

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1



Australian Government
Department of Defence

Defence Signals Directorate

Gatekeeper Guidelines & Checklist

VERSION 3.0.1

Point of Contact: Computer Network Vulnerability Team

Phone: (02) 6265 0197

Email: assist@dsd.gov.au

Organisation: _____

Assessor: _____

© Commonwealth of Australia 2008

This work is copyright. You may download, display, print and reproduce this material in unaltered form only (retaining this notice) for your personal, non-commercial use or use within your organisation. Apart from any use as permitted under the *Copyright Act 1968*, all other rights are reserved.

Page 1

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

© Commonwealth of Australia 2008

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

Document Change Record

Version	Changed By	Date	Changes
2.0	Advice and Assistance	13/05/2004	Convert to checklist with policy consistency check.
2.0.1	Advice and Assistance	14/10/2005	Update for September 2005 ACSI 33 and PSM 2005.
2.0.2	Department of Finance and Deregulation (Finance)	25/10/06	Update for Gatekeeper PKI Framework
3.0	Computer Network Vulnerability Team – Defence Signals Directorate	27/06/2008	Update for Gatekeeper PKI Framework and September 2007 ACSI 33.
3.0	Authentication/Gatekeeper team - Finance	3/07/2008	Further updates to key management sections to correct references and make consistent with ACSI33
3.0.1	Computer Network Vulnerability Team – Defence Signals Directorate	5/09/2008	Release version

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

Table of Contents

Document Change Record2
Table of Contents.....3
Introduction.....4
 Purpose.....4
 Related Documentation.....4
 Key Words.....5
 Definitions.....5
Certification.....7
 Checklist Guidance8
 Requirements8
 Sub-requirements9
 When to tick or cross9
 Waivers10
 Checking the implementation10
 Comments10
 Certification Report10
 Covering Letter11
1.0 Documents reviewed as part of the certification12
 1.1 Criteria to be met as part of the Certification Authority (CA) certification13
 1.2 Criteria to be met as part of the Registration Authority (RA) certification.....14
2.0 Security Profile.....14
 2.1 Security Policy.....14
 2.2 Risk Assessment.....20
 2.3 Security Plan21
 2.4 Key Management Plan29
3.0 Review Implementation.....30
 3.1 Review the Implementation of the Security Plan31
4.0 Technology Evaluation32
 4.1 Review Evaluation Status of Certification Authority/Registration Authority Technology .32
Comments.....33

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

Introduction

Applicants for Gatekeeper Accreditation/Recognition undergo rigorous evaluation of all aspects of their proposed operations, including compliance with physical, logical and technology security and operational procedures. This document includes a compliance Checklist to assist Infosec-Registered Assessor Program (I-RAP) assessors when reviewing an Organisation's risk assessment and security practices.

Purpose

The purpose of this document is to provide I-RAP assessors conducting the certification process for Gatekeeper accreditation/recognition with:

- ◆ guidelines on Gatekeeper requirements for accreditation/recognition; and
- ◆ a Checklist of security practices that an organisation is required to comply for Gatekeeper accreditation/recognition.

Related Documentation

Organisations and I-RAP assessors are encouraged to seek further guidance from the following documents:

- The Australian Government Information & Communication Technology Security Manual (ACSI 33) September 2007, Information Security Branch, Defence Signals Directorate.
- The Protective Security Manual (PSM) 2005, Attorney General's Department.
- AS/NZS 4360:2004 Risk Management, Standards Australia.
- HB 231:2004 Information Security Risk Management Guidelines, Standards Australia
- HB 436:2004 Risk Management Guidelines, Standards Australia.
- Certification Authority Accreditation Criteria, 2008, Australian Government Information Management Office, (AGIMO), Department of Finance and Deregulation, (Finance),
- Registration Authority Accreditation Criteria, 2008, Finance
- Security Guidebook, 2008, Finance
- Security Profile Guidance for Certification Authorities and Registration Authorities, 2008, Finance

The complete set of Gatekeeper documentation can be found at www.gatekeeper.gov.au

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

Key Words

The table below defines the keywords used within this document to indicate the compulsory requirements for DSD or I-RAP certification.

Keyword	Interpretation
MUST	The item is mandatory for certification.
MUST NOT	Non-use is mandatory for certification.
SHOULD	<p>Valid reasons to deviate from the requirement may exist in particular circumstances. The full implications need to be considered before choosing a different course and the deviation needs to be approved by an authorised organisation security representative.</p> <p>Note: Organisations deviating from a SHOULD, MUST document (ACSI 33 1.1.26):</p> <ul style="list-style-type: none">• the reasons for the deviation;• an assessment of the residual risk resulting from the deviation;• the acceptance of the risk by a responsible authority;• a date by which to review the decision;• the IT Security Adviser's (ITSA's) involvement in the decision; and• management's approval. <p>DSD RECOMMENDS that ITSAs retain a copy of all deviations.</p>
SHOULD NOT	<p>Valid reasons to implement the item may exist in particular circumstances. The full implications need to be considered before choosing a different course and the deviation needs to be approved by an authorised organisation security representative.</p> <p>Note: Organisations deviating from a SHOULD NOT, MUST document (ACSI 33 1.1.26):</p> <ul style="list-style-type: none">• the reasons for the deviation;• an assessment of the residual risk resulting from the deviation;

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

	<ul style="list-style-type: none">• the acceptance of the risk by a responsible authority;• a date by which to review the decision;• the ITSA's involvement in the decision; and• management's approval. <p>DSD RECOMMENDS that ITSAs retain a copy of all deviations.</p>
RECOMMENDS RECOMMENDED	<p>A recommendation or suggestion.</p> <p>Note: Organisations deviating from a RECOMMENDS or RECOMMENDED, are encouraged to document the reason(s) for doing so.</p>

Definitions

The Glossary at <http://www.finance.gov.au/e-government/security-and-authentication/gatekeeper/docs/Glossary.pdf> provides a comprehensive list of additional definitions.

1. **Public Key Infrastructure (PKI)** is the combination of hardware, software, people, policies and procedures needed to create, manage, store and distribute Keys and Certificates based on public Key cryptography.
2. A **Certification Authority (CA)** is a Service Provider that digitally signs X.509 v3 Digital Certificates (which may or may not include Key Generation) using its Private Key.
3. A **Registration Authority (RA)** is a Service Provider that:
 - is responsible for the registration of applicants for Digital Certificates by checking Evidence of Identity (EOI) documentation submitted by the applicant for its compliance with Gatekeeper EOI Policy;
 - is responsible for the provision of completed and authorised application form including copies of the submitted EOI documents to the relevant CA; and
 - may be responsible for the secure distribution of signed Digital Certificates to Subscribers.
4. **Service Provider** is a Gatekeeper Accredited or Recognised entity.
5. **Organisation** is a generic term used to refer to a business entity or government agency that is either seeking or has been granted Gatekeeper Accreditation/Recognition.
6. **Facility Security Officer (FSO)** is that individual responsible for the overall security (physical and logical) of a Service Provider's PKI operations. The FSO

Page 6

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

may or may not be the IT Security Adviser (ITSA).

Certification

I-RAP assessors **MUST** forward the following documents to the Gatekeeper Competent Authority (Attention: Director Gatekeeper) in Finance and the DSD I-RAP Manager once the assessment is completed:

- completed checklist;
- additional requirements;
- checklist comments; and
- Certification Report with Covering Letter

The DSD I-RAP Manager's address details are:

The I-RAP Manager
Information Security Branch
Defence Signals Directorate
Locked Bag 5076
KINGSTON ACT 2604

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

The Gatekeeper Competent Authority address details are:

The Gatekeeper Competent Authority
General Manager
Australian Government Information Management Office (AGIMO)
Department of Finance and Deregulation
John Gorton Building
King Edward Terrace
PARKES ACT 2600

Attention Director, Gatekeeper

Checklist Guidance

This section provides guidance upon answering items within the checklist and details the obligations of the assessor.

Checklist requirements must not be scoped out during a review.

Where an Organisation titles its policy documents in a manner different to that specified in the Gatekeeper PKI Framework, the assessor must ensure that there is an appropriate congruence between the relevant documents.

Requirements

Each checklist consists of requirements, designated as a bolded capital 'R' followed by an outline number. The complete requirement consists of: the requirement number, the requirement itself, and a checkbox.

For example:

R2 All systems MUST be covered by an ICT Security Policy document (ICTSP) (ACSI 33 2.4.5).	<input type="checkbox"/>
--	--------------------------

Bolded, capitalised words are key words, as described above. Key words stipulate a condition upon the requirement, and must be considered when deciding whether a requirement has or has not been met by an organisation.

