICTSP be updated to include a description of this Gatekeeper and Defence's Accreditation processes.

Recommendation 4 (Control 15): That the CDMC adapt the existing DPKI SRMP to include the requirements of the Protective Security Risk Review.

Recommendation 5 (Control 15): That the CDMC undertake and document a Protective Security Risk Review as a separate artefact.

Recommendation 6 (Control 21): That the Controls listed within the SRMP be referenced against the ISM categories listed within the ISM.

Recommendation 7 (Control 21): That future iterations of the SRMP specify which Controls within the ISM are relevant to the controls of SRMP.

Recommendation 8 (Control 22): That the CDMC ensure that any delays in the implementation away from Windows XP is reflected within the SRMP and that alternative controls are investigated if the delay is to impact the next assessment period.

Recommendation 9 (Control 29): That the CDMC update the Security Objectives section of the DPKI SSP to include the objectives for the Workstations and Servers.

Recommendation 10 (Control 30): That the CDMC update the Audit/Accountability section of the DPKI SSP to include the ability to protect the logs.

Recommendation 11 (Control 30): That the CDMC update the Audit/Accountability section of the DPKI SSP to include availability.

Recommendation 12 (Control 32): That the CDMC initiate the planning phase to centralise the logging of events.

Recommendation 13 (Control 33): That once the CDMC implement a centralised logging capability, a reference that all systems will log to this location must be included within the DPKI SSP.

Recommendation 14 (Control 34): That the CDMC draft a standard statement to be inserted into all current and future SOPs that specifies that users report all suspicious events to the CDMC Security Officer.

Recommendation 15 (Control 43 & 44): That the CDMC draft a SOP that incorporates the Nagios scanning that is undertaken within the environment as well as any external to DPKI testing that occurs.

Recommendation 16 (Control 45): That at the conclusion of the Gatekeeper Accreditation process, the DRAFT PKI IRP be accepted as final and versioned accordingly.

Recommendation 17 (Control 51): That the CDMC updates the DRBCP to reference the ASD Cyber Security Incident Reporting (CSIR) reporting mechanism.

Recommendation 18 (Control 51): That the CDMC updates the DRBCP to reference reporting cyber security events to the Gatekeeper Competent Authority.

Recommendation 19 (Control 51): That the CDMC ensures that the new IRP reference the ASD CSIR reporting mechanism and the Gatekeeper Competent Authority.

Recommendation 20 (Control 53): That the created CDMC IRP reference the notification process of vendors to the CDMC of detected or suspected vulnerabilities within the CDMC networks and equipment.

Recommendation 21 (Control 63): That the CDMC ICTSP and the PKI SSP be updated to include a specific reference to the emergency change management procedures.

Recommendation 22 (Control 79): That once CDMC PKI POC is relocated to its new facility, the CDMC must engage Defence Security and Vetting Service to assess and rate the facility under the current Australian Government Physical Security Management Protocol if the new facility has not been already physically accredited.

Recommendation 23 (Control 79): That the CDMC PKI engage Defence Security and Vetting Service to assess and rate the BOC facility within HMAS Harman under the current Australian Government Physical Security Management Protocol or validate that the BOC facility is covered by an existing physical accreditation to the new protocol.

Recommendation 24 (Control 79): That on the Defence Security and Vetting Service assessing the POC and BOC facility under the current Australian Government Physical Security Management Protocol, the CDCM SSP be updated to include the new physical certifications.

Recommendation 25 (Control 84 & 98): That once CDMC PKI POC is relocated to its new facility, the CDMC must engage Defence Security and Vetting Service to assess and rate the facility under the current Australian Government Physical Security Management Protocol.

Recommendation 26 (Control 84 & 98): That the CDMC PKI engage Defence Security and Vetting Service to assess and rate the BOC facility within HMAS Harman under the current Australian Government Physical Security Management Protocol or validate that the BOC facility is covered by an existing physical accreditation to the new protocol.

