Australian Government

Digital Transformation Office

Gatekeeper Public Key Infrastructure Framework

Compliance Audit Program

V 2.1 – December 2015

Digital Transformation Office

Licence

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the *It's an Honour* website (http://www.itsanhonour.gov.au)

Contact us

Enquiries or comments regarding this document are welcome at:

Gatekeeper Competent Authority
C/O Director, Trusted Digital Identity Team
Digital Transformation Office
Email: authentication@dto.gov.au

Contents

Figures

1. Guide Management

1.1 Change Log

This is the second published edition of the Gatekeeper Public Key Infrastructure (PKI) Framework (The Framework) Compliance Audit Program (GCAP). This release aligns with the compliance requirements of the current edition of the *Australian Government Protective Security Policy Framework* (PSPF) and *Australian Government Information Security Manual* (ISM).

1.2 Review Date

This document will be reviewed regularly and updated in line with changes to the ISM, PSPF and relevant government policies.

1.3 Conventions

This document adopts the following conventions:

- **MUST** indicates a mandatory requirement that a Service Provider is required to meet in order to satisfy a control test. This convention is also used to describe actions or activities to be undertaken by the Authorised Auditor.
- **SHOULD** indicates something that is not mandatory but is recommended which supports either a control test or is considered best practice.
- **MUST NOT** indicates something that if practiced, exercised or implemented will breach a Gatekeeper Accreditation requirement.
- **NON COMPLIANCE** will result if an Authorised Auditor determines a Service Provider does not meet a mandatory requirement listed in this document. Non-compliance severity ratings are listed at Annex A. A template for recording non-compliance is provided at Annex B.
  - Service Providers may seek a waiver for a NON COMPLIANCE with any mandatory control listed in this document from their Accreditation Authority. The Accreditation Authority for Agencies is their Agency Head or their delegated representative. For commercial organisations the Accreditation Authority is a person or committee with the necessary authority to grant such a waiver.
  - Service Providers are to meet all mandatory controls in this document unless they obtain a waiver for a NON COMPLIANCE from their Accreditation Authority.
  - Service Providers seeking a waiver for a NON COMPLIANCE with any mandatory control listed in this document MUST document the justification for NON COMPLIANCE, alternative mitigation measures to be implemented (if any) and an assessment of the residual security risk.
  - Service Providers MUST retain a copy of all decisions to grant a waiver for any mandatory control listed in this guide.

1.4 Terms and Definitions

The terms and definitions used in this document are defined in the *Identity and Access Management Glossary*.

Note the following terms which are used extensively throughout this document.

Term	Definition
Compliance Audit	An engagement of an Authorised Auditor to conduct an independent audit to determine whether or not a Service Provider is compliant with an accreditation regime.
Authorised Auditor	Refers solely to an endorsed qualified ICT security professional listed on the Australian Signals Directorate Information Security Registered Assessors Program (IRAP) website. See the IRAP website for further information http://www.asd.gov.au/infosec/irap/assessors.htm
Prior audit work	Refers to WebTrust[1] or ETSI[2] audit work successfully completed in the period since the previous Gatekeeper compliance audit (or since accreditation if undertaking the first Gatekeeper compliance audit).
Service Provider	Refers solely to a Gatekeeper Accredited RA, CA or VA, unless explicitly stated otherwise.

1.5 Advice on this Framework

Advice on the IRAP Guide or suggestions for amendment can be forwarded to:

Gatekeeper Competent Authority
C/O Director, Trusted Digital Identity Team
Digital Transformation Office
Email: authentication@dto.gov.au

1.6 Document Structure

This document is structured in the following manner:

- Section 2 provides an introduction to the Gatekeeper PKI Framework Compliance Audit Program.
- Section 3 describes the Gatekeeper PKI Framework.
- Section 4 defines the Gatekeeper audit process.
- Section 5 lists the compliance criteria and suggested audit guidance.
- Annex A list non-compliance severity ratings
- Annex B contains a non-compliance template that Authorised Auditors can use to record their findings for areas on non-compliance
- Annex C and Annex D map WebTrust and the European Telecommunications Standards Institute (ETSI)controls to GCAP to determine the suitability of using prior audit work as part of an annual Gatekeeper compliance audit.

[1] For further information see [WebTrust] in section 13 of the Gatekeeper PKI Framework

[2] For further information see [ETSI] in section 13 of the Gatekeeper PKI Framework

2. Introduction

2.1 Purpose

Under the Gatekeeper PKI Framework, annual compliance audits remain a condition of Gatekeeper accreditation. In accordance with Clause 11 of the Gatekeeper Head Agreement/Memorandum of Agreement, the Digital Transformation Office (DTO) requires that Authorised Auditors conduct an audit of Service Providers' compliance with the Framework on the anniversary of their initial accreditation date.

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 primary objective of the GCAP is to provide a work program to assist Service Providers in meeting the compliance requirements stipulated in the Gatekeeper Head Agreement/Memorandum of Agreement. The GCAP provides guidance to Authorised Auditors on the scope and conduct of the assessment required under Gatekeeper and applies to all Gatekeeper accredited Certification Authorities (CA), Registration Authorities (RA) and Validation Authorities (VA) across all Levels of Assurance (LOA).

Service Providers and Authorised Auditors are encouraged to seek further guidance from the documentation listed in the Framework at:

- Mandatory Requirements (section 5.8) ,
- Recommended Standards and Guides (section 5.9) and
- References (section 13).

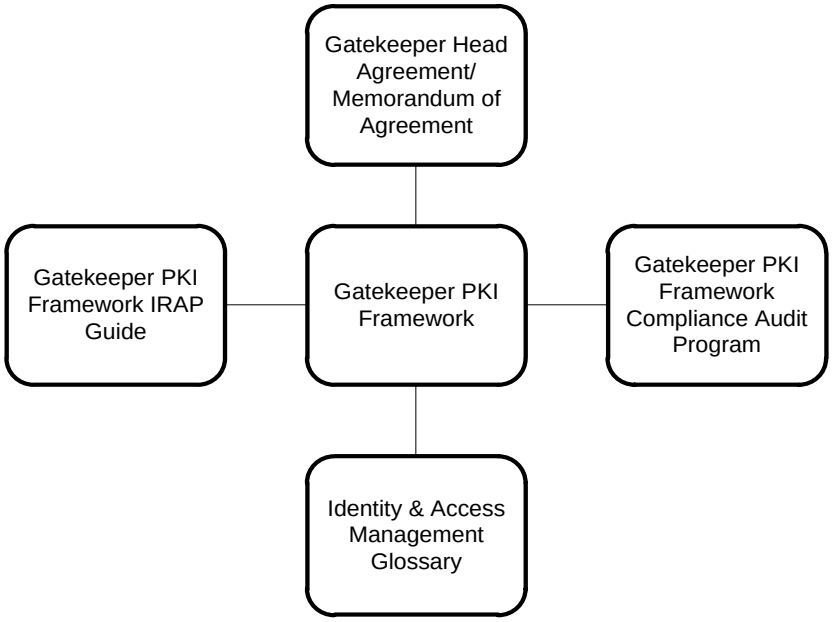
The complete suite of Gatekeeper documents is available at www.dto.gov.au

3. Gatekeeper PKI Framework

3.1 Gatekeeper PKI Framework

The Gatekeeper PKI Framework is a whole-of-government suite of policies, standards and procedures that governs the use of PKI in Government for the authentication of individuals, organisations and non-person entities – such as devices, applications or computing components. The Framework supports accreditation of Registration Authorities (RA), Certification Authorities (CA) and Validation Authorities (VA) and is built around five core documents as shown below.