Assessors should either tick or cross each requirement to indicate that an organisation has succeeded or failed in answering the requirement. The reviewer should record any comments using the comments table that is attached at the end of this checklist. Comments must be submitted with the checklist documentation.

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

Bracketed information towards the end of a requirement's wording implies a reference. The material that is referenced should be examined if further detail or justification of a requirement and any nearby requirements is required.

Sub-requirements

Some requirements are categorised into sub-requirements. Sub-requirements are designated with a two-level number, and a parent requirement from which all sub-requirements stem.

For example:

R16 Areas designated as NLZ areas MUST (ACSI 33 3.1.19):	
R16.1 be suitably sign-posted; and	<input type="checkbox"/>
R16.2 have all entry and exit points appropriately secured.	<input type="checkbox"/>

The key word in the parent item '**MUST**' applies to all sub-requirements. Organisations must achieve a tick in each sub-requirement box in order to satisfy the parent requirement.

Consider another example:

R84 Standard procedures for all personnel with access to the system SHOULD include the requirement to notify the ITSA of (ACSI 33 2.8.28):	
R84.1 any data spillage; and	<input type="checkbox"/>
R84.2 access to any data classified above that for which they are authorised.	<input type="checkbox"/>

The key word in the parent item '**SHOULD**' applies to all sub-requirements, just like the first sub-requirement example given. Organisations must achieve a tick in each sub-requirement box in order to satisfy the parent requirement. This statement should be considered in light of the guidance provided in 'When to tick or cross'.

When to tick or cross

Ticks need only be given where the key word of the requirement is properly addressed.

For a '**MUST / MUST NOT**' you should tick when:

- The requirement is complied with explicitly.

For a '**SHOULD / SHOULD NOT**' you should tick when:

- The requirement is complied with explicitly; or
- Valid reasons exist for non-compliance and the deviation process outlined above has been completed.

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

For a **'RECOMMENDS'** or any of its derivations you should tick when:

- The requirement is complied with explicitly; or
- Valid reasons exist for non-compliance and these reasons are provided to the certifying authority.

You should mark a requirement with a cross in all other situations.

Waivers

Where a waiver has been granted either by Finance or DSD in relation to any aspect of a Service Provider's Gatekeeper PKI operations, the assessor must sight the document and make appropriate allowance for the waiver in the evaluation, and indicate this in the Certification Report and in the relevant section of the Checklist.

Checking the implementation

Assessors must verify consistency between policy, plans, and procedures. In order to verify that procedures mentioned within policy documentation are operational, assessors must have the organisation demonstrate that the procedure is in use.

Comments

Provision is made at the back of the checklist for I-RAP assessors to provide their comments against individual requirements. Specific guidance on using the comments section is provided just prior to the comments table. Comments are also to be used for providing justification for decisions.

I-RAP assessors must comment upon individual requirements within the checklist. Comments must provide an indication of how well the organisation complies with each requirement.

Certification Report

The assessor must:

- prepare a Certification Report based on the review tasks detailed in this document, irrespective of whether or not certification is issued;
- provide any recommendations based on non-mandatory best practice guidelines that have not been demonstrated by the Organisation;
- consider whether to issue certification, provisional certification or no certification. A failed evaluation must result in denial of certification.

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

A failed evaluation is one where, in the opinion of the assessor, the Organisation's implementation of its security policies and procedures, EITHER does not adequately mitigate the threats and risks identified in the Risk Assessment OR does not satisfy the requirements of ACSI 33 or the PSM.

In reaching this decision, the assessor should have due regard to the nature of the PKI services provided by the Organisation and the importance of maintaining a balance between commercial and security considerations.

Where certification is not recommended, the Certification Report to the Gatekeeper Competent Authority and DSD should identify remedial action that could be undertaken to address the non-compliances, which if taken should result in the issuing of certification.

The formal I-RAP Certification Report must include signoff from the Organisation's Facility Security Officer (FSO), stating that to the best of the FSO's knowledge, the I-RAP assessor who has signed the Certification Report has actively participated in conducting the assessment work leading to certification.

A copy of the counter-signed Certification Report must be provided to the Organisation.

Covering Letter

The Covering Letter to the Certification Report must advise the Gatekeeper Competent Authority whether or not the CA has successfully completed the Gatekeeper certification process as per Gatekeeper requirements. A copy of the counter-signed Certification Report must be included with the Covering Letter.

Where the Organisation has failed the certification process, the letter and the report should specify what remedial action is required to be undertaken by the Organisation in order to achieve successful certification.

A copy of the Covering Letter should also be provided to the Organisation.

1.0 Documents reviewed as part of the certification

Document or policy names may vary in name. The assessor should place more emphasis on establishing if policy has been developed and is being implemented than on whether or not documents are named in strict accordance with this document. Documents **MUST** include the title, version number and date.

The Security Profile (SEC1) is a core document that must be prepared and maintained by all Gatekeeper Accredited/Recognised Service Providers. It is a self contained document that addresses all elements of the Service Provider's physical, logical and personnel security. It will also contain, as applicable, links to other documents such as the Certification Practices Statement (CPS), CA/RA Operations Manual and the Disaster Recovery and Business Continuity Plan (DRBCP).

The intent of the Security Profile is to apply a logical progression from threat and risk assessment through to high level security policies and plans that address all aspects of the Service Provider's security (i.e. physical, personnel, and information technology).

The assessor should sight the Operations Manual and DRBCP, and confirm that they contain the requisite information and are appropriately cross referenced in the Security Profile.

The DRBCP and Operations Manuals are integrally linked to the Security Profile, but are regarded as essentially procedures manuals for employees.

These documents are reviewed by Finance for consistency with the Security Profile and public facing documents such as the Certification Practices Statement as part of the accreditation process.

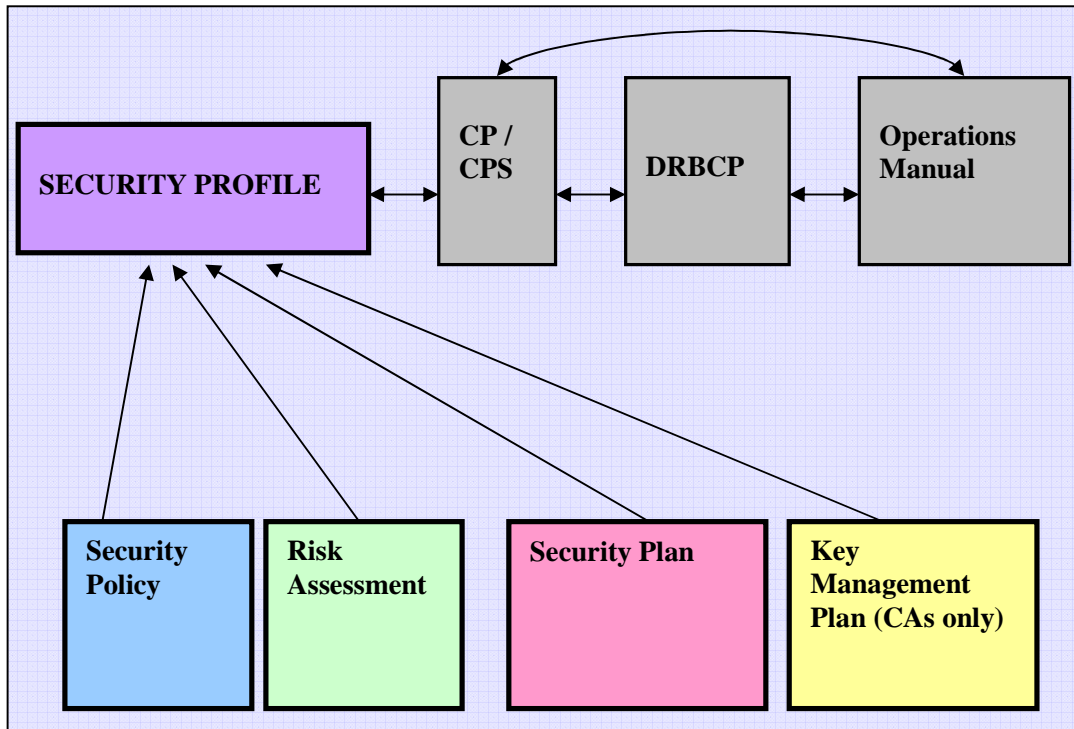


Figure 1 Gatekeeper Documentation

1.1 Criteria to be met as part of the Certification Authority (CA) certification

For a CA certification, the criteria to be met and the associated review tasks are indicated below.

