

UNCLASSIFIED

I-RAP Gateway Certification Report Template

Version 1.0

April 2004



Point of Contact: DSD I-RAP Manager
Phone: (02) 6265 0197
Email: assist@dsd.gov.au

Information Security Group
Defence Signals Directorate
Locked Bag 5076
Kingston ACT 2604

UNCLASSIFIED

1

PURPOSE3

TABLE OF CONTENTS FOR REPORT4

REPORT TEMPLATE5

 Formal Acceptance.....5

 Executive Summary.....5

 Background5

 Assessment Scope.....5

 Documents for Review5

 Waivers5

 References6

 Phase 1 - Documentation Review6

 Introduction6

 The Concept of Operations.....6

 Security Risk Assessment6

 The Gateway Policy Documents7

 Access Policy7

 Security Policy7

 Contingency Policy7

 Incident Detection and Response Policy.....7

 Gateway Logical/Infrastructure Diagram7

 Mandatory Requirements7

 Risk Based Requirements8

 List of Critical Configurations.....8

 Security Administration Tasks8

 Proactive Security Checking Tasks8

 Proactive Security Audit Checks.....9

 Phase 2 - Site Visit9

 Introduction9

 Staff Interviews9

 Configuration Compliance Checks9

 Physical Security10

 Conclusion.....10

PURPOSE

1. The following report template is provided to assist I-RAP assessors in the conduct of a Gateway Certification and FedLink Connection Assessment. This template is to be used as a basis for Gateway Certification Reports, and provides a guide as to what details DSD expects to see within each section. For a more detailed discussion of requirements assessors must read the relevant sections of *Australian Government Information Technology Security Manual (ACSI 33)*, 2004 and the *Gateway Certification Guide (GCG)*, 2004 as well as the *Gateway Certification Checklist*, which can be found on DSD's website: <http://www.dsd.gov.au/infosec>.
2. I-RAP assessors **MUST** compile a certification report as well as completing the I-RAP Gateway Certification Checklist. This report must demonstrate how the I-RAP assessor reviewed the policy documentation and verified that the procedures mentioned therein as operational procedures are operational. Comments in this report are also to be used for providing some justification for decisions.
3. Consider whether to issue certification, provisional certification or NO certification. Certification lasts for 12 months, with the exception of provisional certification. If any of the mandatory requirements have not been demonstrated, NO certification must be the result, apart from the specific cases, including provisional certification, where I-RAP assessors have consulted DSD.
4. In the report, provide any recommendations based on non-mandatory best practice guidelines that have not been demonstrated by the agency or service provider.
5. I-RAP assessors **MUST** forward a copy of the completed checklist and this certification report to DSD if a Gateway is to be certified as meeting the requirements of DSD and Australian Government policy or if an agency/organisation is being assessed for FedLink connection.
6. The formal I-RAP certification report **MUST** include sign off from the ITSA/ITSM of the Australian Government Agency or Service Provider stating that, to the best of the ITSA/ITSM's knowledge, the I-RAP assessor who has signed the certification report has actively participated in conducting the assessment work leading to certification.
7. Where an agency has received a waiver from the Attorney-General's department for a particular mandatory requirement, this **MUST** be indicated in the Gateway Certification Report and in the relevant section of the Gateway Certification Checklist.
8. I-RAP assessors **MUST** verify that the procedures mentioned within policy documentation as being operational procedures, are operational. To do this I-RAP assessors **MUST** have the agency/organisation's IT Security Advisor (ITSA), or an authorised agency/organisation system administrator, demonstrate these procedures. I-RAP assessors **MUST** include comments as to how well the agency or organisation achieved the requirements.
9. Address details for DSD I-RAP Manager:

The I-RAP Manager
Information Security Group
Defence Signals Directorate
Locked Bag 5076
Kingston ACT 2604

TABLE OF CONTENTS FOR REPORT

Formal Acceptance

Executive Summary

Background

Assessment Scope

Documents for Review

Waivers

References

Phase 1 - Documentation Review

Introduction

The Concept of Operations

Security Risk Assessment

The Gateway Policy Documents

 Access Policy

 Security Policy

 Contingency Policy

 Incident Detection and Response Policy

Gateway Logical/Infrastructure Diagram

Mandatory Requirements

Risk Based Design Criteria

List of Critical Configurations

Security Administration Tasks

Proactive Security Checking Tasks

Proactive Security Audit Checks

Phase 2 - Site Visit

Introduction

Staff Interviews

Configuration Compliance Checks

Physical Security

Conclusion

REPORT TEMPLATE

Formal Acceptance

This I-RAP certification report **MUST** include a **sign off from the ITSA/ITSM of the Australian Government Agency or Service Provider**. This states that, to the best of the ITSA/ITSM's knowledge, the I-RAP assessor who has signed this certification report has actively participated in conducting the assessment work leading to certification.