Recommendation 27 (Control 119): That the CDMC PKI operations team complete a copy of the Register (not the individual physical forms) for storage within the BOC for the purpose of remediation in case of loss of the POC.

Recommendation 28 (Control 119): That the CDMC PKI operations team investigate creating an electronic register for such items, such as database register, that is retained in a centralised location that could be accessed from either the POC or BOC.

Recommendation 29 (Control 127, 128, 129, 130, 131, 132, 134, 135, 136 & 143): That the CDMC PKI support infrastructure be an immediate candidate for the replacement of Windows XP.

Recommendation 30 (Control 127, 128, 129, 130, 131, 132, 134, 135, 136 & 143): That the CDMC be allowed to implement their own updated SOE to upgrade PKI support infrastructure independent of the replacement of Windows XP project.

Recommendation 31 (Control 138): That the CDMC draft a single policy or procedures around patch management.

Recommendation 32 (Control 145): That the CDMC draft a single policy or procedure around patch management and ensure it is implemented.

Recommendation 33 (Control 196 & 202): That a transition plan be compiled to ensure the successful implementation of HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512 in the environment as the XP SOE is replaced with the new EUC deployment.

Recommendation 34 (Control 210): That a transition plan be compiled to remove the SSL configurations from the DIE as the XP SOE is replaced with the EUC deployment.

Recommendation 35 (Control 211): That a transition plan be compiled to enable the implementation of TLS in the DIE as the XP SOE is replaced with the EUC deployment.

Recommendation 36 (Control 226): Update all SOPs to include a reference to report all suspicious activities.

7 Conclusion

Under the Gatekeeper PKI Framework, in accordance with Clause 11 of the Gatekeeper Head Agreement/Memorandum of Agreement, Defence must undertake annual compliance audits to retain Gatekeeper accreditation. Specifically the Digital Transformation Office (DTO) requires that Authorised Auditors conduct an audit of Service Providers' compliance with the Framework. Failure to conduct an annual Gatekeeper compliance audit represents a breach of the Gatekeeper Head Agreement/ Memorandum of Agreement and may result in termination of accreditation.

The Defence PKI provides both Certificate and Registration Authority services to support the Gatekeeper accredited PKI hierarchy. These certificates are used in the electronic identification of entities as representatives or affiliates of Defence and to provide authentication and secure online transactions. The processes used by Defence PKI to issue and revoke certificates require significant trust and it for these reasons that Defence PKI have continued to meet their annual assessment requirements.

As part of the Gatekeeper IRAP assessment, a total of 228 controls were assessed. These controls are categorised under the requirement areas of: Documentation (78 controls), Physical (51 controls), Logical (89 controls) and Personnel (10 controls). Of these requirement areas, the Defence PKI was deemed compliant with 65 Documentation controls, 51 (all) Physical controls, 72 Logical controls and 9 Personnel controls. Within the Gatekeeper Framework, non-compliance with a control is rated at one of four levels and increasing with severity: Minor, Partial, Major and Critical. In total, 31 controls were deemed non-compliant with the delineation being:

- Of the 13 Documentation controls deemed non-compliant, 4 had a severity rating of Minor, 6 had a severity rating of Partial, and 3 had a severity rating of Major.
- Of the 17 Logical controls deemed non-compliant, 16 had a severity rating of Partial and one (1) had a severity rating of Major.
- The single Personnel control deemed non-compliant had a severity rating of Partial.

This assessment also documented thirty six (36) Recommendations drawn from the review of the Documentation, Physical, Logical and Personnel Controls sections. The recommendations are consolidated as a single Recommendation could apply to multiple non-compliant Controls. Recommendations also do not exclusively apply to Non-Compliant controls and are included to improve the operations of the Defence PKI environment.

While there were 31 controls deemed non-compliant, none rated Critical; it is therefore the opinion of the IRAP Assessor that the functions of the Defence PKI are still sufficiently compliant with the Gatekeeper Framework that the Australian Department of Defence should retain its Gatekeeper Accreditation.