Table 1: CA Criteria

The organisation MUST comply with criterion	demonstrated by completing the review task(s) in Sections
Security Profile (SEC1) Including review of the evaluation status of the CA Technology	2.1–Security Policy 2.2–Risk Assessment 2.3–Security Plan 2.4–Key Management Plan 3.1–Review the Implementation of the Security Plan 4.1–Review Evaluation Status of Certification Authority/Registration Authority Technology

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

1.2 Criteria to be met as part of the Registration Authority (RA) certification

For a RA certification, the criteria to be met and the associated review tasks are indicated below.

Table 2: RA Criteria

The organisation MUST comply with criterion	demonstrated by completing the review task(s) in Sections
Security Profile (SEC1)	2.1–Security Policy 2.2–Risk Assessment 2.3–Security Plan 3.1–Review the Implementation of the Security Plan

2.0 Security Profile

The Security Profile will contain the following broad elements:

- Security Policy
- Documented Risk Assessment
- Security Plan (for physical and personnel security)
- Key Management Plan

Within these broad elements, the Security Profile will also include a review of the CA/RA technology and Facility Security Officer's role and responsibilities and the security clearance level.

2.1 Security Policy

An Organisation's Security Policy describes its approach to the security of information management, defines information security management responsibilities and its commitment to information security. It addresses the intended security objectives relating to personnel, access controls, business continuity, protection of services, assets and business processes. These objectives are linked to the Organisation's threat and risk assessment.

R1 For CAs the Security Policy element of the Security Profile (SEC1) MUST include all security objectives from the Certification Practice Statement (CPS). These objectives also need to be reflected in Certificate Policies (CP). Evaluation of the CP and the CPS is outside the scope of the I-RAP review.	<input type="checkbox"/>
R2 All systems MUST be covered by an ICT Security Policy document (ICTSP) (ACSI 33 2.4.5).	<input type="checkbox"/>
R3 All systems SHOULD be covered by a System Security Plan (SSP) (ACSI 33 2.4.7).	<input type="checkbox"/>
R4 Organisations SHOULD ensure that the SRMP, ICTSP, SSP and Standard Operating Procedures (SOPs) are logically connected and consistent for each system (ACSI 33 2.4.12).	<input type="checkbox"/>

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

R5 All ICT security documents SHOULD be formally approved and signed off by an appropriate person (ACSI 33 2.4.15).	<input type="checkbox"/>
R6 Organisations MUST use the classification scheme defined in the PSM Part C.	<input type="checkbox"/>
Access Control:	
R7 Organisations MUST specify the level of security clearance and briefings required for each type of user given system access/accounts (ACSI 33 3.2.13).	<input type="checkbox"/>
R8 DSD RECOMMENDS clearing privileged users to a level one classification above the classification of the system to which they have privileged access (ACSI 33 3.2.15).	<input type="checkbox"/>
R9 As a minimum, all privileged users MUST (ACSI 33 2.1.25):	
R9.1 comply with the relevant policies, plans and procedures for the system they are using;	<input type="checkbox"/>
R9.2 possess a security clearance at least equal to the highest classification of information processed on the system;	<input type="checkbox"/>
R9.3 protect the authenticators for privileged accounts at the highest level of information it secures; Example: Passwords for root and administrator accounts.	<input type="checkbox"/>
R9.4 not share authenticators for privileged accounts without approval;	<input type="checkbox"/>
R9.5 be responsible for all actions under their privileged accounts;	<input type="checkbox"/>
R9.6 use privileged access only to perform authorised tasks and functions; and	<input type="checkbox"/>
R9.7 report all potentially security-related information system problems to the ITSA.	<input type="checkbox"/>
R10 Organisations MUST (ACSI 33 2.1.26):	
R10.1 restrict privileged access to the minimum required to fulfil designated roles; and	<input type="checkbox"/>
R10.2 closely audit privileged access.	<input type="checkbox"/>
R11 Access Policy SHOULD ensure that (ACSI 33 3.6.21):	
R11.1 administrators are assigned an individual account for the performance of their administration tasks;	<input type="checkbox"/>
R11.2 privileged accounts are kept to a minimum; and	<input type="checkbox"/>
R11.3 privileged accounts are used for administrative work only.	<input type="checkbox"/>
R12 Organisations SHOULD (ACSI 33 3.7.19):	
R12.1 maintain a secure log of all authorised users, their user identification and who provided the authorisation and when; and	<input type="checkbox"/>
R12.2 maintain the log for the life of the system.	<input type="checkbox"/>
R13 DSD RECOMMENDS that multiple methods are combined for authenticating users (ACSI 33 3.6.7).	<input type="checkbox"/>
Physical Security and Media Control:	

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

<p>R14 Gatekeeper Accredited/Recognised Service Providers MUST locate and operate their PKI facilities within Australia. A Gatekeeper Accredited CA MUST NOT have its Root Certification Authority (RCA) located outside Australia. Where a CA is Gatekeeper Recognised; it may have its RCA located in one of the following countries: Canada, New Zealand, the United Kingdom or the USA.</p>	<input type="checkbox"/>																												
<p>R15 DSD RECOMMENDS that areas containing significant Gatekeeper equipment be designated and operated as No-Lone-Zone (NLZ) areas (ACSI 33 3.1.19).</p>	<input type="checkbox"/>																												
<p>R16 Areas designated as NLZ areas MUST (ACSI 33 3.1.19):</p>	<input type="checkbox"/>																												
<p>R16.1 be suitably sign-posted; and</p>	<input type="checkbox"/>																												
<p>R16.2 have all entry and exit points appropriately secured.</p>	<input type="checkbox"/>																												
<p>R17 The following matrix details the level of information storage required in each defined area within a Gatekeeper Accredited Service Provider’s facility.</p>	<input type="checkbox"/>																												
<p>Please note that these areas are only a guide to the areas that may be found in each type of facility.</p>																													
<table border="1"> <thead> <tr> <th data-bbox="234 813 651 875">Typical Areas</th> <th data-bbox="651 813 903 875">CA</th> <th data-bbox="903 813 1155 875">KCOs/TROs</th> <th data-bbox="1155 813 1407 875">RA</th> </tr> </thead> <tbody> <tr> <td data-bbox="234 875 651 940">Ceremony Room</td> <td data-bbox="651 875 903 940">HP/SECRET</td> <td data-bbox="903 875 1155 940" style="background-color: #cccccc;"></td> <td data-bbox="1155 875 1407 940" style="background-color: #cccccc;"></td> </tr> <tr> <td data-bbox="234 940 651 1005">Key Generation Room</td> <td data-bbox="651 940 903 1005">HP/SECRET</td> <td data-bbox="903 940 1155 1005">HP</td> <td data-bbox="1155 940 1407 1005" style="background-color: #cccccc;"></td> </tr> <tr> <td data-bbox="234 1005 651 1070">Server Room</td> <td data-bbox="651 1005 903 1070">HP/SECRET</td> <td data-bbox="903 1005 1155 1070">HP</td> <td data-bbox="1155 1005 1407 1070" style="background-color: #cccccc;"></td> </tr> <tr> <td data-bbox="234 1070 651 1135">Operations Area</td> <td data-bbox="651 1070 903 1135">HP</td> <td data-bbox="903 1070 1155 1135">HP</td> <td data-bbox="1155 1070 1407 1135">X-IN-CONF</td> </tr> <tr> <td data-bbox="234 1135 651 1200">General Office</td> <td data-bbox="651 1135 903 1200">X-IN-CONF</td> <td data-bbox="903 1135 1155 1200">X-IN-CONF</td> <td data-bbox="1155 1135 1407 1200">X-IN-CONF</td> </tr> <tr> <td data-bbox="234 1200 651 1265">Reception Area</td> <td colspan="2" data-bbox="651 1200 1155 1265">HP</td> <td data-bbox="1155 1200 1407 1265" style="background-color: #cccccc;"></td> </tr> </tbody> </table>		Typical Areas	CA	KCOs/TROs	RA	Ceremony Room	HP/SECRET			Key Generation Room	HP/SECRET	HP		Server Room	HP/SECRET	HP		Operations Area	HP	HP	X-IN-CONF	General Office	X-IN-CONF	X-IN-CONF	X-IN-CONF	Reception Area	HP		
Typical Areas	CA	KCOs/TROs	RA																										
Ceremony Room	HP/SECRET																												
Key Generation Room	HP/SECRET	HP																											
Server Room	HP/SECRET	HP																											
Operations Area	HP	HP	X-IN-CONF																										
General Office	X-IN-CONF	X-IN-CONF	X-IN-CONF																										
Reception Area	HP																												
<p>A Ceremony Room is a term used to describe that part of a CA’s facility where new CAs are generated.</p>																													
<p>Depending on location, position and the operational requirements (including certificate type) within the facility, reception areas may need security increased if they are providing access control and validation services.</p>																													