Figure 1 Framework Structure



- The *Gatekeeper PKI Framework Compliance Audit Program* (this document) provides guidance to Authorised Auditors and Service Providers on the scope and conduct of the compliance assessment required under the Framework.
- The *Gatekeeper PKI Framework* defines the minimum requirements for Service Providers to obtain and maintain Gatekeeper accreditation.
- The *Gatekeeper PKI Framework IRAP Guide* provides IRAP Assessors with a guide to assess the implementation of security controls and practices by Service Providers.
- The *Gatekeeper Head Agreement/Memorandum of Agreement* is the formal agreement between the DTO (on behalf of the Commonwealth) and the Service Provider. This agreement establishes the conditions under which the Service Provider is accredited and what is required in order for the Service Provider to maintain its Gatekeeper Accreditation.
- The *Identity and Access Management Glossary* contains a list of acronyms and associated terms related to the Framework. The Glossary also contains all related terms associated with the National e-Authentication Framework and the Third Party Identity Services Assurance Framework.

4. Gatekeeper Audit Process

4.1 GCAP Audit Engagement

Service Providers **SHOULD** consider the following activities before engaging an Authorised Auditor:

- Develop a Statement of Work (SOW) which describes the audit work to be undertaken. Include any information relating to changes that have occurred in the Service Provider's PKI environment in the period since the previous GCAP, including:
  - Outcomes of prior audit work;
  - Changes to PKI environment or Gatekeeper Approved Documents;
  - Changes in the ownership or management of the Service Provider or PKI environment;
  - Compromises or security incidents;
  - Frequency of internal reviews; and
  - Outcomes from testing Disaster Recovery and Business Continuity plans or Incident Response procedures.
- Release the GCAP SOW with a Request for Tender (RFT);
  - Authorised Auditors may use information within the GCAP SOW to assist in drafting their response to the RFT.
- Review the responses to the RFT.
- Select an Authorised Auditor.
  - A chosen Authorised Auditor **MUST** have a degree of competence in Public Key Infrastructure and general knowledge of Gatekeeper Policies and Criteria.
  - Once an Authorised Auditor has been selected the successful respondent and Gatekeeper Competent Authority **SHOULD** be informed.
- Upon appointment, the Authorised Auditor:
  - defines the scope of the assessment to be conducted in consultation with the Service Provider;
  - formalises a contract with the Service Provider to conduct the Audit;
  - performs the GCAP as required; and
  - reports its findings to the Gatekeeper Competent Authority, the Service Provider and any other parties agreed between the Authorised Auditor and the Service Provider.

4.2 Prior Audit Work

This document provides guidance on how an Authorised Auditor may use the results of previous audit activities to reduce the possibility of duplication.

The Gatekeeper Competent Authority recognises WebTrust and ETSI as suitable commercial audit programs that can be considered by the Authorised Auditor as prior audit work.

An Authorised Auditor **SHOULD** review any WebTrust or ETSI audit work completed in the period since the previous Gatekeeper compliance audit. The Authorised Auditor is free to use their discretion in deciding whether to leverage the WebTrust or ETSI audit work

Service Providers that have completed, or are considering either a WebTrust or ETSI audit program are required to provide status reports to the Authorised Auditor.

Incorporating prior audit work by the Authorised Auditor provides a number of benefits to Service Providers:

- Continuity between audits so that continual improvements to the Gatekeeper PKI operations may be realised;
- Ensuring that previous audit findings and recommendations are given due consideration in the subsequent audit;
- Reducing expenditure on external audit requirements due to overlaps in audit activity; and
- Reducing the extent of interruptions to operations when audits occur.

The GCAP does not unequivocally accept prior audit work as sufficient to meet the compliance requirements for Gatekeeper. Rather, the *modular* structure of GCAP allows, where possible, work programs conducted under WebTrust or ETSI to be used as a substitute for parts of the GCAP work program. This is conditional on the Authorised Auditor being satisfied that the prior audit work provides adequate assurance within the constraints of the GCAP.

The following conditions apply when considering prior audit work:

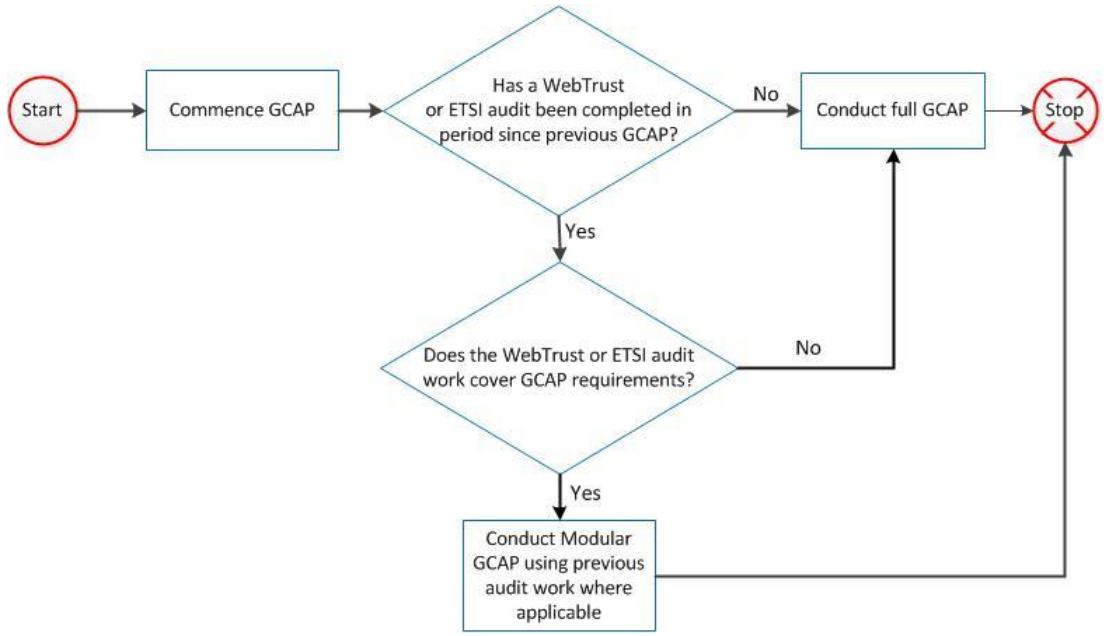
- The Authorised Auditor is required to review the relevant Annex (i.e. Annex C or D), which specifies:
  - the control mappings between GCAP and WebTrust and ETSI; and
  - the suitability of using these control mappings for GCAP.
- For various reasons the Authorised Auditor may choose not to consider previous audit activity and conduct a full Gatekeeper audit. The Authorised Auditor and the Service Provider will discuss and agree the factors contributing to this assessment.
  - The Authorised Auditor may decide to conduct a full Gatekeeper audit if prior work is deemed to be unreliable, insufficient or there is a lack of evidence of the nature of the work undertaken.
- The 'actual' WebTrust or ETSI audit work being considered **MUST** have been undertaken in the period since the previous Gatekeeper compliance audit (or since accreditation if undertaking the first Gatekeeper compliance audit), not the date on which the final Audit report was issued.
  - The GCAP requires the work being considered to have been conducted to a satisfactory outcome.
- The Authorised Auditor may decide whether or not prior audit work will be considered as part of the GCAP.

