

*DEFENCE SIGNALS DIRECTORATE*

*INFOSEC-REGISTERED ASSESSOR PROGRAM*

---



**Policy and Procedures for the  
Infosec-Registered Assessor Program (I-RAP)**

**Version 3.4**

## **FOREWORD**

This Policy and Procedure for the Infosec–Registered Assessor Program (I-RAP) has been developed as an initiative of the Australian Government Department of Defence - Defence Signals Directorate (DSD) utilising the services of SecureLink Pty Ltd (SecureLink). This document details the framework for establishing consistent Australia-wide standards for assessing and registering persons to carry out the assessment of Information and Communications Technology (ICT) security systems applied to Australian Government and other's electronic information systems in accordance with Australian Government information security policies.

It sets out the structure of the Program, including the required assessment, qualifications and training that potential assessors must undertake to be registered, and once registered, the obligations of those registered assessors.

In addition, it provides information to individuals wishing to offer their services, as registered assessors, to Australian Government Departments and Agencies (and others), with the means to demonstrate their understanding of the Program. It will also provide Australian Government Departments and Agencies (and others) preferring their electronic information systems to be assessed to the information security standards set by the DSD with a simple way of identifying consultants, considered competent by the DSD, for consideration to assess their electronic information security assets.

The provisions within the Policy and Procedures will be periodically reviewed by the Australian Government Defence Signals Directorate in conjunction with SecureLink and users of the Program.

**Revision History**

<b>Date of Revision</b>	<b>Author of Changes</b>	<b>Version Number</b>	<b>Summary of Changes</b>
2003-01-31	T Ehret	V1.0	First approved version
2003-02-13	T Ehret	V1.1	Clause 7.2 reviewed - First Published version
2003-03-03	T Ehret	V1.2	Clause 7.5 modified and all references to Gatekeeper removed (Clauses 1.2(d), 10, E.3.4 and Table 3)
2003-04-09	T Ehret	V1.3	Modifications to Clauses 7.2.2, 7.6, 13.3, 15.1, 15.2, E.2, E.3.1 and E.3.2. Also editorial changes throughout.
2003-06-05	T Ehret	V1.4	Clause 2.2 editorial change to Note
2003-08-03	T Ehret	V1.5	Modification to Clause 13.3 and the addition of Clause E.4
2003-08-22	T Ehret	V1.6	Addition of new Clause E3.1. Renumber Clauses E3.2 to E3.7
2004-01-07 (Not Published)	T Ehret	V1.7	Editorial Updates to Foreword, Introduction, Clauses A.2, B.3.3, B.3.4, B.5, G.2.1, G.2.4, G.3.1 and G.3.4. Updates to hyperlinks in Table 3 and Table 4.
2004-02-16	T Ehret	V2.0	V1.7 changes. Gatekeeper re-introduced in Clauses 1.2, 3, 10.1, Table 3 and Appendix E. Also other changes in Clauses 7.2.3, 8.5, 12.2, B.4.3, D.2.3.and Appendix F
31 Nov 2005	D Jarvis	V3.0	Updates as a result of change of Administrator
14 Aug 2006	D Jarvis	V3.1	Updates to reflect minor certificate policy changes
19 Apr 2007	D Healy	V3.2	Updates to reflect security checking requirements
30 Oct 2009	D Jarvis	V3.4	Updates to reflect 2009 ISM and HP Cert' changes

## TABLE OF CONTENTS

FOREWORD .....	II
INTRODUCTION .....	9
1 SCOPE .....	9
1.1 Scope of the Policy and Procedures.....	9
1.2 Scope of the Infosec–Registered Assessors Program .....	9
2 OBJECTIVES .....	10
2.1 Objectives of the Policy and Procedures .....	10
2.2 Objective of the Infosec–Registered Assessors Program .....	11
3 APPLICATION OF THE INFOSEC–REGISTERED ASSESSORS PROGRAM .....	11
4 OVERVIEW OF THE INFOSEC–REGISTERED ASSESSORS PROGRAM.....	11
4.1 General.....	11
4.2 I-RAP overview .....	11
4.3 I-RAP operations .....	12
5 CONTACT WITH THE INFOSEC–REGISTERED ASSESSORS PROGRAM.....	13
5.1 General.....	13
5.2 Contact Policy.....	13
6 FEES .....	13
6.1 General.....	13
6.2 Fee policy .....	13
7 ASSESSOR ENDORSEMENT .....	13
7.1 General.....	13
7.2 Pre-qualification .....	15
7.2.1 Pre-qualification policy.....	15
7.2.2 Pre-qualification requirement .....	15
7.2.3 Academic qualifications .....	15
7.3 I-RAP qualification for endorsement.....	16
7.4 Endorsement maintenance .....	16
7.5 Certificate of endorsement.....	17