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

R18	Required minimum physical security treatments are: <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th style="width: 30%;">Typical Areas</th> <th style="width: 15%;">CA</th> <th style="width: 15%;">KCOs/TROs</th> <th style="width: 15%;">RA</th> </tr> </thead> <tbody> <tr> <td>Ceremony Room</td> <td>SA</td> <td style="background-color: #cccccc;"></td> <td style="background-color: #cccccc;"></td> </tr> <tr> <td>Key Generation Room</td> <td style="background-color: #cccccc;"></td> <td>SA</td> <td style="background-color: #cccccc;"></td> </tr> <tr> <td>Server Room</td> <td>SA</td> <td>SA</td> <td style="background-color: #cccccc;"></td> </tr> <tr> <td>Operations Area</td> <td>SA/IR</td> <td>SA/IR</td> <td>IR</td> </tr> <tr> <td>General Office</td> <td>IR*¹</td> <td>IR*¹</td> <td>IR*¹</td> </tr> <tr> <td>Security Control Room</td> <td>IR*²</td> <td>IR*²</td> <td style="background-color: #cccccc;"></td> </tr> <tr> <td>Reception Area</td> <td>IR*³</td> <td>IR*³</td> <td style="background-color: #cccccc;"></td> </tr> <tr> <td>Pedestrian Entry/Exit</td> <td>IR</td> <td>IR</td> <td>IR</td> </tr> </tbody> </table> <p style="margin-top: 10px;">Note: SA – Secure Area IR – Intruder Resistant</p> <p>*¹ Dependant on location, position and the operational requirements (including digital certificate type) within the facility and public/visitor access and staff separation.</p> <p>*² Dependant on location, position and the operational requirements (including digital certificate type) within the facility. Reception areas may need security increased to Secure Area Standards incorporating ballistic ratings based on Security Risk Assessment.</p> <p>*³ Dependant on location, position and the operational requirements (including digital certificate type) within the facility and public/visitor access and staff separation.</p>	Typical Areas	CA	KCOs/TROs	RA	Ceremony Room	SA			Key Generation Room		SA		Server Room	SA	SA		Operations Area	SA/IR	SA/IR	IR	General Office	IR* ¹	IR* ¹	IR* ¹	Security Control Room	IR* ²	IR* ²		Reception Area	IR* ³	IR* ³		Pedestrian Entry/Exit	IR	IR	IR	<input type="checkbox"/>
Typical Areas	CA	KCOs/TROs	RA																																			
Ceremony Room	SA																																					
Key Generation Room		SA																																				
Server Room	SA	SA																																				
Operations Area	SA/IR	SA/IR	IR																																			
General Office	IR* ¹	IR* ¹	IR* ¹																																			
Security Control Room	IR* ²	IR* ²																																				
Reception Area	IR* ³	IR* ³																																				
Pedestrian Entry/Exit	IR	IR	IR																																			
R19	The following minimum standards for storage of classified information MUST be complied with: <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 10px;"> <thead> <tr> <th style="width: 25%;">Gatekeeper Storage Requirements</th> <th style="width: 15%;">Secure Area</th> <th style="width: 15%;">Partially Secure Area</th> <th style="width: 15%;">Intruder Resistant Area</th> </tr> </thead> <tbody> <tr> <td>Secret or Highly Protected</td> <td>B</td> <td>A</td> <td>A</td> </tr> <tr> <td>Confidential or Protected</td> <td>C¹</td> <td>B</td> <td>B</td> </tr> <tr> <td>Restricted or X-In-Confidence</td> <td>Discretionary</td> <td>Lockable Cabinet</td> <td>Lockable Cabinet</td> </tr> <tr> <td>CRYPTO</td> <td>See note ²</td> <td>See note ²</td> <td>See note ²</td> </tr> </tbody> </table> <p style="margin-top: 5px;">¹ Alternatively, a lockable cabinet with a SCEC endorsed lock suitable for use in Secure Areas is acceptable.</p> <p>² CRYPTO will be stored in accordance with its security classification marking with additional handling requirements. For further details refer to ACSI 33.</p>	Gatekeeper Storage Requirements	Secure Area	Partially Secure Area	Intruder Resistant Area	Secret or Highly Protected	B	A	A	Confidential or Protected	C ¹	B	B	Restricted or X-In-Confidence	Discretionary	Lockable Cabinet	Lockable Cabinet	CRYPTO	See note ²	See note ²	See note ²	<input type="checkbox"/>																
Gatekeeper Storage Requirements	Secure Area	Partially Secure Area	Intruder Resistant Area																																			
Secret or Highly Protected	B	A	A																																			
Confidential or Protected	C ¹	B	B																																			
Restricted or X-In-Confidence	Discretionary	Lockable Cabinet	Lockable Cabinet																																			
CRYPTO	See note ²	See note ²	See note ²																																			
R20	DSD RECOMMENDS that the FSO control the keys or equivalent access mechanism to all locked spaces (ACSI 33 3.1.33).	<input type="checkbox"/>																																				

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

R21	The classification of all media MUST be readily visually identifiable (ACSI 33 3.4.18).	<input type="checkbox"/>
R22	Ready visual identification of media classification SHOULD be achieved by labelling media with a protective marking that states the maximum classification and set of caveats applicable to the information stored on the media (ACSI 33 3.4.18).	<input type="checkbox"/>
R23	DSD RECOMMENDS that all removable media be registered with a unique identifier in an appropriate register (ACSI 33 3.4.22).	<input type="checkbox"/>
	ACSI 33 3.4.22 contains additional information for HIGHLY PROTECTED systems.	
R24	Hardware containing media MUST be classified at or above the classification of the media (ACSI 33 3.4.10).	<input type="checkbox"/>
R25	Storage media MUST be reclassified if (ACSI 33 3.4.16):	
	R25.1 information copied onto that media is of a higher classification; or	<input type="checkbox"/>
	R25.2 information contained on that media is subject to a classification upgrade.	<input type="checkbox"/>
R26	Organisations MUST use an approved method of sanitisation when media is moving from a higher classification to a lower classification (ACSI 33 3.4.26). Approved methods are described in ACSI 33 3.4.25 to 3.4.32.	<input type="checkbox"/>
R27	Repairs and maintenance for hardware containing classified media SHOULD be carried out by appropriately cleared and briefed personnel (ACSI 33 3.4.33).	<input type="checkbox"/>
R28	DSD RECOMMENDS that support contracts do not require the return of classified defective media (ACSI 33 3.4.33).	<input type="checkbox"/>
R29	Organisations MUST have a documented process for the disposal of hardware (ACSI 33 3.4.39).	<input type="checkbox"/>
R30	Organisations MUST (ACSI 33 3.4.36):	
	R30.1 sanitise and declassify, or destroy media containing classified material before disposal; and	<input type="checkbox"/>
	R30.2 use approved methods to declassify or destroy media.	<input type="checkbox"/>
	ACSI 33 3.4.19 and 3.4.23 contain extra information for HIGHLY PROTECTED media.	
R31	Organisations MUST perform the destruction of classified material under the supervision of an officer cleared to the highest level of media being destroyed (ACSI 33 3.4.42).	<input type="checkbox"/>
R32	The officer MUST (ACST 33 3.4.42):	
	R32.1 supervise the handling of the material to the point of destruction; and	<input type="checkbox"/>
	R32.2 ensure that the destruction is complete.	<input type="checkbox"/>
	Change Management:	
R33	Organisations SHOULD ensure that (ACSI 33 2.8.7):	
	R33.1 the change management process defined in ICT security documentation is followed;	<input type="checkbox"/>
	R33.2 proposed changes require approval by the documented authority;	<input type="checkbox"/>