When a decision has been made to use work from a WebTrust or ETSI audit program, the Authorised Auditor **MUST** ensure that the decision is adequately supported. If an Authorised Auditor decides that prior audit work will not be used, the Authorised Auditor **MUST** document the reasons why in the final audit report.

Figure 2 shows the key decision points that an Authorised Auditor **SHOULD** consider when planning the Audit of a Service Provider's PKI operations. This will help Authorised Auditors to consider prior work performed.

A full GCAP is required if the Authorised Auditor chooses not to rely on any audit work performed since the previous GCAP.

Figure 2 Authorised Auditor – GCAP Planning Procedure



4.3 Documents to be reviewed as part of a full GCAP

The following Information Security Documentation **MUST** be reviewed by the Authorised Auditor as part of a full GCAP:

- Information Security Policy;
- Protective Security Risk Review;
- Security Risk Management Plan;
- System Security Plan, comprising;
  - Standard Operating Procedures;
- Physical & Environmental Security Plan;
- Personnel Security Plan;
- Incident Response Plan;
- Cryptographic Key Management Plan; and,
- Disaster Recovery and Business Continuity Plan.

4.4 Controls and waivers

A control is satisfied if the Authorised Auditor determines the Service Provider has successfully met the intent of a control. A control is not satisfied if the Authorised Auditor determines the Service Provider has not successfully met the intent of a control.

Where a waiver has been granted in relation to any aspect of a Service Provider's PKI operations, the Authorised Auditor **MUST** sight the document and make allowance for the waiver in their evaluation and indicate this in the audit report.

The Authorised Auditor **MUST** comment on each instance of **NON COMPLIANCE**. Comments are to include an indication of the extent to which the Service Provider does not comply with the control under evaluation. The severity ratings of **NON COMPLIANCE** are listed in Annex A. A template for providing comments on areas of non-compliance is outlined in Annex B.

4.5 GCAP Audit Reporting

Upon completion of the GCAP, the Authorised Auditor will issue a final Gatekeeper Audit Report to the Gatekeeper Competent Authority, the Service Provider and any other entities agreed to in the GCAP contract. Unless otherwise specified in the contract between the Service Provider and the Authorised Auditor, a Gatekeeper Audit Report is considered to be *sensitive commercial information* and **MUST** be treated with the required level of security controls for their protection.

As part of the Gatekeeper Audit Report, the Authorised Auditor **MUST** detail:

- The work conducted including the outcomes of control tests that were conducted;
- Any adverse issues identified, including potential control or procedural weaknesses;
- Areas of non-compliance and their associated severity ratings[3]; and
- Recommendations to remediate identified issues and non-compliances.

Completed IRAP Guides are to be send to the following address:

Gatekeeper Competent Authority
C/O Director, Trusted Digital Identity Team
Digital Transformation Office
Email: authentication@dto.gov.au

4.6 Audit Report Review

The specific process for dealing with the final Gatekeeper Audit Report findings is contained within each Service Provider's Gatekeeper Head Agreement/Memorandum of Agreement.

The DTO will review the Gatekeeper Audit Report findings and will subsequently issue either a:

- Statement to the Service Provider advising that its Gatekeeper Accreditation will be maintained; or
- Notice to the Service Provider specifying any adverse compliance audit findings and the required remedial actions (including timeframes to implement the remedial action) that will enable the Service Provider to maintain its Gatekeeper accreditation. Depending on the nature of the non-compliance, remedial action may include an additional compliance audit.

[3] Annex A lists the non-compliance severity ratings and their associated definitions.

5. Gatekeeper Audit Criteria

5.1 Audit Assessment

The GCAP consists of 107 audit criteria which cover the protective security requirements specific for the Gatekeeper PKI Framework. Alongside the audit criteria is guidance that can assist the Authorised Auditor in determining the adequacy of a Service Provider's controls. Authorised Auditor's are free to use alternative assessment methods to evaluate the adequacy of the Service Provider's controls.

Below is an example of GCAP control and assessment guidance.

Control	**Assessment Guidance**
Unevaluated products are not used unless the risks have been appropriately documented and accepted.	Seek evidence that the Service Provider is not using unevaluated products unless the risks have been appropriately documented and accepted. Review the Service Provider's Security Risk Management Plan.

5.2 Summary of Audit Criteria

The following table lists the controls to be evaluated.

Section	**Audit Criteria**	**Controls**
	Total Controls	**107**
5.3	Gatekeeper Approved Documents	18
5.4	Personnel Security	5
5.5	Physical and Environmental Security	5

Section	Audit Criteria	Controls
5.6	Media and ICT Equipment Management	16
5.7	Access Control Management	12
5.8	Operations Security	12
5.9	CA Key Lifecycle Management Controls	19
5.910	Subscriber Key Lifecycle Management Controls	10
5.11	Incident Management	5
5.12	Business Continuity Management	4
5.13	Outsourced Arrangements	1