However, significant changes are currently being planned for the Defence PKI environment, such as the relocation of one of the operations centres and upgrades to DIE computing platforms. For these reasons, it is recommended that Gatekeeper Accreditation be granted for only 12 months to ensure that Defence revisit Gatekeeper Accreditation at the completion of these activities.

Appendix A: Non-Compliance to Documentation Controls

Section:	**Documentation Controls**				
Total Section Controls:	78	Compliant controls:	65	Non-compliant controls:	13

IRAP Assessor's comments		
No	Severity Rating	Comment
15	Minor	A Protective Security Risk Review for the DPKI environment *could* ensure an additional leverage of risk assessment that is supplemental to the extensive DPKI SRMP. Due to the existing DPKI SRMP for the Defence PKI environment, the severity rating for non-compliance to Control 15 is considered Minor. **Recommendation 5 (Control 15):** That the CDMC undertake and document a Protective Security Risk Review as a separate artefact.
21	Minor	By correlating the controls within the DPKI SRMP to the latest version of the ISM, the CDMC can identify a supplemental statement of risk and map the change to these risks through the changes to the specific sections of the ISM. As the risk and control mapping is considered supplemental, the severity rating for non-compliance to Control 21 is considered Partial. **Recommendation 7 (Control 21):** That future iterations of the SRMP specify which Controls within the ISM are relevant to the controls of SRMP.

Section:		Documentation Controls
29	Minor	By increasing the *Security Objectives* section listings in the DPKI SSP to include server and workstation security objectives, the CDMC can ensure that the key foundation elements of the Defence PKI environment are encompassed in the central plan that enforces security within the environment. As the majority of this control is covered, the severity rating for non-compliance to Control 29 is considered Minor. **Recommendation 9 (Control 29):** 29: That the CDMC update the Security Objectives section of the DPKI SSP to include the objectives for the Workstations and Servers.
30	Minor	The level of detailed required by this Control is not explicitly stated within the current DPKI SSP. The list of events is specified within the *Audit/Accountability* section of the DPKI SSP with a description of nightly archival but no real description of protection. Due to the existing coverage of archiving in the DPKI SSP, the severity rating for non-compliance to Control 30 is considered Minor. **Recommendation 10 (Control 30):** That the CDMC update the Audit/Accountability section of the DPKI SSP to include the ability to protect the logs. **Recommendation 11 (Control 30):** That the CDMC update the Audit/Accountability section of the DPKI SSP to include availability.
32	Major	The DPKI SSP does not specify or describe a centralised logging capability. By centralising the logging of a facility in one location, the control of the risks to this core function can be managed and monitored. As accountability, enabled by logging, is a central tenant to modern information security practices, the severity rating for non-compliance to Control 32 is considered Major. **Recommendation 12 (Control 32):** That the CDMC initiate the planning phase to centralise the logging of events.
33	Major	The severity rating for non-compliance to Control 33 inherits the non-compliance value for Control 32, Major. **Recommendation 13 (Control 33):** That once the CDMC implement a centralised logging capability, a reference that all systems will log to this location must be included within the DPKI SSP.

Section:		Documentation Controls
34	Partial	While policies such as the DPKI SSP and CDMC ICTSP state this, there was no specification of this requirement within the initial SOPs examined. As the frequent use of a SOP could ensure that the user is fully aware of the responsibility to report security incidents to the Security Officer, the severity rating for non-compliance to Control 34 is considered Partial. **Recommendation 14 (Control 34):** That the CDMC draft a standard statement to be inserted into all current and future SOPs that specifies that users report all suspicious events to the CDMC Security Officer.
43	Partial	While vulnerability management activities are undertaken, such as Nagios scanning and monitoring of the environment, without proper governance, there is the possibility that the activity could be neglected. Due to the existing but undocumented procedures being undertaken within the Defence PKI environment, the severity rating for non-compliance to Control 43 is considered Partial. **Recommendation 15 (Control 43 & 44):** That the CDMC draft a SOP that incorporates the Nagios scanning that is undertaken within the environment as well as any external to DPKI testing that occurs.
44	Partial	Without the relevant controls and methods as specified within control 43, the enforcement of control 44 cannot occur. The severity rating for non-compliance to Control 44 inherits the non-compliance value for Control 43, Partial.
45	Partial	Incident Response has been an evolving element within the Information Security Manual over the recent years, with the recent iteration focused on it being a mandatory requirement, a requirement that has been adapted by the Gatekeeper Competent Authority. While the Defence PKI environment has categorised elements of incident response into the Disaster Recovery and Business Continuity Plan (DRBCP), the lack of no explicit plan does mean no compliance with this control. As the PKI IRP will be central governance article for the support and management of incidents within the CDMC and Defence PKI, the DRAFT and non-finalised version of this article dictates the severity rating for non-compliance to Control 45 as Partial. **Recommendation 16 (Control 45):** That at the conclusion of the Gatekeeper Accreditation process, the DRAFT PKI IRP be accepted as final and versioned accordingly.