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

R33.3 any proposed change that may impact the security of the ICT system is submitted to the Accreditation Authority for approval; and	<input type="checkbox"/>
R33.4 all associated system documentation is updated to reflect changes.	<input type="checkbox"/>
R34 The change management process SHOULD define appropriate actions to be followed before and after urgent changes are implemented (ACSI 33 2.8.7).	<input type="checkbox"/>
Education and Training:	
R35 Organisations MUST (ACSI 33 3.2.7):	
R35.1 ensure that all personnel who have access to ICT systems have sufficient training; and	<input type="checkbox"/>
R35.2 provide ongoing ICT security training and awareness for staff on topics such as responsibilities, potential security risks and countermeasures.	<input type="checkbox"/>
R36 The degree and content of security training SHOULD be aligned to user responsibilities (ACSI 33 3.2.9).	<input type="checkbox"/>
System Security:	
R37 All server and workstation security objectives and mechanisms SHOULD be documented in the relevant SSP or similar document (ACSI 33 3.5.7).	<input type="checkbox"/>
R38 Organisations SHOULD reduce potential vulnerabilities on systems by (ACSI 33 3.5.8):	
R38.1 removing unneeded software;	<input type="checkbox"/>
R38.2 removing unused accounts;	<input type="checkbox"/>
R38.3 removing unnecessary file shares;	<input type="checkbox"/>
R38.4 renaming required default accounts;	<input type="checkbox"/>
R38.5 replacing default passwords;	<input type="checkbox"/>
R38.6 ensuring patching is up-to-date;	<input type="checkbox"/>
R38.7 disabling unused features on installed software and operating systems; and	<input type="checkbox"/>
R38.8 disabling access to all unnecessary input/output devices at the BIOS level, which may include CD-ROMS, floppy disks, USB drives or wireless network interfaces. The risk assessment should be used to determine the specific devices that will be disabled.	<input type="checkbox"/>
R39 DSD RECOMMENDS that organisations consider seeking and applying additional information on hardening techniques relevant to their specific equipment (ACSI 33 3.5.8).	<input type="checkbox"/>
R40 DSD RECOMMENDS that organisations (ACSI 33 3.5.10):	
R40.1 limit information that could be disclosed about what software is installed; and	<input type="checkbox"/>
R40.2 implement access controls on relevant objects to limit users and programs to the minimum access required to perform their duties. This may include application whitelisting.	<input type="checkbox"/>
For further information for HIGHLY PROTECTED systems, please see ACSI 33 3.5.11.	

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

2.2 Risk Assessment

The Risk Assessment section of the Security Profile is the documented outcome of a risk assessment process conducted by a CA/RA. Given that the principal product sold by a CA and RA is 'trust', there is a critical requirement to be able to demonstrate a thorough understanding of the security threats faced by the CA/RA.

R41 Organisations MUST have security risk assessments, policies and plans that cover all Gatekeeper systems (ACSI 33 2.4.4).	<input type="checkbox"/>
R42 The Gatekeeper PKI SHOULD be covered by a comprehensive Security Risk Management Plan (SRMP) (ACSI 33 2.4.6). This will form part of the Service provider's Security Profile.	<input type="checkbox"/>
R43 It is RECOMMENDED that the Risk Assessment is written in accordance with AS/NZS 4360:2004 and HB 436:2004 (ACSI 33 2.2.9).	<input type="checkbox"/>
R44 Assets to be protected MUST be identified in the Risk Assessment. Key assets to be protected in a PKI include: <ul style="list-style-type: none">• Certificates of end users (Subscribers);• Private Keys of end users (Subscribers) where generated by the facility;• Private Keys of the CA;• Private Keys of RA operators where applicable;• PKI equipment (CA servers, Hardware Security Modules, RA workstations);• essential services equipment (network infrastructure, communications systems, perimeter security devices, backup systems and power supplies);• copies taken of Evidence of Identity (EOI) and other registration information;• other operational information (audit logs, transaction histories, CA lifecycle, archives, Online Certificate Status Protocol (OCSP) logs which are especially privacy-sensitive);• property; and• staff.	<input type="checkbox"/>
R45 Threats to PKI services, assets and business processes MUST be outlined in the Risk Assessment document.	<input type="checkbox"/>

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

R46	Key risks that SHOULD be considered include:	<input type="checkbox"/>																								
	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; vertical-align: top;"> <ul style="list-style-type: none"> • Building location, type and construction (green field, under construction or refurbishment) </td> <td style="width: 50%; vertical-align: top;"> <ul style="list-style-type: none"> • Shared tenancy requirements within the same building and/or floor </td> </tr> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Local crime activity </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Location of Rooms for creation and issue of digital certificates </td> </tr> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Availability and redundancy of entry points for communications services </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Availability and redundancy of entry points for other essential services </td> </tr> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Building set backs relative to street frontage </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Vehicular traffic </td> </tr> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Pedestrian traffic </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Inadequate vetting of Staff </td> </tr> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Lack of regular review of security </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Internet connectivity outages </td> </tr> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Intermittent electricity outage </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Long term electricity outage </td> </tr> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Fire </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Poor disaster recovery / business continuity planning </td> </tr> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Inappropriate storage of Keys and Certificates and pass-phrases </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Failure in the EOI process when enrolling new applicants for digital certificate </td> </tr> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Cryptographic product failure </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Systems integration failure </td> </tr> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Relying Party software application error </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Failure to comply with standards </td> </tr> <tr> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Inadequate treatment to physical security requirements </td> <td style="vertical-align: top;"> <ul style="list-style-type: none"> • Inadequate TRA undertaken </td> </tr> </table>	<ul style="list-style-type: none"> • Building location, type and construction (green field, under construction or refurbishment) 	<ul style="list-style-type: none"> • Shared tenancy requirements within the same building and/or floor 	<ul style="list-style-type: none"> • Local crime activity 	<ul style="list-style-type: none"> • Location of Rooms for creation and issue of digital certificates 	<ul style="list-style-type: none"> • Availability and redundancy of entry points for communications services 	<ul style="list-style-type: none"> • Availability and redundancy of entry points for other essential services 	<ul style="list-style-type: none"> • Building set backs relative to street frontage 	<ul style="list-style-type: none"> • Vehicular traffic 	<ul style="list-style-type: none"> • Pedestrian traffic 	<ul style="list-style-type: none"> • Inadequate vetting of Staff 	<ul style="list-style-type: none"> • Lack of regular review of security 	<ul style="list-style-type: none"> • Internet connectivity outages 	<ul style="list-style-type: none"> • Intermittent electricity outage 	<ul style="list-style-type: none"> • Long term electricity outage 	<ul style="list-style-type: none"> • Fire 	<ul style="list-style-type: none"> • Poor disaster recovery / business continuity planning 	<ul style="list-style-type: none"> • Inappropriate storage of Keys and Certificates and pass-phrases 	<ul style="list-style-type: none"> • Failure in the EOI process when enrolling new applicants for digital certificate 	<ul style="list-style-type: none"> • Cryptographic product failure 	<ul style="list-style-type: none"> • Systems integration failure 	<ul style="list-style-type: none"> • Relying Party software application error 	<ul style="list-style-type: none"> • Failure to comply with standards 	<ul style="list-style-type: none"> • Inadequate treatment to physical security requirements 	<ul style="list-style-type: none"> • Inadequate TRA undertaken 	
<ul style="list-style-type: none"> • Building location, type and construction (green field, under construction or refurbishment) 	<ul style="list-style-type: none"> • Shared tenancy requirements within the same building and/or floor 																									
<ul style="list-style-type: none"> • Local crime activity 	<ul style="list-style-type: none"> • Location of Rooms for creation and issue of digital certificates 																									
<ul style="list-style-type: none"> • Availability and redundancy of entry points for communications services 	<ul style="list-style-type: none"> • Availability and redundancy of entry points for other essential services 																									
<ul style="list-style-type: none"> • Building set backs relative to street frontage 	<ul style="list-style-type: none"> • Vehicular traffic 																									
<ul style="list-style-type: none"> • Pedestrian traffic 	<ul style="list-style-type: none"> • Inadequate vetting of Staff 																									
<ul style="list-style-type: none"> • Lack of regular review of security 	<ul style="list-style-type: none"> • Internet connectivity outages 																									
<ul style="list-style-type: none"> • Intermittent electricity outage 	<ul style="list-style-type: none"> • Long term electricity outage 																									
<ul style="list-style-type: none"> • Fire 	<ul style="list-style-type: none"> • Poor disaster recovery / business continuity planning 																									
<ul style="list-style-type: none"> • Inappropriate storage of Keys and Certificates and pass-phrases 	<ul style="list-style-type: none"> • Failure in the EOI process when enrolling new applicants for digital certificate 																									
<ul style="list-style-type: none"> • Cryptographic product failure 	<ul style="list-style-type: none"> • Systems integration failure 																									
<ul style="list-style-type: none"> • Relying Party software application error 	<ul style="list-style-type: none"> • Failure to comply with standards 																									
<ul style="list-style-type: none"> • Inadequate treatment to physical security requirements 	<ul style="list-style-type: none"> • Inadequate TRA undertaken 																									
R47	PSM Part B 5.67 - 5.68 and Part C requires organisations to determine availability requirements for their systems. Once these have been determined, organisations MUST implement appropriate measures to support these requirements (ACSI 33 2.8.13).	<input type="checkbox"/>																								
R48	Organisations SHOULD (ACSI 33 2.8.14):																									
	R48.1 backup all information identified as critical;	<input type="checkbox"/>																								
	R48.2 store backups of critical information, with associated documented recovery procedures, at a remote location secured in accordance with the standards for the classification of the information; and	<input type="checkbox"/>																								
	R48.3 test backup and restoration processes regularly to confirm their effectiveness.	<input type="checkbox"/>																								
R49	Movement of classified information to and from remote storage MUST be done in accordance with the PSM Part C.	<input type="checkbox"/>																								