5.3 Gatekeeper Approved Documents

Control	Assessment Guidance
Management, Publication and Communication 1. Gatekeeper Approved Documents are approved by management.	Obtain the latest copy of the Gatekeeper Approved Documents from the Service Provider and the date and approved version of the Gatekeeper Approved Documents from the DTO. Review the Gatekeeper Approved Documents to check if the version number and date are the same as those provided by the DTO. If the Gatekeeper Approved Documents have changed in the period since the previous Gatekeeper compliance audit (or since accreditation if undertaking the first Gatekeeper compliance audit), obtain evidence of the Service Provider's submission to the DTO for re-evaluation and the subsequent approval. If an amended Gatekeeper Approved Document has been submitted to the DTO for re-evaluation and has not yet been approved, detail the submission and any reason why it has not been approved.
Security Risk Management Plan (SRMP) 2. Security risks are identified, evaluated and managed by the Service Provider. 3. All PKI-related systems are covered by a SRMP. 4. Assets to be protected are identified. 5. Risk owners are identified for every security risk. 6. Security risk tolerances are specified. 7. Security risks deemed unacceptable are treated. 8. Unevaluated products are not used unless the risks have been appropriately documented and accepted.	Verify that the Service Provider has a defined risk management process which includes responsibilities, assets to be protected, risk tolerance levels and approved treatment options for unacceptable risks. Determine when the last threat and risk assessment was undertaken. • Was this completed in the timeframe prescribed in the SRMP? • Were there any adverse findings? • Have all remediation actions been authorised and implemented? • If any remediation actions do not appear to have been implemented and the reasons are not given are they addressed as residual risks? • Have they been officially approved and signed off by risk owners or management? • Verify that if the Service Provider is using unevaluated products, the risks have been appropriately documented and accepted.

Control	Assessment Guidance
Cryptographic Key Management Plan (CKMP) 9. A policy on the use and lifetime protection of cryptographic controls is developed, implemented and maintained through their whole lifecycle. 10. The level of detail in the CKMP is consistent with the criticality and classification of the information to be protected.	Review each of the processes within the CKMP and test to determine if they are implemented as prescribed. Consider in particular the outcomes of the following procedures that relate to both Certification Authority (CA) and Subscriber keys: • generating, distributing and activating keys; • storing, accessing, changing and 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; • recovering keys that are lost or corrupted as part of business continuity; • backing up and archiving keys; • logging and auditing of key management related activities; and • escrowing keys (if service is provided).
11. Australian Signals Directorate (ASD) evaluated cryptographic products, algorithms and protocols are used.	Check product evaluation documentation to determine if any product specific requirements apply. Check the ISM to determine if ASD Approved Cryptographic Algorithms (AACAs) and ASD Approved Cryptographic Protocols (AACPs) are used.
12. An annual inventory of cryptographic material is undertaken.	Verify that the Service Provider has conducted an inventory of cryptographic material in the period since the previous Gatekeeper compliance audit (or since accreditation if undertaking the first Gatekeeper compliance audit).
Certification Practice Statement & Certificate Policy 13. The Certification Practices Statement (CPS) and Certificate Policy(s) are formally approved.	Verify that the PKI has a management group (e.g. Policy Approval Authority, Policy Management Authority or equivalent group) which final authority and responsibility for specifying and approving the CPS and CP(s). Verify that the responsibilities for maintaining the CPS have been formally assigned.

14. The CPS and CP(s) conform to the document structure defined in RFC3647 15. PKI services are provided in accordance with disclosed practices in the CPS and CP(s). 16. All certificates issued by the PKI are compliant with a published CP. 17. The CA makes the Subscriber aware of applicable certificate and key management obligations. 18. Terms and conditions are made available to Relying Parties.	Check RFC3647 to determine if the CPS and CP(s) include the headings listed in section 4 of the standard. The CA provides its certification services in accordance with the CPS and CA CP. Review the controls listed in the CPS and cross reference them against the policies contained within each CP to determine if they reflect and achieve the objectives set forth in each CP. Check if the CPS and CP(s) contain sections for Subscribers relating to: • The protection of personal information; • Any reliance or financial limits for certificate usage; • Liability arrangements; • Accuracy of representations in certificate application; • Information on the protection of the subscribers private key; • Restrictions on private key and certificate use; • The associated LOA for a certificate; and • Notification procedures for private key compromise. In addition to the above, check if the CPS and CP(s) contain sections for Relying Parties relating to: • The purposes for which a certificate is used • Digital signature verification responsibilities • Revocation and suspension (if supported) checking responsibilities • Acknowledgement of liability caps and warranties Examine the previous three months of statistical data relating to certificates that have been issued, renewed, rekeyed, revoked and suspended (if supported) and: • Determine using event logging or other means if the certificates have been processed as described and report any anomalies, and • Determine over the same period that certificate distribution to subscribers and CRL and OCSP processing (if supported) was also conducted as prescribed.

5.4 Personnel security

Control	Assessment Guidance
19. Employees undergo an appropriate employee screening, and where necessary hold a Security Clearance appropriate for their job requirements. 20. Employees and contractors (where relevant) receive appropriate annual security awareness education and training as relevant for their job function. 21. Training records for every PKI-specific position are maintained. 22. A Trusted Persons Register is maintained.	Verify that all staff hold an appropriate security clearance for their position. Verify that the Service Provider provides aftercare arrangements which enable staff to advise the Australian Government Security Vetting Agency (AGSVA) of any significant change in their personal circumstances. Verify that information security awareness, education and training programs have been established for employees and contractors (where relevant). • Are the programmes in line with the Service Provider's Gatekeeper Approved Documents? • Do they include training requirements and training procedures for each role? • Do they include re-training requirements and re-training procedures for each role? Review training records to verify personnel maintain a skill level which enables them to perform their duties satisfactorily. Review the Trusted Persons Register and verify the details are correct. • Are all employees in Positions of Trust or users with privileged access listed? • Is a Manager appointed? • Is the Trusted Persons Register reviewed and updated in accordance with the Gatekeeper Approved Documents?

Control	Assessment Guidance
23. All information security roles and responsibilities are defined and allocated.	Verify that the authorisations and security clearance requirements necessary for system access are specified in the System Security Plan (SSP). • Verify that the Service Provider has appointed a security expert, as an Information Technology Security Advisor (ITSA) or equivalent position. • Verify that the Service Provider has appointed an Information Technology Security Manager (ITSM) or equivalent position. • Verify that each PKI system has a system owner. Verify that standard procedures for all personnel with access to PKI systems include: • Requirements to notify the ITSM of any Cyber Security Incident as soon as possible after the Cyber Security Incident is discovered • Requirements to notify the ITSM of access to any data or systems they are not authorised to access. • Responsibilities for the protection of assets and for carrying our specific security processes are clearly defined. – Have staff been made aware of these obligations? – Have the procedures been tested so that they can be followed during an emergency, Cyber Security Incident or other adverse event?