7.6	Endorsement fees.....	17
8	ASSESSOR REGISTRATION.....	17
8.1	General.....	17
8.2	Publication of registration.....	17
8.3	Registered information .....	18
8.4	Registration period.....	18
8.5	Registration fee.....	18
9	ASSESSOR OBLIGATIONS .....	18
9.1	General.....	18
9.2	Assessor obligations .....	18
9.3	Declaration.....	19
10	CONDUCT OF REGISTERED ASSESSORS .....	19
10.1	General .....	19
10.2	Conduct Requirements .....	19
11	REVIEW OF WORK CONDUCTED BY REGISTERED ASSESSORS .....	20
11.1	General .....	20
11.2	Initiation of review .....	20
12	WITHDRAWAL OF ENDORSEMENT .....	20
12.1	General .....	20
12.2	Grounds for withdrawal .....	20
12.3	Notice of withdrawal.....	21
12.4	Fee considerations with respect to withdrawal of I-RAP registration.....	21
13	CONFLICT OF INTEREST .....	22
13.1	General .....	22
13.2	Assessor conflict of interest obligations.....	22
13.3	Potential conflict of interest .....	22
13.4	Potential conflict of interest penalties .....	22
14	COMPLAINTS AND DISPUTES.....	23
14.1	General.....	23
14.2	Scope of complaints and disputes .....	23
14.3	Handling and recording.....	23

14.4	Acknowledgement and responsiveness .....	23
14.4.1	Complaints .....	23
14.4.2	Disputes .....	24
15	PUBLICITY AND DOCUMENTATION .....	25
15.1	General .....	25
15.2	Advertising and promotion.....	25
15.3	Documentation .....	25
15.4	Administrative reporting .....	25
15.5	Register of Infosec Assessors.....	26
APPENDIX A	SCHEDULE OF FEES (INFORMATIVE) .....	27
A.1	General.....	27
A.2	Schedule of fees .....	27
APPENDIX B	ASSESSOR QUALIFICATION PROCEDURE (NORMATIVE) .....	28
B.1	General.....	28
B.2	Initial contact .....	28
B.3	The Application .....	28
B.3.1	Announcement of intake.....	28
B.3.2	Contents of the Application .....	28
B.3.3	Criminal History Check .....	30
B.3.4	Application fee.....	30
B.3.5	Lodgement of the application .....	31
B.3.6	Application verification .....	31
B.4	Training and assessment .....	31
B.4.1	Confirmation of training .....	31
B.4.2	Training.....	33
B.4.3	Assessment test .....	33
B.5	Qualification fees.....	34
APPENDIX C	ASSESSMENT GUIDES/REFERENCE DOCUMENTS (NORMATIVE) ...	35
C.1	General.....	35
C.2	I-RAP assessment guides.....	35

C.3	Reference documents.....	35
APPENDIX D	REGISTRATION RENEWAL PROCEDURE (NORMATIVE).....	37
D.1	General.....	37
D.2	Refresher training .....	37
D.2.1	Confirmation of training.....	37
D.2.2	Training.....	37
D.2.3	Assessment test.....	38
D.3	Registration update .....	38
D.4	Renewal fees.....	39
APPENDIX E	REQUIREMENTS FOR CONDUCTING ACTIVITIES WITHIN THE SCOPE OF THE I-RAP (NORMATIVE).....	40
E.1	General.....	40
E.2	Advertising and Promotion.....	40
E.3	Provision of services.....	40
E.3.1	Execution of assessments.....	40
E.3.2	Reporting of assessments.....	41
E.3.3	Gateway/CDS Assessments.....	41
E.3.4	Information system assessments.....	42
E.3.5	Gatekeeper assessments.....	42
E.3.6	FedLink audits .....	42
E.3.7	FedLink connection assessments.....	42
E.3.8	Physical security reviews.....	43
E.4	Provision of the DSD ICT security system compliance certificate template.....	43
APPENDIX F	WITHDRAWAL OF ENDORSEMENT PROCEDURES (NORMATIVE) ..	44
F.1	General.....	44
F.2	Handling considerations for withdrawal of I-RAP registration .....	44
F.3	Notice of withdrawal of I-RAP registration.....	44
F.4	Appeals against withdrawal of I-RAP registration .....	44
APPENDIX G	COMPLAINTS AND DISPUTE PROCEDURES (NORMATIVE).....	45
G.1	General.....	45
G.2	Complaints.....	45

G.2.1	Lodgement of complaints .....	45
G.2.2	Handling of general complaints .....	45
G.2.3	Handling of complaints about I-RAP endorsed assessors.....	46
G.2.4	Legal complaints.....	47
G.2.5	Complaint appeals .....	48
G.3	Disputes .....	48
G.3.1	Advice of disputes .....	48
G.3.2	Handling of operational disputes .....	48
G.3.3	Handling of disputes against an application or assessment results .....	49
G.3.4	Legal disputes .....	49
G.3.5	Dispute appeals .....	50

## **POLICY AND PROCEDURES: INFOSEC–REGISTERED ASSESSORS PROGRAM (I-RAP)**

### **Introduction**

The Infosec–Registered Assessors Program (I-RAP) is an initiative of the Australian Government Department of Defence – Defence Signals Directorate (DSD). The Program has been developed by the DSD, utilising the services of SecureLink Pty Ltd (SecureLink), to provide advice and to produce Program tools, including the Program policy, operational documents and a support website. SecureLink has also been appointed by DSD as the I-RAP Administrator.

The Program had an initial operational timeframe of three years. The Program was reviewed and evaluated at the end of the third year of operation by the DSD in conjunction with SecureLink, and a decision was made to continue the Program for the foreseeable future.

If the Program was to cease to operate, Australian Government agencies and all assessors registered under the Program will be notified and all assessor intakes and renewals scheduled for training will be cancelled.

NOTE : The DSD can decide to dissolve the Program if it deems it appropriate to do so.

## **1 Scope**

### **1.1 Scope of the Policy and Procedures**

This document sets out the rules and procedural requirements for the qualification and registration of persons as Information and Communications Technology (ICT) security system assessors endorsed by the Infosec–Registered Assessors Program (I-RAP).