2.3 Security Plan

R50	A site security plan and SOPs MUST be developed (ACSI 33 3.1.20). These may form part of the Security Profile.	<input type="checkbox"/>
------------	---	--------------------------

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

R51	Key points that SHOULD be included in Standard Operating Procedures include:	<input type="checkbox"/>		
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; vertical-align: top;"> <ul style="list-style-type: none"> • Security Philosophy • Management of Staff • Management of Contractors • Key management • Training Requirements • Operation of technology including but not limited to CCTV System • Clearance requirements and procedures. </td> <td style="width: 50%; vertical-align: top;"> <ul style="list-style-type: none"> • Security Roles and Responsibilities • Management of Visitors • Response details in the event of an incident i.e. bomb threat and loss of power • Maintenance regimes • Role of guards • Intruder Alarm System • Access Control System </td> </tr> </table>			<ul style="list-style-type: none"> • Security Philosophy • Management of Staff • Management of Contractors • Key management • Training Requirements • Operation of technology including but not limited to CCTV System • Clearance requirements and procedures. 	<ul style="list-style-type: none"> • Security Roles and Responsibilities • Management of Visitors • Response details in the event of an incident i.e. bomb threat and loss of power • Maintenance regimes • Role of guards • Intruder Alarm System • Access Control System
<ul style="list-style-type: none"> • Security Philosophy • Management of Staff • Management of Contractors • Key management • Training Requirements • Operation of technology including but not limited to CCTV System • Clearance requirements and procedures. 	<ul style="list-style-type: none"> • Security Roles and Responsibilities • Management of Visitors • Response details in the event of an incident i.e. bomb threat and loss of power • Maintenance regimes • Role of guards • Intruder Alarm System • Access Control System 			
R52	Information relating to the system-specific roles and responsibilities of IT security advisers, system managers, system administrators and system users SHOULD be included in the system documentation (ACSI 33 2.1.2).	<input type="checkbox"/>		
R53	Security SOPs SHOULD be developed for each of the following roles (ACSI 33 2.6.5):	<input type="checkbox"/>		
	R53.1 ITSA;	<input type="checkbox"/>		
	R53.2 System Manager;	<input type="checkbox"/>		
	R53.3 System Administrator; and	<input type="checkbox"/>		
	R53.4 System Users.	<input type="checkbox"/>		
R54	The ITSA and System Manager SHOULD be familiar with all SOPs (ACSI 33 2.6.5).	<input type="checkbox"/>		
R55	Procedures SHOULD be documented in the ITSA SOPs for (ACSI 33 2.6.10):	<input type="checkbox"/>		
	R55.1 instructing new users to comply with ICT security requirements;	<input type="checkbox"/>		
	R55.2 reviewing system audit trails and manual logs, particularly for privileged users;	<input type="checkbox"/>		
	R55.3 reviewing user accounts, system parameters and access controls;	<input type="checkbox"/>		
	R55.4 checking the integrity of system software;	<input type="checkbox"/>		
	R55.5 testing access controls;	<input type="checkbox"/>		
	R55.6 inspecting equipment and cabling;	<input type="checkbox"/>		
	R55.7 managing the review of removable media containing data that is to be transferred off-site;	<input type="checkbox"/>		
	R55.8 managing the review of incoming media for viruses or unapproved software;	<input type="checkbox"/>		
	R55.9 labelling, registering and mustering assets, including removable media; and	<input type="checkbox"/>		
	R55.10 reporting and managing security incidents, including involvement in physical security incident management where the incident could impact on ICT security.	<input type="checkbox"/>		
R56	Procedures SHOULD be documented in the System Manager SOPs for (ACSI 33 2.6.11):	<input type="checkbox"/>		

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

R56.1 managing the ongoing security and functionality of system software and hardware, including:	
R56.1.1 maintaining awareness of current software vulnerabilities;	<input type="checkbox"/>
R56.1.2 testing and applying software patches/updates;	<input type="checkbox"/>
R56.1.3 applying appropriate hardening techniques;	<input type="checkbox"/>
R56.1.4 updating anti-virus software;	<input type="checkbox"/>
R56.2 managing the destruction of unserviceable equipment and media;	<input type="checkbox"/>
R56.3 authorising new system users;	<input type="checkbox"/>
R56.4 approving and releasing changes to the system software or configuration;	<input type="checkbox"/>
R56.5 authorising access rights to applications and data; and	<input type="checkbox"/>
R56.6 recovering from system failures.	<input type="checkbox"/>
R57 Procedures SHOULD be documented in the System Administrator's SOPs for (ACSI 33 2.6.12):	
R57.1 securing the system when not in use;	<input type="checkbox"/>
R57.2 implementing access rights to applications and data;	<input type="checkbox"/>
R57.3 adding and removing users;	<input type="checkbox"/>
R57.4 setting user privileges;	<input type="checkbox"/>
R57.5 cleaning up directories and files when a user departs or changes roles;	<input type="checkbox"/>
R57.6 backing up data, including audit logs;	<input type="checkbox"/>
R57.7 securing backup media; and	<input type="checkbox"/>
R57.8 recovering from system failures.	<input type="checkbox"/>
R58 The System User's SOPs SHOULD document (ACSI 33 2.6.14):	
R58.1 who is responsible for what aspects of security;	<input type="checkbox"/>
R58.2 a warning that:	
R58.2.1 users' actions may be audited;	<input type="checkbox"/>
R58.2.2 users will be held accountable for their actions;	<input type="checkbox"/>
R58.3 guidelines on choosing and protecting passwords;	<input type="checkbox"/>
R58.4 guidelines on enforcing need-to-know on the system;	<input type="checkbox"/>
R58.5 what to do in the case of a suspected or actual security incident;	<input type="checkbox"/>
R58.6 the highest level of classified material that can be processed on the system and handling procedures for classified information;	<input type="checkbox"/>
R58.7 procedures for controlling and sanitising media;	<input type="checkbox"/>
R58.8 procedures for labelling, handling and disposing of hardcopy;	<input type="checkbox"/>

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

R58.9	preventing overview of data by visitors; and	<input type="checkbox"/>
R58.10	what to do for hardware and software maintenance.	<input type="checkbox"/>
R59	Organisations MUST provide guidance to users on their responsibilities relating to ICT security, and the consequences of non-compliance (ACSI 33 2.6.15).	<input type="checkbox"/>
R60	System Users SHOULD sign a statement that they have read and agree to abide by the System Users' SOP (ACSI 33 2.6.13).	<input type="checkbox"/>
R61	SOPs SHOULD be maintained and updated (ACSI 33 2.6.7). This may be done as:	
R61.1	a response to changes to the system; and	<input type="checkbox"/>
R61.2	part of a regular review of documentation.	<input type="checkbox"/>
R62	Organisations SHOULD ensure that data transfers are either (ACSI 33 3.11.2):	
R62.1	individually approved by the ITSA; or	<input type="checkbox"/>
R62.2	performed in accordance with processes and/or procedures approved by the Accreditation Authority.	<input type="checkbox"/>
	ACSI 33 3.11.3 contains further information for HIGHLY PROTECTED systems.	
R63	Organisations MUST ensure that users (ACSI 33 3.11.4):	
R63.1	are held accountable for the data they transfer, and	<input type="checkbox"/>
R63.2	are instructed to perform the following checks prior to initiating the data transfer: 1) protective marking check; 2) visual inspection; and 3) metadata check, if relevant.	<input type="checkbox"/>
R64	Organisations SHOULD strictly define and limit the types of files that may be transferred, based on business requirements and the results of a risk assessment (ACSI 33 3.11.9).	<input type="checkbox"/>
	ACSI 33 3.11.10 contains further information for HIGHLY PROTECTED systems.	
R65	Organisations transferring data manually between two systems SHOULD use (ACSI 33 3.11.14): 1) a previously unused piece of media; or 2) a pool of media items used only for data transfer between the two relevant systems; or 3) a media item which has been sufficiently sanitised to permit its reuse on the less classified of the systems between which the data transfer is occurring.	<input type="checkbox"/>
R66	Organisations importing data to a classified system MUST ensure that the data is scanned for malicious and active content (ACSI 33 3.11.24).	<input type="checkbox"/>