5.5 Physical and environmental security

Control	Assessment Guidance
24. Security perimeters are used to protect areas that contain either sensitive or critical information or information processing facilities. 25. Secure areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access. 26. Physical protection against natural disasters, malicious attacks or accidents are designed and applied. 27. PKI services are not directly accessible from the Internet. 28. Networks are managed and controlled to protect information processing facilities and information in systems and applications.	Confirm the Information Security Documentation contains a Physical & Environmental Security Plan. Review the Information Security Documentation to verify that each physical and environmental security control detailed in the document is still in place and operating as intended. Verify that any instances of compromise or suspected compromise have been managed in accordance with the Information Security Documentation Obtain evidence that a review of physical and environmental security arrangements has been conducted in the period since the last Gatekeeper compliance audit (or since accreditation if undertaking the first Gatekeeper compliance audit)? • Examine the results of the last security review • Were there any adverse findings? • Have all remediation actions been authorised and implemented? Verify that all physical control tests and maintenance checks were conducted in the period since the last Gatekeeper compliance audit (or since accreditation if undertaking the first Gatekeeper compliance audit). Consider: • Alarm and physical security control systems. • Emergency response processes. • Intrusion detection and prevention systems. • Firewall rules. • Environmental and fire control systems. • UPS and power generators. • The number of telecommunication service providers used. Examine the results of these tests and checks. • Were there any adverse findings? • Have all remediation actions been authorised and implemented?

5.6 Media and ICT equipment management

Control	Assessment Guidance
Information classification and labelling 29. Information is classified in terms of legal requirements, value, business criticality and sensitivity to unauthorised disclosure, loss, or compromise. 30. An appropriate set of procedures for information labelling are developed and implemented in accordance with the information classification scheme adopted by the Service Provider. **Asset management** 31. Every asset is owned and subsequently controlled. 32. Asset owners review user access rights at regular intervals. 33. Assets associated with information and information processing facilities are identified, managed and protected to a commensurate classification or sensitivity level of the information being handled. 34. Rules for the acceptable use of assets associated with information and information processing facilities are identified, documented and implemented. 35. Procedures for handling assets are developed and implemented in accordance with the information classification scheme adopted by the Service Provider. 36. All items of equipment containing storage media is verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. 37. Security is applied to off-site assets taking into account the different risks of working outside the Service Provider's premise. 38. Media is disposed of securely when no longer required using formal procedures. **Asset protection** 39. Media containing information is protected against unauthorised access, misuse or corruption during transportation.	Verify that the Service Provider manages their assets in accordance with the requirements outlined in the Information Security Documentation • Has the Service Provider implemented handling procedures for the use of assets? • Has the Service Provider nominated a person to be responsible for the management and control of assets? • Identify this person and verify they are performing their duties in accordance with the Information Security Documentation. • Are assets labelled in accordance with the Service Provider's information classification scheme and documented procedures? • Do procedures exist for the classification, sanitisation, disposal, destruction or re-classification of assets? • Are inventories of sensitive or classified assets maintained? • Can staff account for all sensitive and classified ICT equipment and media? • Determine using asset handling procedures or other means if staff meet their security obligations when transporting media offsite and report any anomalies. Verify that a review of access rights to assets has occurred in the period since the previous Gatekeeper compliance audit (or since accreditation if undertaking the first Gatekeeper compliance audit).

Control	Assessment Guidance
40. Equipment is maintained to ensure its continued availability and integrity. 41. Equipment is suitably protected to reduce the risks from environmental threats and hazards and opportunities for unauthorised access. 42. Equipment is protected from power failures and other disruptions caused by failures in supporting utilities. 43. Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage. 44. Unattended equipment has appropriate protection.	• If any remediation actions do not appear to have been implemented and the reasons are not given are they addressed as residual risks? Verify that equipment and media are adequately protected against typical information security threats. **Note**: a non-exhaustive list of typical information security threats is listed in Section 9 of the Gatekeeper Framework.

5.7 Access control management

Control	Assessment Guidance
User access management 45. An access control policy is established, documented and reviewed based on business and security requirements. 46. Access to information and application system functions is restricted in accordance with the Service Provider's access control policy 47. A formal user registration and de-registration process is implemented to enable the assignment of access rights. 48. A formal user access provisioning process is implemented to assign and revoke access rights for all user types to all systems and services. 49. Employees and contractors are only provided with access to the network and network services that they have been specifically authorised to use. 50. Access to information and the application system functions is restricted in accordance with the access control policy. 51. The access rights of all employees, contractors and external party users to information and information process facilities is removed upon termination of their employment, contract or agreement, or adjusted upon change.	Review the Information Security Documentation to verify that an access control policy exists. Consider the controls in the Information Security Documentation relating to access control and verify that: • Information dissemination and authorisation (need-to-know, need-to-access principles) are enforced. • Consistency between the access rights and information classification policies of networks, assets and ICT equipment is maintained. • Access rights are formally managed. • Access rights are removed when no longer required. Examine the previous three months of statistical data relating to system access and: • Determine using event logging or other means if system access events have been recorded as described in the Information Security Documentation and report any anomalies, and • Determine over the same period if system access controls were operated as prescribed.

Control	Assessment Guidance
Authentication Credentials 52. Access to systems and applications is controlled by a secure log-in procedure 53. Strong passphrases are used for access to systems. 54. Multi-factor authentication is used for database administrators, privileged users, Positions of Trust and remote access. 55. The allocation and use of privileged access rights is restricted and controlled. 56. The use of utility programs that might be capable of overriding system and application controls are restricted and tightly controlled.	Consider the controls in the Information Security Documentation relating to single and multi-factor authentication credentials and verify that: • Multi-factor authentication is used for database administrators, privileged users, Positions of Trust and remote access. • Passphrase policy complies with the ISM requirements for passphrase management. • A review of privileged access rights has occurred in the period since the previous Gatekeeper compliance audit (or since accreditation if undertaking the first Gatekeeper compliance audit). • Users with privileged access rights are incapable of overriding system and application security controls. • The controls are operating as prescribed.

5.8 Operations security

Control	Assessment Guidance
Strategies to Mitigate Targeted Cyber Intrusions (Top 4) 57. The ASD 'Top 4' mitigation strategies are implemented. 58. **Note**: the Top 4 mitigation strategies include: – Application whitelisting, – Patch applications – Patch operating systems, and – Restrict administrative privileges.	Verify that the Top 4 mitigation strategies are implemented. Inspect the application white list to determine if users can only execute a defined set of trusted applications. Also determine if the white list can be disabled by general users or users with privileged access. Verify that security patches and updates are implemented in accordance with the Information Security Documentation.