Section:		Documentation Controls
51	Partial	While reporting to ASD should be updated to include the CSIR scheme, it is essential that the Gatekeeper Competent Authority is also a party that incidents are reported to. While it is central responsibility that the reporting of incidents to the relevant authorities occurs, the inability of the GCA to immediately influence the outcome of an incident within the Defence PKI environment validates the severity rating for non-compliance to Control 51 as Partial. **Recommendation 17 (Control 51):** That the CDMC updates the DRBCP to reference the ASD Cyber Security Incident Reporting (CSIR) reporting mechanism. **Recommendation 18 (Control 51):** That the CDMC updates the DRBCP to reference reporting cyber security events to the Gatekeeper Competent Authority. **Recommendation 19 (Control 51):** That the CDMC ensures that the new IRP reference the ASD CSIR reporting mechanism and the Gatekeeper Competent Authority.
53	Partial	The severity rating for non-compliance to Control 53 inherits the non-compliance value for Control 45, Critical. **Recommendation 20 (Control 53):** That the created CDMC IRP reference the notification process of vendors to the CDMC of detected or suspected vulnerabilities within the CDMC networks and equipment.
63	Major	Urgent or emergency changes are undertaken in response to significant threats to the Defence PKI environment, for this reason, the accountability and reason for these actions, must be documented and guided by governance considerations. As urgent or emergency changes are not within a governance article describing the actions for these changes within the CDMC and Defence PKI, the lack of this article dictates the severity rating for non-compliance to Control 63 as Major. **Recommendation 21 (Control 63):** That the CDMC ICTSP and the PKI SSP be updated to include a specific reference to the emergency change management procedures.

Appendix B: Non-Compliance to Physical Controls

No non-compliance to Physical Controls was identified during the assessment.

Appendix C: Non-Compliance to Logical Controls

Section:	**Logical Controls**				
Total Section Controls:	89	Compliant controls:	72	Non-compliant controls:	17
IRAP Assessor's comments					

No	Severity Rating	Comment
127	Partial	The management console operating system, Windows XP, is no longer a supported platform. Defence however has initiated additional vendor support from Microsoft to continue. However, this software should still be considered not supported, as vulnerabilities within the application layer may have no applicable patches that are provided to prevent presently discovered vulnerabilities within the operating systems. The risk of not being able to implement this control however is mitigated through the minimal exposure of the PKI support environment to exploitation mechanisms, such as segmented network environment. Due to this enforced supporting of legacy protocols and operating systems by the CDMC and Defence PKI but with planned mitigations and migrations, the severity rating for non-compliance to Control 127 is considered Partial. **Recommendation 29 (Control 127, 128, 129, 130, 131, 132, 134, 135, 136, 142 & 143):** That the CDMC PKI support infrastructure be an immediate candidate for the replacement of Windows XP. **Recommendation 30 (Control 127, 128, 129, 130, 131, 132, 134, 135, 136, 142 & 143):** That the CDMC be allowed to implement their own updated SOE to upgrade PKI support infrastructure independent of the replacement of Windows XP project.