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

R67	Organisations MUST develop and document audit requirements reflecting the overall audit objectives, derived from the ICTSP and SRMP, covering (ACSI 33 3.7.26):	
R67.1	the scope of audits;	<input type="checkbox"/>
R67.2	the audit schedule;	<input type="checkbox"/>
R67.3	actions to be taken when violations are detected;	<input type="checkbox"/>
R67.4	reporting requirements; and	<input type="checkbox"/>
R67.5	specific responsibilities.	<input type="checkbox"/>
R68	Organisations SHOULD (ACSI 33 3.5.19):	
R68.1	characterise all devices whose functions are critical, and those identified as being at high risk of compromise;	<input type="checkbox"/>
R68.2	store the characterisation information securely;	<input type="checkbox"/>
R68.3	update the characterisation information after every legitimate change to the system;	<input type="checkbox"/>
R68.4	as part of the ongoing audit schedule, compare the stored characterisation information against current characterisation information to determine whether a compromise or a legitimate but incorrectly completed system modification has occurred;	<input type="checkbox"/>
R68.5	perform the characterisation from a trusted environment rather than the standard operating system wherever possible; and	<input type="checkbox"/>
R68.6	resolve any detected changes in accordance with the documented incident management procedures.	<input type="checkbox"/>
R69	DSD RECOMMENDS that organisations meet the requirement for characterisation using a SHA DACA to perform cryptographic checksums (ACSI 33 3.5.19).	<input type="checkbox"/>
R70	Organisations MUST develop and document logging requirements reflecting the overall audit objectives derived from the ICTSP and SRMP, covering (ACSI 33 3.7.12):	
R70.1	the logging facility, including:	
R70.1.1	log server availability requirements;	<input type="checkbox"/>
R70.1.2	the reliable delivery of log information to the log server;	<input type="checkbox"/>
R70.2	the list of events associated with a system or software component to be logged; and	<input type="checkbox"/>
R70.3	event log protection and archival requirements.	<input type="checkbox"/>
R71	For each event identified as needing to be logged, organisations MUST ensure that the log facility records at least the following details, where possible (ACSI 33 3.7.16):	
R71.1	date and time of the event;	<input type="checkbox"/>
R71.2	relevant user(s) or process;	<input type="checkbox"/>
R71.3	event description;	<input type="checkbox"/>
R71.4	success or failure of the event;	<input type="checkbox"/>
R71.5	event source (e.g. application name); and	<input type="checkbox"/>

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

R71.6	terminal location/identification.	<input type="checkbox"/>
R72	Event logs MUST be (ACSI 33 3.7.17):	
R72.1	protected from modification and unauthorised access;	<input type="checkbox"/>
R72.2	archived and retained for future access; and	<input type="checkbox"/>
R72.3	protected from whole or partial loss within the defined retention period.	<input type="checkbox"/>
ACSI 33 3.7.14 and 3.7.18 contain additional information for HIGHLY PROTECTED systems.		
R73	The ITSA SHOULD be responsible for managing and auditing the event logs (ACSI 33 3.7.25).	<input type="checkbox"/>
R74	DSD RECOMMENDS that organisations deploy tools for (ACSI 33 3.7.10):	
R74.1	the management and archival of security event information; and	<input type="checkbox"/>
R74.2	the correlation of events of interest.	<input type="checkbox"/>
R75	A system management log SHOULD be used to record the following information (ACSI 33 3.7.20):	
R75.1	sanitisation activities;	<input type="checkbox"/>
R75.2	system start-up and shutdown;	<input type="checkbox"/>
R75.3	component or system failures;	<input type="checkbox"/>
R75.4	maintenance activities;	<input type="checkbox"/>
R75.5	housekeeping activities; Examples: Backup and archival runs.	<input type="checkbox"/>
R75.6	system recovery activities; and	<input type="checkbox"/>
R75.7	special or out-of-hours activities.	<input type="checkbox"/>
R76	DSD RECOMMENDS that organisations maintain system management logs for the life of the system (ACSI 33 3.7.21).	<input type="checkbox"/>
ACSI 33 3.7.22 contains additional information for HIGHLY PROTECTED systems.		
R77	Organisations SHOULD ensure that a sufficient number of appropriately trained personnel and tools are available to analyse all logs for potential violations of security policy (ACSI 33 3.7.28).	<input type="checkbox"/>
R78	DSD RECOMMENDS that an accurate time source is used consistently throughout the PKI to assist with the correlation of logged events across multiple systems (ACSI 33 3.7.16).	<input type="checkbox"/>

2.3.1 Incident response plan

R79	Organisations MUST develop an Incident Response Plan (which may form part of the Security Profile) that, as a minimum, defines (ACSI 33 2.8.41):	
R79.1	broad guidelines on what constitutes an incident;	<input type="checkbox"/>
R79.2	the minimum level of training for users and system administrators;	<input type="checkbox"/>

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

R79.3	the authority responsible for initiating investigations of an incident;	<input type="checkbox"/>
R79.4	the steps necessary to ensure the integrity of information supporting a compromise;	<input type="checkbox"/>
R79.5	the steps necessary to ensure that critical systems remain operational; and	<input type="checkbox"/>
R79.6	how to formally report incidents.	<input type="checkbox"/>
R80	The Incident Response Plan SHOULD also contain (ACSI 33 2.8.42):	
R80.1	clear definitions of the types of incidents that are likely to be encountered;	<input type="checkbox"/>
R80.2	the expected response to each incident type;	<input type="checkbox"/>
R80.3	the authority within the organisation who is responsible for initiating:	
R80.3.1	a formal (administrative) investigation;	<input type="checkbox"/>
R80.3.2	a police investigation of an incident;	<input type="checkbox"/>
R80.3.3	an ASIO investigation of national security incidents, in accordance with Part G of the PSM;	<input type="checkbox"/>
R80.4	the criteria by which the responsible authority would initiate formal, police or ASIO investigations of an incident;	<input type="checkbox"/>
R1.1.	references to other related documents; Examples: Business Continuity Plan, Fraud Control Plan.	<input type="checkbox"/>
R80.5	which other organisations or authorities need to be informed in the event of an investigation being undertaken; and	<input type="checkbox"/>
R80.6	the details of the system contingency measures, or a reference to these details if they are located in a separate document.	<input type="checkbox"/>
R81	Organisations SHOULD develop and maintain procedures supporting the plan to (ACSI 33 2.8.44):	
R81.1	detect potential security breaches;	<input type="checkbox"/>
R81.2	establish the cause of any security incident, whether accidental or deliberate;	<input type="checkbox"/>
R81.3	detail the action to be taken to recover and minimise the exposure to a system compromise;	<input type="checkbox"/>
R81.4	report the incident; and	<input type="checkbox"/>
R81.5	document any recommendations on preventing a recurrence.	<input type="checkbox"/>
R82	Organisations MUST detail security incident responsibilities and procedures in the SSP and in the SOPs (ACSI 33 2.8.22).	<input type="checkbox"/>
R83	Staff MUST be directed to report security incidents to the ITSA as soon as possible after the incident is discovered (ACSI 33 2.8.23).	<input type="checkbox"/>
R84	Standard procedures for all personnel with access to the system SHOULD include the requirement to notify the ITSA of (ACSI 33 2.8.28):	
R84.1	any data spillage; and	<input type="checkbox"/>

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

R84.2 access to any data classified above that for which they are authorised.	<input type="checkbox"/>
R85 When a data spill occurs, organisations SHOULD assume that the information has been compromised (ACSI 33 2.8.28).	<input type="checkbox"/>
R86 Organisations MUST treat any such spillage as an incident, and follow the Incident Response Plan to deal with it (ACSI 33 2.8.28).	<input type="checkbox"/>
Please see ACSI 33 2.8.29 for additional requirements for HIGHLY PROTECTED systems.	
R87 Organisations SHOULD ensure that all security incidents are recorded in a register. The purpose of the register is to highlight the nature and frequency of the incidents and breaches so that corrective action may be taken (ACSI 33 2.8.26).	<input type="checkbox"/>
R88 The recorded information SHOULD include, at a minimum (ACSI 33 2.8.26):	
R88.1 the date the incident was discovered;	<input type="checkbox"/>
R88.2 the date the incident occurred;	<input type="checkbox"/>
R88.3 a description of the incident, including the people and locations involved;	<input type="checkbox"/>
R88.4 the action taken; and	<input type="checkbox"/>
R88.5 to whom the incident was reported.	<input type="checkbox"/>
R89 Organisations SHOULD (ACSI 33 2.8.32):	
R89.1 transfer a copy of raw audit trails onto media such as CD-ROM or DVD-ROM for secure archiving, as well as securing manual log records for retention, and	<input type="checkbox"/>
R89.2 ensure that all personnel involved in the investigation maintain a record of actions undertaken to support the investigation.	<input type="checkbox"/>