Control	Assessment Guidance
Standard Operating Procedures 59. Operating procedures are documents and made available to all users who need them to carry out their duties.	Review the Information Security Documentation to verify that Standard Operating Procedures are documented and communicated to staff. Verify that the SOPs are formally approved prior to release.
Change Management 60. Changes to systems are formally managed. 61. Changes to the organisation, business processes, information processing facilities and systems that affect information security are controlled. 62. Modifications to software packages are limited to necessary changes and all changes are strictly controlled.	Review the change management process and determine the adequacy of the controls implemented. Consider the following: • Are formal procedures implemented for proposed changes? • Are staff aware of their responsibilities in terms of managing change? • How are changes identified and categorised? • Where are proposed changes documented? • Are there separate processes for managing standard, urgent and emergency changes? • Are the security impacts of proposed changes assessed? • Are changes planned and tested prior to implementation in the production environment? • How are aborted changes managed (i.e. provisions for fall back) • How are the details of implemented changes communicated to relevant staff?
Backup 63. Backup copies of information, software and system images are taken and tested regularly in accordance with the Information Security Documentation. 64. Security controls are implemented to protect data transfers through communication facilities.	Review the Information Security Documentation to verify that a backup process exists. Verify that the backup process is tested in accordance with the Information Security Documentation. Verify that data transfers are conducted as prescribed in the Information Security Documentation.

Control	Assessment Guidance
System monitoring and event logging 65. Event logs recording user activities, exceptions, faults and information security events are produced, centrally stored and regularly review. 66. Logging facilities and log information is protected against tampering and unauthorised access. 67. System administrator and system operator activities are logged and the logs protected and regularly reviewed. 68. The clocks of all relevant information processing systems within an organisation or security domain are synced to a single authoritative reference time source.	Verify system monitoring and event logging is undertaken in accordance with the requirements defined in the Information Security Documentation. • What types of system events are logged? • How often are logs reviewed? • What types of events are considered suspicious activity? • What staff know how to handle suspicious log activity? Verify that monitoring and logging facilities are adequately protected. Verify the retention period for audit log information retained in backup or archive is in accordance with the Information Security Documentation. Inspect the reference time source used for event logging and verify it is consistent with Information Security Documentation. If multiple time sources are used verify that they are synchronised across the PKI environment.

5.9 CA key lifecycle management controls

Control	Assessment Guidance
CA Key Generation 69. CA key pairs are generated in controlled circumstances. **CA key usage** **70.** CA private signing keys are not used inappropriately. **CA key storage, backup and recovery** 71. CA private keys are secured and their integrity maintained throughout their lifetime. 72. CA private keys are backed up, stored and recovered in a secure manner. **CA key archive, escrow and destruction** 73. Archived CA keys remain secured and are never put back into production 74. Escrowed (if supported) CA private signing keys remain secured and their integrity maintained. 75. CA private signing keys are not used beyond the end of their life cycle. 76. CA keys are destroyed at the end of their key pair lifecycle in accordance with the CPS and CA's CP.	Review the Cryptographic Key Management Plan, CPS and CA's CP and verify the controls are implemented as prescribed. Consider the following and verify: • CA keys generated, used and controlled in accordance with the CPS and CA's CP. • CA key generation scripts are used when generating CA keys. • CA keys are generated in a physically secure environment. • The generation of CA keys is performed by personnel in trusted roles. • CA key generation activities are logged. • Keys are secured throughout their lifetime. • The security of CA keys exported from cryptographic equipment. • The controls implemented prevent inappropriate use of CA keys. • A commensurate level of security is implemented for escrowed (if supported) and backed-up copies of CA private signing keys as CA keys used in operation.
CA Public Key Distribution 77. The integrity and authenticity of the CA public key and any associated parameters are maintained during its distribution to Subscribers and Relying Parties.	Verify that the distribution of CA public keys is controlled in accordance with the CPS and CA's CP.

Control	Assessment Guidance
CA key compromise 78. Continuity of operations is maintained in the event of a suspected or actual compromise of the CA's private keys and certificates 79. Any Certificate Signing Requests or certificates signed with the compromised keys are revoked and reissued.	Review the Information Security Documentation, CPS and CA's CP and verify a compromise or a suspected compromise of a CA's private signing key is covered. Interview staff and verify they are aware of their responsibilities when handling a CA private key compromise. • What would they do? • Who would they tell?
CA cryptographic equipment lifecycle management 80. Cryptographic equipment used for CA private key storage and recovery and the interfaces to these devices are tested before usage for integrity 81. CA cryptographic hardware is functioning correctly. 82. Access to CA cryptographic equipment is limited to authorised personnel in trusted roles	Verify that CA cryptographic equipment used by the Service Provider has undergone an ASD approved cryptographic evaluation process. Verify that CA cryptographic equipment used by the Service Provider is stored in accordance with the Information Security Documentation. Verify that access to CA cryptographic equipment is controlled as prescribed in the Information Security Documentation.
Hardware token lifecycle management 83. Hardware tokens are issued to Subscribers (if supported) in a secure manner. 84. The procurement, preparation and personalisation of hardware tokens are securely controlled by the CA 85. Hardware token usage is enabled by the CA prior to issuance to Subscribers 86. Hardware token activation and re-activation is securely controlled by the CA 87. Hardware tokens are securely stored, distributed, replaced and terminated by the CA	Review the CPS and relevant CP(s) and verify that the prescribed controls are implemented. Verify that hardware tokens are generated, managed and controlled in accordance with the CPS and relevant CP(s). Verify that Subscribers are made aware of obligations regarding the use and protection of hardware tokens.

5.10 Subscriber key lifecycle management controls

Control	Assessment Guidance
Privacy of Personal Information 88. Privacy and protection of personally identifiable information is consistent with the Privacy Act 1988 and the Australian Privacy Principles. **Records Retention** 89. Records are protected from loss, destruction, falsification, unauthorised access and release in accordance with legislative, regulatory, contractual and business requirements. **Subscriber Registration** 90. Applicants are accurately identified in accordance with the Registration Authority Operations Manual, CPS and relevant CP(s) **Certificate Requests** 91. Certificate requests are accurate, authorised and complete. **Certificate Generation and Issuance** 92. Certificates are generated and issued in accordance with the CPS and relevant CP(s). **Certificate Distribution** 93. Upon issuance, complete and accurate certificates are distributed to Subscribers and Relying Parties in accordance with the CPS and relevant CP(s) **Certificate Renewal and Rekey** 94. Requests for certificates issued to a subscriber who has previously been registered with the same CA are complete, accurate and duly authorised. This includes certificate renewals, rekey following revocation or prior to expiration, or update due to change to the subscribers attributes.	Review the RA Ops Manual, CPS and relevant CP(s) and verify the following: • The processes used by the Registration Authority to verify, authenticate and validate the identity of an applicant are operating as prescribed. • The processes used by the RA comply with the Privacy Act and Australian Privacy Principles. • The controls implemented by the RA protect the sensitivity of personal information collected. • The terms and conditions regarding the use of certificates are made available to Subscribers and Relying Parties. • The RA validates requests to revoke or suspend (if supported) certificates prior to carrying out the action. **Note:** Gatekeeper requires Registration Authorities to assign, at a minimum, a Dissemination Limiting Marker of *Sensitive: Personal* to all personal information held, processed, stored or disclosed. Examine the previous three months of statistical data relating to certificate and revocation requests. Verify using event logging or other means if the certificate and revocation requests have been processed as documented in the RA Ops Manual, CPS and relevant CP(s) and report any anomalies.