It covers the provision of policy for the structure and operation of the Program and outlines the obligations of individuals, once registered, under the Program. It does not cover the commercial or contractual aspects of service procurement activities occurring between assessors and their clients.

This document also provides a set of procedures, which will satisfy these requirements.

### **1.2 Scope of the Infosec–Registered Assessors Program**

The Infosec–Registered Assessors Program provides an infrastructure for endorsing assessors as competent to assess ICT security systems in accordance with Australian Government information security standards and policy documents.

Individual candidates qualifying for endorsement and registration as I-RAP registered assessors are endorsed to carry out the following types of assessment work for Australian Government agencies (and others):

- a) Gateway/Cross Domain Solution (CDS) assessments of IT systems at X-IN-CONFIDENCE, PROTECTED, HIGHLY PROTECTED and RESTRICTED levels, subject to the assessor having appropriate security clearances;
- b) Network and ICT System reviews for compliance with Part C of the Protective Security Manual (PSM), and consistency with the Australian Government Information Security Manual (ISM), ISO AS/NZS standards, and best practice for X-

IN-CONFIDENCE, PROTECTED, HIGHLY PROTECTED and RESTRICTED level IT systems, subject to the assessor having appropriate security clearances;

- c) FedLink audits for agencies that have conducted FedLink self-review connection at X-IN-CONFIDENCE level and FedLink assessments, subject to the assessor having appropriate security clearance; and
- d) Gatekeeper assessments and reviews for ICT systems at HIGHLY PROTECTED level, subject to the assessor having appropriate security clearances.

and will be granted the right to issue a Certificate of Compliance with DSD and Australian Government policy and best practice standards where an ICT security system or Gateway/CDS is found to be in accordance with DSD and Australian Government policy and best practice requirements.

NOTE : Other than a Criminal Records check and declaration of Citizenship, the provision of security clearances is not an objective of the I-RAP and is considered a matter between assessors and the agencies engaging them.

It is envisaged that Australian Government agencies (and others) that would normally request the DSD to assess their ICT security systems will use the Program as a means of selecting assessors to carry out the assessments using I-RAP endorsement as a reference of competency. The selection of assessors registered in the Program would be on a commercial competitive basis. Registration in the Program does not guarantee that individuals will be engaged by Australian Government agencies to undertake information security assessments.

NOTE : The reference to “and others” throughout this document refers to those non-Australian Government entities which have a requirement to have their ICT security systems assessed to the same standard, using the same criteria that Australian Government departments and agencies must be assessed against.

## **2 Objectives**

### **2.1 Objectives of the Policy and Procedures**

The objectives of this Policy and Procedures document are as follows:

- a) To provide I-RAP Administrators with the guidance required to enable management of the Program;
- b) To provide candidates and I-RAP registered assessors with the obligations they are required to undertake to comply with endorsement by the Program; and
- c) To provide Australian Government agencies (and others) with information and guidance about the Program.

## **2.2 Objective of the Infosec–Registered Assessors Program**

The objective of the I-RAP is to provide Australian Government agencies (and others) with a pool of competent Information and Communications Technology (ICT) security assessors that can be engaged to undertake security evaluations and assessments of their ICT systems within the scope of the Program. Access to information about this pool of assessors will be via the Register of Infosec Assessors available on the Internet.

NOTE : DSD retains the right to conduct work at these levels where it deems it appropriate to do so. The Defence Security Authority (DSA) also retains the right to conduct Defence work at these levels where it deems is appropriate to do so.

## **3 Application of the Infosec–Registered Assessors Program**

I-RAP Endorsement and Registration is restricted to individuals.

Employers of I-RAP registered assessors must not advertise that their organisation is I-RAP registered. Organisations may advertise that they have I-RAP registered assessors on staff.

Unless otherwise directed by DSD, candidates qualifying for endorsement and registration as I-RAP registered assessors may enter into contracts, either individually or through their employers, with Australian Government agencies to assess and report on ICT security systems processing classified information at the IN-CONFIDENCE, PROTECTED, HIGHLY PROTECTED or RESTRICTED levels, providing they have the appropriate level of security clearance. A standard Australian Government contract will be supplied for use between the assessor (or their employer) and Australian Government agencies. An Australian Government agency may choose to use the standard Australian Government contract for this purpose, or alternatively, may use its own contractual template.

NOTE : Other than a Criminal Records check and declaration of Citizenship, the provision of security clearances is not an objective of the I-RAP and is considered a matter between assessors and the agencies engaging them.

Apart from potential conflict of interest situations, agencies and organisations must be allowed the freedom to employ the I-RAP registered assessor of their choice. Agencies or organisations should not be forced to use the services of any particular I-RAP registered assessor.

## **4 Overview of the Infosec–Registered Assessors Program**

### **4.1 General**

The sub clauses that follow in this Clause (4) provide a general description of the I-RAP including the qualifying stages for I-RAP endorsement and review of work within the scope of the Program carried out by I-RAP endorsed assessors. The policy details of each stage are contained in subsequent Clauses.

### **4.2 I-RAP overview**

The I-RAP is a program of activities sponsored by the Australian Government Department of Defence - Defence Signals Directorate (DSD) that culminates in the endorsement and registration of candidates on the Register of Infosec Assessors as meeting the Program criteria and therefore being familiar with the specific requirements for carrying out security evaluation and assessment work within the scope of the program. The Register of Infosec Assessors is maintained in conjunction with the Program.