Executive Summary

The Executive Summary **summarises key details of the process and findings, the outcome and maybe some recommendations**. Include who conducted the certification, when, for whom and to what level eg IN-CONFIDENCE, RESTRICTED or PROTECTED and whether to issue certification, provisional certification or NO certification. If issuing provisional or no certification, include an outline of the reasons for this.

Background

This sets the scene for the certification. Provide brief details of the Australian Government agency or organisation or Service Provider, and any previous DSD or I-RAP certifications.

Assessment Scope

I-RAP assessment is based on compliance with MANDATORY REQUIREMENTS and a value judgement against industry best practice. To pass certification, **ALL** mandatory requirements **MUST** be met, unless specific written approval for this instance has been given by DSD and it is fully documented in the Risk Assessment. This scope **identifies areas to be included in or excluded from the assessment, apart from these mandatory requirements**.

Documents for Review

This is a **list of all the documents provided to assist in the certification assessment** by the agency or organisation or service provider.

Waivers

Detail any waivers the agency has received from the Attorney-General's department for any particular

mandatory requirements.

References

This is a **list of all documents used by the I-RAP assessor as references during the conduct of the certification assessment**. Include the PSM, ACSI33, any Standards Australia materials and other such references.

Phase 1 - Documentation Review

Introduction

A major component of an I-RAP certification assessment is the documentation review. The agency or organisation **MUST** document their policies, procedures and configurations to form a clear understanding for all staff of the agency's or organisation's sound security management philosophy.

Documentation **MUST** be examined for consistency within each document and across all the documentation.

Outline here the process you undertook to conduct the documentation review.

Concept of Operations

The Concept of Operations is a brief overview that provides a basic background on how the Gateway was designed and its key features, as well as the agency or organisation's overall security culture.

Outline here what is included in the document, and recommendations to any shortcomings that would improve its usefulness.

Security Risk Assessment

The Security Risk Assessment is critical to the success of a Gateway environment, especially with the current trend toward using risk-managed approaches. It should provide enough details to guide the priority of countermeasures, and therefore be reflected in all the policy and operational documents.

The likelihood and consequence levels **MUST** be defined in the Risk Assessment, and that the CEO or delegate **MUST** have signed off as having read and accepted the Risk Assessment.

Describe your findings in relation to these requirements and outline the risk assessment methodology used.

Gateway Policy Documents

The Gateway policy documents need to describe the philosophy by which the Gateway is managed. They should be easily communicated and understood throughout the agency or organisation, and need to be enforceable. Well-written policies should be brief, clearly detailing the key policy objectives and responsibilities. Details on how the gateway is managed, and how policy issues are implemented are to be addressed in plans and procedures documents, not in the policy documents.

For each policy document, **outline what is included in the particular document in relation to the requirements, and recommendations to any shortcomings that would improve the particular policy document's usefulness.**

Access Policy

A clear link **MUST** be demonstrated between the Access Policy and the Security Risk Assessment, and the policy objectives and countermeasures **MUST** be appropriate to the level of identified risk.

Security Policy

A clear link **MUST** be demonstrated between the Security Policy and the Security Risk Assessment, and the policy objectives and countermeasures **MUST** be appropriate to the level of identified risk.

Contingency Policy

A clear link **MUST** be demonstrated between the Contingency Policy and the Security Risk Assessment, and the policy objectives and countermeasures **MUST** be appropriate to the level of identified risk.

Incident Detection and Response Policy

It **MUST** be stated in this policy that there is notification to DSD in accordance with ACSI 33 and GCG minimum policy standards, and that DSD and gateway clients for service providers **MUST** be information addressees on off-line analytical reports and on all incidents that require investigative action.

Gateway Logical/Infrastructure Diagram

The Gateway Logical/Infrastructure Diagram should be a reflection of what connectivity exists outside of gateway safeguards and what steps will be taken to minimise and control these other connections.

Any connectivity that does not pass through the gateway **MUST** be documented and considered in the Risk Assessment.

Outline any connectivity that does not pass through the gateway and how it is addressed in the Risk Assessment.

Mandatory Requirements

DSD has established requirements to ensure that there is a minimum required standard for all gateways. The I-RAP checklist contains many of these requirements and they are addressed throughout this report.