2.3.2 Reporting security incidents

R90 Organisations MUST report significant ICT security incidents to DSD (ACSI 33 2.8.36).	<input type="checkbox"/>
R91 Reporting of incidents to DSD SHOULD be undertaken using the Information Security Incident Reporting (ISIR) form (ACSI 33 2.8.34).	<input type="checkbox"/>
R92 Reporting any incident involving the loss or misuse of cryptographic keying material is particularly important. Organisations MUST notify all system users of any suspected loss or compromise of keying material (ACSI 33 2.8.38).	<input type="checkbox"/>

2.3.3 Dealing with malicious software

R93 Organisations MUST develop, implement and maintain tools and procedures, derived from a risk assessment, covering the detection of potential security incidents, incorporating (ACSI 33 2.8.17):	
R93.1 countermeasures against malicious code;	<input type="checkbox"/>
R93.2 intrusion detection strategies;	<input type="checkbox"/>
R93.3 audit analysis;	<input type="checkbox"/>
R93.4 system integrity checking; and	<input type="checkbox"/>
R93.5 vulnerability assessments.	<input type="checkbox"/>

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

R94	Organisations MUST (ACSI 33 3.5.69):	
R94.1	develop and maintain a set of policies, plans and procedures, derived from a risk assessment, covering how to:	
R94.1.1	minimise the likelihood of malicious code being introduced into the system(s);	<input type="checkbox"/>
R94.1.2	detect any malicious code installed on the system(s);	<input type="checkbox"/>
R94.2	make users aware of the policies, plans and procedures; and	<input type="checkbox"/>
R94.3	ensure that all instances of detected malicious code outbreaks are handled according to the procedures.	<input type="checkbox"/>
R95	Organisations SHOULD (ACSI 33 2.8.24):	
R95.1	encourage staff to note and report any observed or suspected security weakness in, or threats to, systems or services; Examples: unexpected dialog boxes or excessive processing.	<input type="checkbox"/>
R95.2	establish and follow procedures for reporting software malfunctions;	<input type="checkbox"/>
R95.3	put mechanisms in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored; and	<input type="checkbox"/>
R95.4	deal with the violation of organisational security policies and procedures by employees through a formal disciplinary process.	<input type="checkbox"/>

2.4 Key Management Plan

The Key Management Plan (part of the Security Profile) details procedures for organisations with encryption systems used to protect classified information. Check that procedures match the requirements of the policy and plans. In particular look for registering of material, mustering and destruction.

The Plan identifies the implementation, standards, procedures and methods for key management in the organisation.

R96	Encryption products used to protect Australian Government classified information MUST be listed on DSD's EPL. If the product is listed as "in-evaluation", then this must be stated in the certification report.	<input type="checkbox"/>
R97	Service Providers MUST only use DSD Approved Cryptographic Algorithms (DACAs) as specified in ACSI33 3.9.10 – 3.9.13	<input type="checkbox"/>

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

R98	<p>The Key Management element of the Security Profile should describe Key use and lifecycle, and specify the usage periods of the various Keys. In particular, it SHOULD include the identification of standards, procedures and secure methods for:</p> <ul style="list-style-type: none"> • generating Keys; • distributing Keys to intended users, including how Keys should be activated when received; • storing Keys, including how authorised users obtain access to Keys; • changing or updating Keys including rules governing Key changes and how this will be done; • dealing with compromised Keys; • revoking Keys including how Keys should be withdrawn or deactivated, e.g. when Keys have been compromised or when a user leaves an organisation (in which case Keys should also be archived); • recovering Keys that are lost or corrupted as part of business continuity management, e.g. for recovery of encrypted information; • backing up and archiving Keys, e.g. for information archived or backed up; • destroying Keys; • logging and auditing of Key management related activities; and • escrowing keys, if this is to be provided. 	<input type="checkbox"/>
R99	Cryptographic key management MUST be in accordance with DSD's requirements (ACSI 33 3.9.57-73).	<input type="checkbox"/>
R100	The Key Management Plan MUST contain adequate information against each of the topics listed in the table in ACSI33 3.9.73 consistent with the criticality and classification of the information to be protected.	<input type="checkbox"/>
R101	Organisations SHOULD be able to readily account for all transactions relating to cryptographic system material including identifying hardware and software, and who has been issued with the equipment (ACSI 33 3.9.66).	<input type="checkbox"/>
R102	Audits of cryptographic system material SHOULD be conducted (ACSI 33 3.9.67):	<input type="checkbox"/>
	R102.1 on handover/takeover of administrative responsibility for the system;	<input type="checkbox"/>
	R102.2 on change of individuals with access to the cryptographic system; and	<input type="checkbox"/>
	R102.3 at least annually.	<input type="checkbox"/>

3.0 Review Implementation

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

Gatekeeper Certification Guidelines & Checklist V3.0.1

3.1 Review the Implementation of the Security Plan

This is where the implementation of procedures and plans defined in the Security Plan, Key Management Plan and subordinate procedures are reviewed to ensure they are in place. Implementation of plans and procedures **MUST** be demonstrated.

The process is a combination of interviews with appropriate organisational staff and audits on site. Plans and procedures must be in place for use when operational.

R103	Procedures and plans defined in the Security Plan MUST be in place and have been implemented.	<input type="checkbox"/>
R104	Procedures and plans defined in the Key Management Plan MUST be in place and have been implemented.	<input type="checkbox"/>
R105	Staff appointed in plans and procedures MUST be available.	<input type="checkbox"/>
R106	Staff MUST have a good understanding of their roles as defined in plans and procedures.	<input type="checkbox"/>
R107	Privileged user set, as defined in plans and procedures MUST be consistent with what is in place on the system.	<input type="checkbox"/>
R108	The configuration and management of the evaluated product(s) SHOULD be in compliance with the product's security target and certification report or guidance. Note: Where non-evaluated components are in use, assessors must contact the DSD I-RAP Manager. DSD will advise if the use of the non-evaluated components in question have the potential to compromise certification to Australian Government best practice standards.	<input type="checkbox"/>
R109	Reviews have taken place in line with policy for:	
	R109.1 security documentation.	<input type="checkbox"/>
	R109.2 new or changed threat to the organisation, products in use, new services.	<input type="checkbox"/>
R110	Some examples MUST be sighted. DSD RECOMMENDS viewing as many as possible in developing an opinion for Section 3.1. Look for these examples: <ul style="list-style-type: none">• Time, date and location of security incident or security investigation.• User awareness training log.• Visitor's log.• Results of key accounting.• Summary of action taken by the Facility Security Officer.• Audit trail review.• Configuration management review.• User account management.	<input type="checkbox"/>

4.0 Technology Evaluation

4.1 Review Evaluation Status of Certification Authority/Registration Authority Technology

The following is required for a Certification Authority/Registration Authority to gain certification for Gatekeeper Accreditation (Gatekeeper Criteria for Accreditation of CAs / Gatekeeper Criteria for Accreditation of RAs):

R111 Certification Authority/Registration Authority Technology MUST have completed evaluation and be listed on DSD's Evaluated Products List as certified/validated to at least the ITSEC E3 or Common Criteria EAL4 level.	<input type="checkbox"/>
---	--------------------------

Comments

The following table will assist you to record responses to the IRAP checklists. It is not a substitute for a Certification Report.

You should enter a response for each check-marked requirement in the checklists, even where you do not wish to record detailed information about compliance or otherwise. This will assist in preparing your Certification Report, and will assist in maintaining appropriate historical records. It will also keep numbering consistent.

Fields

The 'Requirement' field is an auto-numbered field designed to increment each time that you move to a new line. It increments from 'R1' upwards. In order to achieve sub-requirement numbers under the 'Requirement' heading, you need only click on the 'Increase Indent' button – usually in the top-right region of your toolbar. Similarly, to revert to a requirement number from a sub-requirement number, you need only click on the 'Decrease Indent' button.

You should not need to alter the requirement numbering in any fashion as it is automatically configured to increment. This may be the case if you do not enter responses for a particular comment.

The 'Comment' field is a text field for you to record details against the requirement.

Requirement	Comment
R1	
R2	