The Register of Infosec Assessors is used by Australian Government agencies (and others) as a means of sourcing assessors, with confidence that those assessors satisfy DSD's requirements to carry out the types of operations within the scope of the Program. The Register of Infosec Assessors will provide the I-RAP endorsed assessor's business contact details.

Assessors endorsed by the program will have tangible means of demonstrating to potential Australian Government agency clients (and others) that they are endorsed to assess ICT security systems in accordance with I-RAP policy.

There is a requirement for certain background checks to be performed as a result of the type of operations that an I-RAP assessed person will be expected to perform. Details are provided in the following sections.

### **4.3 I-RAP operations**

The I-RAP requires candidate assessors to successfully complete a number of discrete stages that culminate in qualification to be registered. They are:

1. Applications are invited and training dates announced on the I-RAP Register of Infosec Assessors and through various targeted marketing methods. Included with the invitation to apply is a closing date for applications.
2. Candidates apply for assessment to be registered as an I-RAP endorsed assessor in accordance with the Program. The application will require:
  - A criminal records check performed by the AFP or evidence of a current security clearance that required such a check,
  - A declaration that the applicant is an Australian Citizen, and
  - proof of the qualification prerequisites required to undertake the assessment for registration.
3. Applications are vetted to ensure that appropriate evidence of qualification prerequisites has been presented.
4. Candidates are contacted to either clarify application deficiencies or to be advised of qualification to undertake I-RAP training and assessment.
5. Candidates attend the I-RAP training session that includes instruction and assessment components.
6. The assessments are marked. Candidates are notified of the outcome of the assessment and review.
7. The I-RAP Administrator enters the candidates' business details on to the I-RAP register as endorsed assessors and issues certificates of competency to the candidates, valid for 12 months.

I-RAP registered assessors undertake update training and are reassessed every 12 months. This is done through a maintenance program that provides assurance that assessors have satisfactorily completed any mandatory training maintenance requirements throughout the 12 months of their registration. The performance of work within the scope of the Program carried out by assessors will also be subject to review at the time of re-registration.

## **5 Contact with the Infosec–Registered Assessors Program**

### **5.1 General**

The sub clause that follows in this Clause (5) specifies the I-RAP policy concerning contact with the I-RAP.

### **5.2 Contact Policy**

All contact with the I-RAP concerning the operation of the program shall be through the I-RAP Administrator. Where contact requirements change with respect to individual events (such as complaints or disputes) the person contacting the I-RAP shall be advised by the I-RAP Administrator.

I-RAP endorsed assessors requiring clarification of Australian Government ICT information security policy will be able to contact the DSD’s Client Services Team (Assist) directly – email [assist@dsd.gov.au](mailto:assist@dsd.gov.au).

Current contact details for both the I-RAP Administrator and the DSD I-RAP Manager shall be available on the Register of Infosec Assessors website at [www.irap.securelink.com.au](http://www.irap.securelink.com.au).

Applicants may contact the AFP directly when submitting Criminal Records documentation using the forms provided by the I-RAP Administrator.

Contact details required to comply with procedures contained in this document are contained within those procedures.

## **6 Fees**

### **6.1 General**

The sub clause that follows in this Clause (6) specifies the I-RAP policy concerning the levy of Program fees.

NOTE : The current schedule of fees is advised in Appendix A.

### **6.2 Fee policy**

The I-RAP shall levy fees to recover the cost of maintaining the Program. The fees shall be set by the DSD in consultation with the I-RAP Administrator.

Where a fee is levied for a particular aspect of the program, that fee is specified in the appropriate Clause.

Training and application fees are not refundable where training has been provided to a candidate.

## **7 Assessor endorsement**

### **7.1 General**

The sub clauses that follow in this Clause (7) specify the I-RAP policy concerning the qualifications required for candidates to receive and maintain I-RAP endorsement.

Appendix B specifies the assessor qualification procedure that includes procedures for application, training and assessment.

Appendix C identifies the documents required for undertaking the qualification training program and relevant reference Standards and other documents that provide the background knowledge required for qualification.

Appendix D specifies the procedures for maintaining I-RAP endorsement and registration.

NOTE : In order to carry out information security assessment work for Australian Government agencies, appropriate security clearances are required. Other than a Criminal Records check and declaration of Citizenship, the provision of security clearances is not a part of the I-RAP endorsement process and is considered a matter between assessors and the agencies engaging them.

Fees associated with a criminal records check will be met by DSD.

## **7.2 Pre-qualification**

### **7.2.1 Pre-qualification policy**

Candidates shall be subject to a pre-qualification requirement to be eligible to undertake I-RAP training and assessment. Candidates shall supply this pre qualification requirement as part of the application described in the application procedures contained in the assessor qualification procedure.

The purpose of this requirement is to demonstrate an adequate understanding of the ICT security systems being assessed at the technical level and ICT security system auditing practices. The provision of training about the technical aspects of ICT security systems and auditing principles is outside the scope of the Program.

Candidates shall also be subject to a criminal records check to be eligible to be “Registered” as an I-RAP assessor. The purpose of this requirement is to preserve the program’s integrity and reputation. Individuals may submit evidence of a current clearance that also meets this requirement.