Control	Assessment Guidance
Subscriber Obligations 95. The CA's terms and conditions are made available to all Subscribers and Relying Parties. **Certificate Revocation and Suspension** 96. Subscriber certificates are revoked or suspended (if supported) based on authorised and validated certificate revocation requests within the timeframe in accordance with the CPS and relevant CP(s). **Certificate Validation** 97. Timely, complete and accurate certificate status information (including CRLs and OCSP) is made available to subscribers and relying parties in accordance with the CPS and relevant CP(s).	

5.11 Incident management

Control	Assessment Guidance
98. Information security events are assessed to determine if they are to be classified as Information Security Incidents. 99. Information Security Incidents are reported through appropriate channels as soon as possible. 100. The Service Provider define and apply procedures for the identification, collection, acquisition and preservation of information which can serve as evidence. 101. Responses to Information Security Incidents occur in accordance with documented procedures. 102. Knowledge gained from analysing and resolving Information Security Incidents is used to reduce the likelihood or impact of future incidents.	Review the Incident Response Plan and test the Service Provider's incident management controls. Verify that the incident response plan has been reviewed in the period since the previous Gatekeeper compliance audit (or since accreditation if undertaking the first Gatekeeper compliance audit), Verify the incident monitoring, management and response capabilities operate as prescribed in the Information Security Documentation. Interview staff to verify they are aware of their responsibilities when handling an Information Security Incident. • What would they do? • Who would they tell?

5.12 Business continuity management

Control	Assessment Guidance
103. The organisation determines its requirements for information security and the continuity of information security management during adverse situations, e.g. during a crisis. 104. The Service Provider has established, documented, implemented and maintains processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation. 105. The Service Provider verify the information security continuity controls at least annually to ensure they are valid and effective during adverse situations. 106. Information processing facilities implement with redundancy sufficient to meet availability requirements.	Obtain evidence that the Disaster Recovery and Business Continuity plan has been tested in the period since the previous Gatekeeper compliance audit (or since accreditation if undertaking the first Gatekeeper compliance audit). Verify that the outcome of DRBCP testing has been documented. Verify the last test included a full restoration of the Root CA servers, databases, keys and data and report any anomalies. Verify that if any remediation actions do not appear to have been implemented and the reasons are not given that they are addressed as residual risks in the SRMP. Interview staff and verify they are aware of their roles and responsibilities in the event of a disaster. Verify that training programs referenced in the DRBCP have been implemented in accordance with the documented procedures?

5.13 Outsourced arrangements

Control	Assessment Guidance
107. All relevant information security requirements are established and agreed with each supplier that access, process, store, communicate or provide IT infrastructure components for the Service Provider's PKI operations.	Verify that agreements with external organisations referenced in the Service Provider's Gatekeeper Approved Documents are current and in place.

ANNEX A: Non-Compliance Ratings

Severity Rating	Definition
CRITICAL	An Authorised Auditor's determination that the Service Provider does not comply with essential protective security requirements of the Gatekeeper Framework shall be classified as a critical failure. For example, the inappropriate storage of cryptographic keys, digital certificates or passphrases shall be classified as a critical failure.
MAJOR	An Authorised Auditor's determination that the Service Provider does not comply with significant protective security requirements of the Gatekeeper Framework shall be classified as a major failure. For example, a Service Provider does not review their SRMP annually. Escalation of the problem to a critical failure shall be imposed if additional related events impact on the Service Provider's operations simultaneously.
PARTIAL	An Authorised Auditor's determination that the Service Provider does not comply with important protective security requirements of the Gatekeeper Framework shall be classified as a partial failure. For example Standard Operating Procedures not implemented in a manner consistent with the System Security Plan. Escalation of the problem to a major failure shall be imposed if additional related events impact on the Service Provider's operations simultaneously.
MINOR	An Authorised Auditor's determination that the Service Provider does not comply with general requirements of the Gatekeeper Framework shall be classified as a minor failure. For example broken links within publically available documents.

ANNEX B: Non-Compliance Template

Audit Criteria:	{e.g. Gatekeeper Approved Documents, Operations Security**}**				
Total Section Controls:	{number}	Compliant controls:	{number}	Non-compliant controls:	{number}
Authorised Auditor comments					

Control No	Severity Rating	Comment
{control #}	{As per Annex A}	
{control #}	{As per Annex A}	
{control #}	{As per Annex A}	

ANNEX C: Control Mappings – WebTrust to GCAP

The following table maps the controls listed in WebTrust to GCAP. The aim of this table is to enable Authorised Auditors a method to quickly determine what prior audit work is acceptable to be considered for a Gatekeeper compliance audit.

The column with the heading 'suitable?' provides the basis of considering previous audit work. Any row with a 'yes' means that the WebTrust audit work is suitable to cover the applicable Gatekeeper controls. Any row with a 'no' means the audit work is not considered suitable for GCAP because the controls do not adequately cover the required Gatekeeper controls.

	WebTrust		**GCAP**	**Suitable?**
1.0	**CA Business Practices Disclosure**	**5.2**	**Gatekeeper Approved Documents**	
1.1	Certification Practice Statement	5.2.4	Certification Practice Statement and Certificate Policy	Yes
1.2	Certificate Policy	5.2.4	Certification Practice Statement and Certificate Policy	Yes
2.0	**CA Business Practices Management**	**5.2**	**Gatekeeper Approved Documents**	
2.1	Certificate Policy Management	5.2.4	Certification Practice Statement and Certificate Policy	Yes
2.2	Certification Practice Statement Management	5.2.4	Certification Practice Statement and Certificate Policy	Yes
2.3	CP and CPS consistency	5.2.4	Certification Practice Statement and Certificate Policy	Yes
3.0	**CA Environmental Controls**	**-**	**Various**	
3.1	Security Management	-	Various	No
3.2	Assess Classification and Management	5.5	Media and ICT Equipment Management	Yes