Detail here the overall adherence to the requirements and any instances where there are issues with meeting them.

Risk Based Requirements

The Risk Based Requirements document identifies the Gateway components that have been designed to mitigate specific risks that were referenced in the Security Risk Assessment.

Outline here what is included in the document, and any risks that have not been addressed.

List of Critical Configurations

The List of Critical Configurations summarises the expected configurations and security parameters of key elements within the Gateway environment.

The agency or organisation **MUST** have consistently listed critical configurations, which are then reflected in Incident Detection, Configuration Management and Contingency strategies.

Describe your findings in relation to these requirements and outline recommendations to any shortcomings that would improve the list's usefulness.

Security Administration Tasks

Standard security administration tasks that form part of the gateway security management should be formalised and approved by the ITSA/ITSM. These formal plans and procedures need to be realistic and achievable.

The agency or organisation **MUST** have:

- Accounts Administration Plan and Procedures
- Privileged Users Plan and Procedures
- Access Control Plan and Procedures
- Key Management Plan and Procedures
- Physical Access Plan and Procedures
- Backup, Maintenance and Media Control Plan and Procedures.

Describe your findings in relation to these requirements and outline recommendations to any shortcomings that would improve the agency / organisation's gateway security management.

Proactive Security Checking Tasks

Proactive security checking tasks are crucial to the security of the gateway environment and should be formalised and approved by the ITSA/ITSM.

The agency or organisation **MUST** have:

- Firewall Configuration Checking Plan and Procedures
- Proxy Server Configuration Checking Plan and Procedures
- Crypto Configuration Checking Plan and Procedures
- Alarm and Access Control Plan and Procedures.

Describe your findings in relation to these requirements and outline recommendations to any shortcomings that would improve the agency / organisation's gateway security management.

Proactive Security Audit Checks

Proactive security audit checks are crucial to the security of the gateway environment and should be formalised and approved by the ITSA/ITSM.

These procedures **MUST** be written, approved by the ITSA/ITSM and have a demonstrated implementation. The agency / organisation **MUST** have Real Time Reporting and Off-Line or Analytical Reporting Plans and Procedures.

Describe your findings in relation to these requirements and outline recommendations to any shortcomings that would improve the agency / organisation's gateway security auditing.

Phase 2 - Site Visit

Introduction

Very briefly describe your site visit. Include when, which sites and your key objectives from the visit.

Staff Interviews

Interviewing key personnel should address any questions and clarify any issues raised from the documentation review. It should also provide the I-RAP assessor with an understanding of staff attitudes and the security culture within the agency / organisation.

Outline the results of any staff interviews in helping to resolve any issues.

Configuration Compliance Checks

The firewall is the most important policy-enforcing device within the gateway environment, and therefore it is essential for it to be configured appropriately. As firewalls are evaluated within certain configurations, the I-RAP assessor needs to ensure that the firewall configuration is appropriate

UNCLASSIFIED

Firewalls used to protect the internal networks **MUST** conform to DSD's minimum standard as outlined in ACSI 33, and the configuration and management of the firewalls **MUST** be in compliance with the EPL certification report. Any security checking and auditing tools referred to in the documentation **MUST** be operational.

Describe your findings in relation to these requirements and outline any shortcomings that would improve the agency / organisation's gateway security.

Physical Security

The physical security of the gateway premises **MUST** be certified as meeting minimum standards prescribed by ASIO T4. An Agency Security Advisor (ASA) can conduct this certification, however, for service providers, this **MUST** be conducted by T4.

Describe your findings in relation to this requirement and outline recommendations to any shortcomings that would improve the agency / organisation's physical gateway security. If certified by T4, cite the letter and forward a copy with the report to T4.

Conclusion

The conclusion brings together your findings as outlined in the report and checklist. It explains whether the agency / organisation has provided enough evidence for the I-RAP assessor to be confident that the minimum requirements are met, and the agency or organisation is following industry best practice and adhering to their policies and procedures.

The conclusion should also contain **the I-RAP assessor's verdict for certification and at what level.**

Advise when the certification expires or if provisional certification has been granted, specify a date by which the issues must be fixed or lose the certification (contact the DSD I-RAP Manager for further guidance about provisional certification).

Advise of the requirement to maintain a policy documentation suite to reflect major changes to key components so that changes do not compromise best practice evaluation.

Advise Australian Government agencies and Australian Government Service Providers that they should provide regular advice to DSD on significant changes to the gateway environment or the analysed threat level.

UNCLASSIFIED

10