### **7.2.2 Pre-qualification requirement**

The pre-qualification requirement shall be the provision of one of the following:

- a) Evidence of current “Certified Information Systems Auditor” (CISA) or “Certified Information Systems Manager” (CISM) certification and evidence of a minimum one (1) year experience gained within 3 years of the time of application of auditing ICT security systems, or
- b) Evidence of current “Certified Information System Security Professional” (CISSP) certification and evidence of a minimum one (1) year experience gained within 3 years of the time of application of auditing ICT security systems, or
- c) Evidence of appropriate academic qualifications relating to Information Technology, relevant to understanding ICT security systems and evidence of a minimum one (1) year experience gained within 3 years of the time of application of auditing ICT security systems, or
- d) Evidence of a minimum two (2) years experience, gained within 3 years of the time of application of auditing ICT security systems.

### **7.2.3 Academic qualifications**

The appropriate academic qualifications referenced in Clause 7.2.2 shall include:

- a) Australian Professional Engineering Programs (Degrees) or Engineering Technology Programs (Degrees) relating to ICT systems that are accredited by The Institution of Engineers, Australia, or overseas qualifications assessed as being equivalent by The Institution of Engineers, Australia, or
- b) Vocational Education and Training Diploma level programs relating to IT systems that are accredited by the Australian National Training Authority (ANTA).

### 7.3 I-RAP qualification for endorsement

Qualification for endorsement and registration in the Program shall include two (3) mandatory requirements:

1. Completing a training program presented by the I-RAP. In order to fully benefit from the training, candidates shall be required to familiarise themselves with the appropriate Standards and associated documents upon which the Program is based.
2. Passing an assessment test presented by the I-RAP at the end of the training session.
3. Having a clear criminal history check or evidence that a check of this nature has already been performed through an existing clearance procedure.

The assessment test will be presented in discrete sections. The pass requirement for each section shall be a score of 75% or greater and the pass criteria shall be met for all sections to qualify as a successful assessment.

In order to successfully complete the qualification for endorsement, candidates are required to be familiar with auditing techniques, risk assessment application and the relevant Standards and reference documents including the Australian Government Information Security Manual (ISM) that provide the background knowledge required for qualification. The I-RAP training program is not intended to provide in depth instruction in these topics. The training program will review them as they pertain to work within the scope of the program.

The structure of the training program and the assessment test is specified in the training and assessment procedures contained in the assessor qualification procedure.

### 7.4 Endorsement maintenance

I-RAP registered assessors shall be required to undertake an I-RAP re-assessment to remain endorsed and registered in accordance with the Program. This re-assessment shall be carried out at the discretion of the I-RAP as close as possible to being at 12-month intervals referenced from the date of initial assessment.

NOTE : The reassessments will be aligned with scheduled application assessments which are intended to be carried out at regular intervals, however the actual periods between each may vary dependent on venue availability etc.

Re-assessment to remain endorsed and registered shall include three (3) mandatory requirements:

1. Completing update training presented by the I-RAP that will highlight any pertinent changes that have occurred since the initial training.
2. Review by the I-RAP administration in conjunction with the DSD of the complaints and disputes records and any reviews of the assessor's work undertaken by the DSD during the period since the last assessment.
3. Passing an assessment test presented by the I-RAP at the end of the training session.

The pass requirement for the assessment test shall be a score of 75% or greater and a satisfactory review of mandatory Item 2.

The I-RAP incorporates the capacity to waive the application of the assessment test as part of a re-assessment session where it deems appropriate to do so. Where this occurs the requirement from that particular session, to remain endorsed, shall be completing Item 1 and a satisfactory result from Item 2 of the mandatory requirements. I-RAP registered assessors shall be notified whether

an assessment test will be included in the re-assessment when advised that the re-assessment is due.

I-RAP registered assessors shall be advised when re-assessment is scheduled as specified in the training and assessment procedures contained in the registration renewal procedure. Where the scheduled re-assessment is inconvenient to the I-RAP registered assessor, alternative arrangements shall be made by the I-RAP registered assessor to attend the next scheduled session. To maintain registration, I-RAP registered assessors will be required to undertake I-RAP re-assessment within 3 months of the anniversary date of endorsement at the next I-RAP scheduled re-assessment venue. During the period between the expiry of the registration and assessment of the results of the re-assessment (30 days), the status of the assessor's registration shall be specified: "registration renewal is pending".

### **7.5 Certificate of endorsement**

Candidates qualifying for endorsement shall receive a certificate specifying endorsement by the I-RAP. The certificate shall be valid as long as the I-RAP assessor's status is current on the I-RAP web site referred to on the DSD web site ([www.dsd.gov.au](http://www.dsd.gov.au)).

The contents of the certificate shall include:

1. I-RAP identification
2. Identification of the endorsed assessor by name.
3. A statement of endorsement.
4. Scope of expertise
5. The signature of the appropriate Defence Signals Directorate representative.

### **7.6 Endorsement fees**

The following Fee structure applies:

1. Application assessment in accordance with the Program,
2. Training and Assessment,
3. Maintenance Training and Assessment.

Should the candidate accept and undertake training yet fail to meet the requirements of the criminal records check, the application and training fee will not be reimbursed.

If the candidate does not qualify for registration as an I-RAP endorsed assessor after completing the qualification training and assessment session and undertakes to repeat the qualification training and assessment within 6 months from the initial session attended, only the qualification training and assessment fee shall apply for the second attempt.

## **8 Assessor registration**

### **8.1 General**

The sub clauses that follow in this Clause (8) specify the I-RAP policy concerning the registration of candidates acquiring I-RAP endorsement.

