

I-RAP FedLink Audit Guidelines & Checklist

Version 1.4

JUNE 2003



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 (SECURITY-IN-CONFIDENCE after first entry)

The following guidelines and checklist are provided to direct I-RAP assessors during the conduct of a FedLink audit. **Note:** All elements of this checklist are **MANDATORY REQUIREMENTS**. An Agency/Organisation must meet all requirements within this checklist to satisfactorily meet the requirements for ongoing FedLink connection. If assessors have extra comments they should attach these to the back of the checklists. **Note:** For the purposes of ensuring compliance with Commonwealth policy it is important that I-RAP assessors and others consider all FedLink policy, not just the information contained within this checklist. For FedLink policy guidance see the FedLink website: <http://www.fedlink.gov.au>.

Background

1. FedLink audits are a requirement levied on agencies connected to FedLink at IN-CONFIDENCE level. The FedLink Management Committee (FEDMAC) will identify which agencies connected to FedLink at IN-CONFIDENCE level must undergo a FedLink security compliance audit. **Note:** The FEDMAC may also identify agencies with PROTECTED level connection for FedLink security compliance audit.
2. Once FEDMAC has identified an agency for a FedLink security compliance audit an I-RAP assessor must be engaged to perform the audit, unless DSD has directed that DSD auditors will undertake the work. Audits must be conducted against claims made in the claim for compliance checklist in the FedLink Gateway Self Assessment Guide.
3. The Gateway Self Review Statement of Compliance must be completed by all agencies and organisations applying to join FedLink at IN-CONFIDENCE level that do not have DSD Gateway Certification or are not hosted by a DSD-certified Gateway Service Provider with DSD-assessed FedLink connectivity.

The FedLink audit process

4. A FedLink audit is comprised of two components, these are:
 - A. A documentation review; and
 - B. A physical inspection of the gateway environment.

Documentation review

5. The documentation review is to establish that appropriate documentation exists, as claimed in the Gateway Self Review Statement of Compliance.

Physical inspection

6. The physical inspection is to examine the security of the gateway environment, particularly the physical security measures protecting the FedLink router. The FedLink router should be co-located with other security enforcing devices.
7. I-RAP assessors should work through the supplied checklist to verify agency claims made for compliance.
8. The results of this checklist must be compared to claims made in the original checklist (a copy of this original checklist will be supplied by FEDMAC to the I-RAP assessor conducting the assessment). Current contact details for FEDMAC can be obtained from the National Office for the Information Economy on (02) 6271 1585.
9. I-RAP assessors must forward a copy of this completed checklist to DSD. DSD will review the results and forward the checklist to FEDMAC (see address below).

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

10. It is also a **MANDATORY REQUIREMENT** that the formal FedLink audit checklist includes sign off from the ITSA/ITSM of the Commonwealth Dept./Agency or Commonwealth Service Provider stating that, to the best of the ITSA/ITSM's knowledge, the I-RAP assessor who has signed the FedLink audit checklist has actively participated in conducting the assessment work.

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

I-RAP Checklist for FedLink Audit

Agency/Organisation Name: _____

Address of Gateway: _____

Gateway Administration Procedures

17. Have the following gateway administration procedures been developed as a minimum:

- | | Yes | No |
|---|-----|----|
| - Account administration | Y | N |
| - Backup, maintenance and media control | Y | N |
| - Change control | Y | N |
| - Incident reporting | Y | N |
| - Archive requirements | Y | N |

18. List any other developed gateway administration procedures:

19. Are gateway administration staff aware of all developed gateway administration procedures?

Yes No
Y N

20. Have developed procedures been implemented in practice?

Y N

21. Are all gateway administration procedures consistent with the agency security policy document?

Y N

Comments: _____

Change Control

22. Has a formal change control process been developed?

Yes No
Y N

23. Does the change control process include formal testing procedures?

Y N

24. Does the change control process include a formal process for review and approval of changes?

Y N

25. Are gateway administration staff aware of change control procedures and is there evidence of implementation?

Y N

Comments: _____

Incident Reporting

Yes No

26. Are gateway administration staff aware of the correct procedures to follow when an incident occurs? Y N

27. Do gateway administration staff understand the PSM requirement to report all Category 3 or higher incidents to DSD as soon as practicable? Y N

Comments: _____

Physical Security

Yes No

28. Has a minimum of an ASIO SCEC certified intruder alarm been installed? Y N

29. List any other physical security measures in place:

Comments: _____

Archives Requirements

Yes No

30. Do staff understand the requirement to retain logs in accordance with the National Archives Act of Australia, 1983? Y N

31. Are procedures in place to retain and appropriately store logs for the required period of time and is this demonstrated? Y N

Comments: _____

Recovery of Gateway Services

	Yes	No
32. Have policies, processes and procedures been developed and implemented to ensure recovery of gateway services?	Y	N

Comments: _____

Gateway Design

	Yes	No
33. Are all services passing through the gateway denied by default unless expressly permitted?	Y	N

34. Is all traffic between the internal FedLink servers and the Internet routed through a firewall that is listed on the DSD Evaluated Products List (EPL) as evaluated to EAL2?	Y	N
--	---	---

35. Is management of the firewall via a secure, authenticated link?	Y	N
---	---	---

36. Have systems been developed, tested and implemented to mitigate the high risk of end-users sending classified information over the Internet (an email classification system is one example)?	Y	N
--	---	---

AND/OR

37. Are end-user education policy, plans and procedures in place to mitigate the risk of end-users sending classified information over the Internet?	Y	N
--	---	---

Comments: _____

Executive Signature

38. Has the Gateway Self Review Statement of Compliance been signed by the IT Security Manager (ITSM) and CEO or delegate?	Y	N
--	---	---

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)

39. As the ITSA/ITSM or authorised IT security delegate I can state that, to Y N
the best of my knowledge (insert I-RAP assessor name: _____)
has actively participated in the conduct of this FedLink audit.

ITSA/ITSM/Authorised IT Security Delegate name: _____

Position held within organisation: _____

UNCLASSIFIED (SECURITY-IN-CONFIDENCE after first entry)