Section:	Logical Controls	
128	Partial	The management console operating system, Windows XP, used as the desktop environment does not have a native ability to apply Application Whitelisting. The risk of not being able to implement this control however is mitigated through the minimal exposure of the PKI support environment to exploitation mechanisms, such as segmented network environment. Due to this enforced supporting of legacy protocols and operating systems by the CDMC and Defence PKI but with planned mitigations and migrations, the severity rating for non-compliance to Control 128 is considered Partial.
129	Partial	The severity rating for non-compliance to Control 129 inherits the non-compliance value for Control 128, Partial.
130	Partial	The severity rating for non-compliance to Control 130 inherits the non-compliance value for Control 128, Partial.
131	Partial	The severity rating for non-compliance to Control 131 inherits the non-compliance value for Control 128, Partial.
132	Partial	The severity rating for non-compliance to Control 132 inherits the non-compliance value for Control 128, Partial.
134	Partial	The management console operating system, Windows XP, is no longer a supported platform. As it is not supported, there are no applicable patches that are provided to prevent presently discovered vulnerabilities within the operating systems. The risk of not being able to implement this control however is mitigated through the minimal exposure of the PKI support environment to exploitation mechanisms, such as segmented network environment. Due to this enforced supporting of legacy protocols and operating systems by the CDMC and Defence PKI but with planned mitigations and migrations, the severity rating for non-compliance to Control 134 is considered Partial.
135	Partial	The severity rating for non-compliance to Control 135 inherits the non-compliance value for Control 134, Partial.
136	Partial	The severity rating for non-compliance to Control 135 inherits the non-compliance value for Control 134, Partial.
138	Partial	The severity rating for non-compliance to Control 135 inherits the non-compliance value for Control 134, Partial. **Recommendation 31 (Control 138):** That the CDMC draft a single policy or procedures around patch management.

Section:		Logical Controls
142	Partial	The severity rating for non-compliance to Control 135 inherits the non-compliance value for Control 134, Partial.
143	Partial	The severity rating for non-compliance to Control 135 inherits the non-compliance value for Control 134, Partial.
145	Major	The lack of patch management strategy could introduce the possibility of exploitation through an uncontrolled or non-response to a vulnerability within the Defence PKI environment or network. Due to this lack of key policy to support the logical controls within the CDMC and Defence PKI, the severity rating for non-compliance to Control 145 is considered Major. **Recommendation 32 (Control 145):** That the CDMC draft a single policy or procedure around patch management and ensure it is implemented.
196	Partial	While SHA-1 is no longer an approved AACA, the Defence PKI environment continues to support this algorithm for legacy purposes only. A migration plan exists for the full transition once support for legacy systems, including Windows XP is no longer required. Due to this enforced supporting of legacy protocols and operating systems by the CDMC and Defence PKI but with planned mitigations and migrations, the severity rating for non-compliance to Control 196 is considered Partial. **Recommendation 33 (Control 196 & 202):** That a transition plan be compiled to ensure the successful implementation of HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512 in the environment as the XP SOE is replaced with the new EUC deployment.
202	Partial	The severity rating for non-compliance to Control 202 inherits the non-compliance value for Control 196, Partial.
210	Partial	While SSL is stated extensively within the documentation, the later versions of TLS (1.1 and 1.2) are not supported on Windows XP. Therefore the support for this legacy algorithm is required until Defence DIE transitions to a later edition of Windows that supports later versions of TLS. Due to this enforced supporting of legacy protocols and operating systems by the CDMC and Defence PKI but with planned mitigations and migrations, the severity rating for non-compliance to Control 210 is considered Partial. **Recommendation 34 (Control 210):** That a transition plan be compiled to remove the SSL configurations from the DIE as the XP SOE is replaced with the EUC deployment.

Section:		Logical Controls
211	Partial	The severity rating for non-compliance to Control 211 inherits the non-compliance value for Control 210, Partial. **Recommendation 35 (Control 211):** That a transition plan be compiled to enable the implementation of TLS in the DIE as the XP SOE is replaced with the EUC deployment.