A candidate will not be registered until results of the criminal history check (or evidence of a current clearance which requires the same) can be verified.

### **8.2 Publication of registration**

The I-RAP shall publish the contact and endorsement details of Candidates on the Register of Infosec Assessors.

### **8.3 Registered information**

The following candidate information shall be published:

1. Name.
2. Business contact details.
3. Date of registration and subsequent re-registrations (endorsements).
4. A brief resume limited to 750 characters (including spaces) supplied by the candidate, where applicable.

### **8.4 Registration period**

The period of registration shall be 12 months from the date of endorsement.

### **8.5 Registration fee**

A subscription fee shall apply for registration and registration renewals.

Failure to comply with the terms of payment specified on the invoices issued for subscription fees shall be considered failure to comply with Item 3 of Clause 12.2 and endorsement will be withdrawn as specified in Clause 12.3.

## **9 Assessor obligations**

### **9.1 General**

The sub clauses that follow in this Clause (9) specify the I-RAP policy concerning the obligations of candidates intending to gain and maintain I-RAP endorsement.

### **9.2 Assessor obligations**

Candidates and I-RAP registered assessors shall comply with the Rules of the Program as specified in the Policy and Procedures for the Infosec–Registered Assessor Program (I-RAP) including the following obligations:

1. To participate in the application and qualification processes specified in the Policy and Procedures for the Infosec–Registered Assessor Program (I-RAP) and abide by the qualification assessment decision of the I-RAP (except where a dispute regarding the assessment arises).
2. To participate in the re-assessment process each 12 months where the candidate wishes to remain endorsed by the I-RAP and abide by the qualification re-assessment decision of the I-RAP (except where a dispute regarding the assessment arises).
3. To grant permission to the I-RAP to publish professional details of the candidate as specified in the Policy and Procedures for the Infosec–Registered Assessor Program (I-RAP).
4. To notify the I-RAP administration of any change to the information provided with the application that occurs during the term of registration (e.g. address change, change of employment contact details etc.) within 14 days of the change occurring.
5. To comply with the conduct requirements of the Infosec–Registered Assessor Program (I-RAP) while undertaking assignments within the scope of the Program.
6. To abide by any dispute resolution rulings negotiated and agreed with the DSD via the I-RAP Administrator, DSD I-RAP Manager or arbitrated by the Assistant Secretary of the Information Security Group - DSD.

### **9.3 Declaration**

Candidates shall provide a formal declaration of understanding and agreement to the obligations specified in the Policy and Procedures for the Infosec–Registered Assessor Program (I-RAP). The declaration (which includes a declaration of citizenship) shall be included as a part of the I-RAP Application Form submitted by the applicant as a part of the application procedures contained in the assessor qualification procedure.

## **10 Conduct of Registered Assessors**

### **10.1 General**

The sub clause that follows in this Clause (10) specifies the I-RAP policy concerning the conduct of I-RAP registered assessors while undertaking assignments within the scope of the Program.

Appendix E specifies the rules for I-RAP compliance that must be adhered to, as an I-RAP registered assessor, when undertaking Gateway/CDS Assessment, Network/System Assessments, Gatekeeper Assessments and FedLink Audits.

### **10.2 Conduct Requirements**

When undertaking assignments within the scope of the Program, I-RAP registered assessors shall comply with the Rules of the Program as specified in the Policy and Procedures for the Infosec–Registered Assessor Program (I-RAP), including the following requirements:

1. I-RAP registered assessors conducting work within the scope of the Program shall ensure they use the most recent versions of Australian Government policy and relevant documentation. Assessors can download the latest versions of DSD's documentation from: <http://www.dsd.gov.au/Infosec/>.
2. I-RAP registered assessors entering into work within the scope of the Program for the Australian Government shall report according to the requirements of the Program. This will ensure a reporting standard is maintained for the purpose of consistency and comparison.
3. I-RAP registered assessors shall not represent themselves as an employee or agent of DSD or the Australian Government when conducting work within the scope of the Program.
4. I-RAP registered assessors who access, handle and/or store Australian Government classified information are required to comply with the requirements of the Protective Security Manual. It is the responsibility of the client to ensure that these measures are in place
5. I-RAP registered assessors are required to report the results of an assessment carried out to DSD's and the Australian Government's policy standards for a Australian Government agency to the DSD I-RAP Manager.

I-RAP Registered assessors may undertake work other than Australian Government IT system security assessment work within the scope of the Program.

I-RAP Registered assessors may advertise the fact that they are I-RAP registered.

## **11 Review of work conducted by Registered Assessors**

### **11.1 General**

The sub clause that follows in this Clause (11) specifies the I-RAP policy concerning the review of work within the scope of the Program carried out by I-RAP registered assessors.

### **11.2 Initiation of review**

The DSD, whenever it deems appropriate, may conduct a review of work carried out by I-RAP registered assessors that is within the scope of the Program.

Australian Government agencies may request that DSD review reports produced by I-RAP assessors. The DSD is not required to meet these requests and may choose to do so on a case-by-case basis.

## **12 Withdrawal of endorsement**

### **12.1 General**

The sub clauses that follow in this Clause (12) specify the I-RAP policy concerning the withdrawal of I-RAP endorsement.

Appendix F specifies the procedures for withdrawal of endorsement and I-RAP registration.