	WebTrust		GCAP	Suitable?
3.3	Personnel Security	5.3	Personnel Security	No
3.4	Physical and Environmental Security	5.4	Physical and Environmental Security	Yes
3.5	Operations Management	5.7	Operations Security	No
3.6	System Access Management	5.6	Access Control Management	Yes
3.7	Systems Development and Maintenance	5.7.3	Change Management	Yes
3.8	Business Continuity Management	5.11	Business Continuity Management	Yes
3.9	Monitoring and Compliance	-	Various	No
3.10	Audit Logging	5.7.5	System Monitoring and Event Logging	Yes
4.0	**CA Key Lifecycle Management Controls**	**5.8**	**CA Key Lifecycle Management Controls**	
4.1	CA Key Generation	5.8.1	CA Key Generation	Yes
4.2	CA Key Storage, Backup and Recovery	5.8.3	CA Key Storage, Backup and Recovery	Yes
4.3	CA Public Key Distribution	5.8.5	CA Public Key Distribution	Yes
4.4	CA Key Usage	5.8.2	CA Key Usage	Yes
4.5	CA Key Archival and Destruction	5.8.4	CA key archive, escrow and destruction	Yes
4.6	CA Key Compromise	5.8.6	CA Key Compromise	Yes

	WebTrust		GCAP	Suitable?
4.7	CA Cryptographic Hardware Lifecycle Management	5.8.7	CA Cryptographic Equipment Lifecycle Management	Yes
4.8	CA Key Escrow	5.8.4	CA key archive, escrow and destruction	Yes
5.0	**Subscriber Key Lifecycle Management Controls**	**5.9**	**Subscriber Key Lifecycle Management Controls**	
5.1	CA-Provided Subscriber Key Generation Services	-	Not covered by GCAP	No
5.2	CA-Provided Subscriber Key Storage and Recovery Services	-	Not covered by GCAP	No
5.3	Integrated Circuit Card Lifecycle Management	5.8.8	Hardware Token Lifecycle Management	Yes
5.4	Requirements for Subscriber Key Management	5.9.8	Subscriber Obligations	Yes
6.0	**Certificate Lifecycle Management Controls**	**5.9**	**Subscriber Key Lifecycle Management Controls**	
6.1	Subscriber Registration	5.9.3	Subscriber Registration	Yes
6.2	Certificate Renewal	5.9.7	Certificate Renewal and Rekey	Yes
6.3	Certificate Rekey	5.9.7	Certificate Renewal and Rekey	Yes
6.4	Certificate Issuance	5.9.5	Certificate Generation and Issuance	Yes
6.5	Certificate Distribution	5.9.6	Certificate Distribution	Yes
6.6	Certificate Revocation	5.9.9	Certificate Revocation and Suspension	Yes

	WebTrust		GCAP	Suitable?
6.7	Certificate Suspension	5.9.9	Certificate Revocation and Suspension	Yes
6.8	Certificate Validation	5.9.10	Certificate Validation	Yes
7.0	**Subordinate CA Certificate Lifecycle Management Controls**	**-**	**Not covered by GCAP**	**No**
7.1	Subordinate CA Certificate Lifecycle Management	-	Not covered by GCAP	No

ANNEX D: Control Mappings – ETSI to GCAP

The following table maps the controls listed in ETSI to GCAP. The aim of this table is to enable Authorised Auditors a method to quickly determine what prior audit work is acceptable to be considered for a Gatekeeper compliance audit.

The column with the heading 'suitable?' provides the basis of considering previous audit work. Any row with a 'yes' means that the ETSI audit work is suitable to cover the applicable Gatekeeper controls. Any row with a 'no' means the audit work is not considered suitable for GCAP because the controls do not adequately cover the required Gatekeeper controls.

	ETSI		**GCAP**	**Suitable?**
6	**Obligations, Warranties and liability**			
6.1	Certification authority obligations and warranties	5.2.4	Certification Practice Statement and Certificate Policy	Yes
6.2	Subscriber obligations	5.2.4	Certification Practice Statement and Certificate Policy	Yes
6.3	Information for relying parties	5.2.4	Certification Practice Statement and Certificate Policy	Yes
6.4	Liability	5.2.4	Certification Practice Statement and Certificate Policy	Yes
7	**Requirements on CA practice**			
7.1	Certification practice statement	5.2.4	Certification Practice Statement and Certificate Policy	Yes
7.2	Public key infrastructure – key management lifecycle			
7.2.1	Certification authority key generation	5.8.1	CA Key Generation	Yes

7.2.2	Certification authority key storage, backup and recovery	5.8.3	CA Key Storage, Backup and Recovery	Yes
7.2.3	Certification authority public key distribution	5.8.5	CA Public Key Distribution	Yes
7.2.4	Key escrow	5.8.4	CA Key Archive, Escrow and Destruction	Yes
7.2.5	Certification authority key usage	5.8.2	CA Key Usage	Yes
7.2.6	End of CA key lifecycle	5.8.4	CA Key Archive, Escrow and Destruction	Yes
7.2.7	Lifecycle management of cryptographic hardware used to sign certificates	5.8.7	CA Cryptographic Equipment Lifecycle Management	Yes
7.2.8	CA provided subject key management services	5.8.8	Hardware Token Lifecycle Management	Yes
7.2.9	Secure user device preparation	5.8.8	Hardware Token Lifecycle Management	Yes
7.3	Public key infrastructure – Certificate management lifecycle			
7.3.1	Subject registration	5.9.3	Subscriber Registration	Yes
7.3.2	Certificate renewal, rekey and update	5.9.7	Certificate Renewal and Rekey	Yes
7.3.3	Certificate generation	5.9.5	Certificate Generation and Issuance	Yes
7.3.4	Dissemination of terms and conditions	5.9.8	Subscriber Obligations	Yes
7.3.5	Certificate dissemination	5.9.6	Certificate Distribution	Yes

7.3.6	Certificate revocation and suspension	5.9.9	Certificate Revocation and Suspension	
7.4	CA management and operation			
7.4.1	Security management	-	Various	No
7.4.2	Asset classification and management	5.5	Media and ICT equipment management	No
7.4.3	Personnel security	5.3	Personnel Security	Yes
7.4.4	Physical and environmental security	5.4	Physical and Environmental Security	No
7.4.5	Operations management	-	Various	No
7.4.6	System access management	5.6	Access Control Management	Yes
7.4.7	Trustworthy systems development and maintenance	5.7.3	Change Management	Yes
7.4.8	Business continuity management and incident handling	-	Various	No
7.4.9	CA termination	-	Not covered by GCAP Covered in Gatekeeper Head Agreement/Memorandum of Agreement	No
7.4.10	Compliance with legal requirements	5.9.1	Privacy of Personal Information	Yes
7.4.11	Recording of information concerning certificates	5.9.5	Certificate Generation and Issuance	Yes

7.5	Organisational	5.2.4	Certification Practice Statement and Certificate Policy	Yes
7.6	Additional requirements	-	Not covered by GCAP	No
7.6.1	Additional testing	-	Not covered by GCAP	No
7.6.2	Cross certificates	-	Not covered by GCAP	No
8	**Framework for the definition of other certificate policies**			
8.1	Certificate policy management	5.2.4	Certification Practice Statement and Certificate Policy	
8.2	Additional requirements	-	Not covered by GCAP	No
8.3	Conformance	-	Not covered by GCAP	No