Appendix D: Non-Compliance to Personnel Controls

Section:	**Personnel Controls**				
Total Section Controls:	10	Compliant controls:	9	Non-compliant controls:	1

IRAP Assessor's comments		
No	Severity Rating	Comment
226	Partial	The examined SOPs did not explicitly state what to do in the event of an incident. However the coverage within the *ICT Security Incident Response* section of the CDMC ICTSP and the *Security Administration* section of the PKI SSP does instruct the user on the requirements to report incidents. Due to the importance of user being aware of their role in reporting incidents within the Defence PKI environment but some existing instances of this requirement being documented, the severity rating for non-compliance to Control 226 is considered Partial. **Recommendation 36 (Control 226):** Update all SOPs to include a reference to report all suspicious activities.

Appendix E: Documents Reviewed

Version	Title	Date
1.0	Defence Public Key Infrastructure Levels of Assurance Requirements Certificate Policy Object Identifiers (OIDs)	November 2014
5.1	X.509 Certification Practice Statement for the Australian Department of Defence	December 2014
5.1	X.509 Certificate Policy for the Australian Department of Defence Root Certification Authority and Subordinate Certificate Authorities	May 2014
3.1	X.509 Certificate Policy for the Australian Department of Defence Root Interoperability Certificate Authority	May 2014
4.0	X.509 Certificate Policy for the Australian Department of Defence Individual – Hardware Certificates (High Assurance)	May 2014
4.0	X.509 Certificate Policy for the Australian Department of Defence Individual – Software Certificates (Medium Assurance)	May 2014
4.0	X.509 Certificate Policy for the Australian Department of Defence Secure Communications Certificates	May 2014
4.0	X.509 Certificate Policy for the Australian Department of Defence Automatic Enrolment Resource Certificates	May 2014
4.1	X.509 Certificate Policy for the Australian Department of Defence Network Resource Certificates	October 2014
4.0	X.509 Certificate Policy for the Australian Department of Defence Code Signing Resource Certificates	May 2014
2.0	X.509 Certificate Policy for the Australian Department of Defence Timestamp Authority	May 2014
4.0	Public Key Infrastructure Disaster Recovery and Business Continuity Plan (PKI DRBCP)	November 2014
7.3	Defence Public Key Infrastructure Security Risk Management Plan (PKI SRMP)	January 2016
4.0	Certificate and Directory Management Centre Information and Communications Technology Security Policy (CDMC ICTSP)	December 2014
5.0	Australian Department of Defence Public Key Infrastructure System Security Plan (SSP)	December 2014
4.0	Australian Department of Defence Public Key Infrastructure Operations Manual	November 2014
1.2	Certificate and Directory Management Centre – Certificate Management – PKI Passphrase Management Procedures	August 2012
5.2	Public Key Infrastructure Key Management Plan (PKI KMP)	January 2016
---	PKI-009 – PKI Staff Access Registration	March 2012
---	PKI-010 – PKI Smartcard/Key Access Register	April 2008
---	PKI-012 – Trusted Element Form	August 2013
---	PKI-017 – Trusted Element Register	January 2008

Version	Title	Date
1.2	Defence PKI Subscriber Deed of Agreement	---
---	Daily_Weekly_System Operation Task-Checklist _Current	December 2014
1.1	Certificate and Directory Management Centre – Certificate Management – PKI System 2048 Upgrade Guide	July 2010
2.0	Computer Network & Data Security Operations – CDMC Platform Support – CDMC Antivirus – Officescan 10.0 – SOE 125 – Upgrade Installation and Configuration	November 2012
1.1	Certificate and Directory Management Centre – Certificate Management – PKI Installation Checklist	June 2011
1.1	Defence ASA build procedure	July 2010
1.1	Certificate and Directory Management Centre – Certificate Management – PKI Standalone Server Build – RCA (PKISSN02/PKISSNN22) – Build – PKI Services	July 2010
0.1	Public Key Infrastructure Incident Response Plan	DRAFT