### **12.2 Grounds for withdrawal**

The I-RAP incorporates the capacity for withdrawal of endorsement and registration of an I-RAP registered assessor in the following circumstances:

1. Withdrawal from the program by the I-RAP registered assessor.
2. Failure to meet the requirements of the annual re-assessment.
3. Failure to meet any of the assessor obligations specified in the Policy and Procedures for the Infosec–Registered Assessor Program (I-RAP).
4. An unsatisfactory review of the I-RAP registered assessor's work within the scope of the Program carried out by the DSD I-RAP Manager, either independently or for the Australian Government.
5. Where a conflict of interest arises and cannot be satisfactorily resolved.
6. Misrepresentation or concealment of the facts by the I-RAP endorsed assessor.
7. Where a complaint is received concerning the assessor's qualifications and cannot be satisfactorily resolved.
8. Where I-RAP registered assessors represent themselves as an employee or agent of DSD or the Australian Government when conducting work within the scope of the Program.
9. Where I-RAP registered assessors who access, handle and/or store Australian Government classified information fail to comply with the requirements of the Protective Security Manual and the client has met their responsibility to ensure that these measures are in place.

The DSD I-RAP Manager shall resolve withdrawal of endorsement issues arising from items 3 to 9 of this Clause 12.2. Where the decision of the DSD I-RAP Manager is challenged, the

Assistant Secretary of the Information Security Group - DSD shall be the final arbiter for withdrawal of endorsement issues arising from items 3 to 9 of this Clause 12.2.

### **12.3 Notice of withdrawal**

Where an approval is withdrawn the I-RAP Administrator shall advise the assessor of the reasons for withdrawal and what action is required for reinstatement.

Details of all endorsements that are withdrawn in accordance with items 3 to 9 of Clause 12.2 shall be noted on the register for 12 months after the date of withdrawal, unless the approval is reinstated.

### **12.4 Fee considerations with respect to withdrawal of I-RAP registration**

Where I-RAP registration is withdrawn, any I-RAP application, training or registration fees incurred by the assessor will not be refunded except in the circumstance of item 1 in Clause 12.2 occurring during the registration renewal period. In that circumstance, fees will be assessed in accordance with the registration renewal procedure in Clause D 4.

## **13 Conflict of interest**

### **13.1 General**

The sub clauses that follow in this Clause (13) specify the I-RAP policy concerning conflicts of interest with activities within the scope of I-RAP endorsement.

### **13.2 Assessor conflict of interest obligations**

I-RAP registered assessors should avoid undertaking assessments where a conflict of interest arises. The assessor shall advise the I-RAP Administrator if any conflict of interest with the Program is perceived and seek the guidance of the I-RAP concerning its potential impact on I-RAP endorsement.

### **13.3 Potential conflict of interest**

A Certificate of Compliance should be the result of an independent assessment of an IT system's security compliance with Australian Government policy by an I-RAP registered assessor not having been involved with the development or implementation of the IT system's security plan and associated documentation.

The following demonstrate examples of potential conflict of interest situations:

- Where agencies/organisations contract an I-RAP registered assessor to prepare the IT system security plan and associated documentation for their IT system and then contract the same I-RAP registered assessor to certify that IT system security plan and associated documentation.
- Where organisation X with I-RAP registered assessors on staff and organisation Y with I-RAP registered assessors on staff are involved with the preparation of the IT system security plan and associated documentation of a joint agency /organisation IT system and organisation X contracts an I-RAP registered assessor on organisation Y's staff to certify that joint system, or vice versa
- Where organisations with I-RAP registered assessors on staff use those assessors to certify their own Organisation IT systems.

DSD will consider whether the Certificate of Compliance should be revoked. Agencies are encouraged to use independent I-RAP assessors if the intention of the assessment is to achieve Certification.

### **13.4 Potential conflict of interest penalties**

Where a conflict of interest with respect to the manner that the registered assessor has executed an assignment is deemed by either the I-RAP or the DSD to have occurred, the I-RAP incorporates the capacity for withdrawal of endorsement and registration of an I-RAP registered assessor.

Where a conflict of interest with respect to the employment of the registered assessor with respect to a certification carried out by that assessor is deemed by the DSD to have occurred, the DSD retains the right to consider whether that Certification should be revoked.

## **14 Complaints and disputes**

### **14.1 General**

The sub clauses that follow in this Clause (14) specify the I-RAP policy concerning the handling of complaints and disputes.

Appendix G specifies the complaints and dispute resolution procedures.

### **14.2 Scope of complaints and disputes**

The resolution of complaints and disputes shall be confined to complaints about the Program or disputes arising from the operation of the Program. Complaints or disputes arising from general competency or commercial arrangements between assessors and their clients are outside the scope of this Program. The DSD, either directly or through the I-RAP, will not become involved in matters of contract or payment dispute between Australian Government agencies and I-RAP registered assessors.

It is anticipated that complaints will originate from users of the Program having concerns about the operation of the program or third parties having used the services of I-RAP registered assessors and considering them to be unsuitable for I-RAP endorsement.

Disputes will originate from candidates disputing application or assessment results provided by the I-RAP or the operation of the Program.

### **14.3 Handling and recording**

The I-RAP Administrator shall manage the process for assessing complaints and resolving disputes. A Complaints and Disputes Log shall be established for recording the pertinent details of complaint handling and dispute resolution. The structure of the log is specified in the Complaints and Dispute procedures.

### **14.4 Acknowledgement and responsiveness**

#### ***14.4.1 Complaints***

All complaints from customers and stakeholders shall be handled expeditiously and courteously and any failure in operational processes that has resulted in that complaint will be amended to ensure that similar complaints do not recur.

All complaints from customers and stakeholders must be in writing, with supporting evidence.

The I-RAP Administrator shall acknowledge all complaints within 10 working days of receipt and enter the complaint in the Complaints and Disputes Log.

As far as possible, the time frame for resolving the complaint shall be agreed with the complainant. This time frame shall be recorded in the Complaints and Disputes Log.

Where the complaint is about the activities of a particular I-RAP endorsed assessor, the assessor against whom the complaint has been made shall be advised in writing of the allegations and requested to submit a response.

If the complaint is taking longer to resolve than agreed, the I-RAP Administrator shall advise the complainant and the advice shall be recorded in the Complaints and Disputes Log.

Wherever possible, remedial actions resulting from complaint resolution shall be assessed by the I-RAP Administrator in conjunction with the DSD I-RAP Manager.

When a response to the complaint has been formulated, the I-RAP Administrator shall advise the complainant in a timely manner and enter details of how the complaint was resolved in the Complaints and Disputes Log.

Where the complaint is about the activities of a particular I-RAP endorsed assessor and has been substantiated the DSD I-RAP Manager shall determine an appropriate level of action.

Where a complainant or an I-RAP endorsed assessor (where the I-RAP endorsed assessor is the subject of the complaint), is dissatisfied with the resolution of a complaint, an appeal will be referred to the Assistant Secretary of the Information Security Group – DSD, who shall arbitrate a resolution.

Following an appeal, the decision of the Assistant Secretary of the Information Security Group – DSD shall be final.

#### ***14.4.2 Disputes***

All disputes arising from the operation of the program shall be handled expeditiously and courteously and any failure in operational processes that has resulted in that dispute will be amended to ensure that similar disputes do not recur.

All disputes shall be lodged in writing within one (1) month from the action that the dispute addresses.

When notified of the dispute, the I-RAP Administrator shall record the dispute in the Complaints and Disputes Log.

The means of resolving operational disputes shall be by discussion between the I-RAP Administrator, the DSD I-RAP Manager and the person lodging the dispute. A decision to resolve the dispute shall then be drafted by the I-RAP Administrator.

The I-RAP Administrator shall respond to the person lodging the dispute with the decision as soon as possible after the last discussion between the I-RAP Administrator, the DSD I-RAP Manager and the person lodging the dispute. The I-RAP Administrator shall record the decision and provision of advice in the Complaints and Disputes Log.

The DSD I-RAP Manager shall arbitrate disputes appealing I-RAP decisions about application or assessment results. Notification and the logging of the result shall be in the same manner as for an operational dispute.

Where the person lodging the dispute is dissatisfied with the resolution of the dispute, the matter will be referred to the Assistant Secretary of the Information Security Group – DSD, who shall arbitrate a resolution.

Following an appeal, the decision of the Assistant Secretary of the Information Security Group – DSD shall be final.

Failure of the person lodging the dispute to pursue the dispute with the I-RAP Administrator within 10 working days shall be interpreted as an end to the dispute.

## **15 Publicity and documentation**

### **15.1 General**

The sub clauses that follow in this Clause (15) specify the I-RAP policy concerning publicity and documentation associated with the Infosec–Registered Assessors Program.

Appendix E specifies the rules for I-RAP compliance that must be adhered to when undertaking advertising and promotion of I-RAP Registration.

### **15.2 Advertising and promotion**

The I-RAP undertakes that advertising and promotion of the Program shall be clear, truthful and accurate in content and should not be likely to mislead the customer, either by intent or otherwise.

Registered Assessor's and their employer's advertising and promotion of their involvement in the Program shall be clear, truthful and accurate in content and should not be likely to mislead the customer, either by intent or otherwise; I-RAP Endorsement and Registration is restricted to individuals. I-RAP registered assessors may advertise the fact that they are I-RAP registered. Employers of I-RAP registered assessors must not advertise that their organisation is I-RAP registered. Organisations may advertise that they have I-RAP registered assessors on staff.

Registered Assessors and their employers may, subject to terms and conditions, use the I-RAP Logo in their promotional material. The means of obtaining the terms and conditions for use of the I-RAP Logo and the Logo itself are contained in the advertising and promotion procedure.

### **15.3 Documentation**

All I-RAP policy and associated documentation, including information on how customers' complaints are to be addressed and with copies of the complaints handling procedure, shall be available on request.

### **15.4 Administrative reporting**

The I-RAP Administrator shall report to the Program sponsor (DSD) in the following manner:

1. Statistical reports on a quarterly basis. The statistical reports shall include the following information for the previous quarter:
  - a) The number of candidates applying for registration,
  - b) The names and details of all candidates registered,
  - c) The names and details of all registered assessors who are re-registered,
  - d) Number of training courses provided, and
  - e) Such other statistical details pertaining to the Program as are reasonably required by DSD.
2. Complaints and dispute reports on a quarterly basis. The complaints and dispute reports shall include the following information:
  - a) A breakdown of all complaints received by the I-RAP Administrator in connection with the Program,
  - b) A breakdown of all disputes received by the I-RAP Administrator in connection with the Program.

## **15.5 Register of Infosec Assessors**

The I-RAP shall establish and maintain a web based Register of Infosec Assessors containing information about the Program, documentation required for participating in the program, including the Program's Policy and Procedures, contact details for the I-RAP Administrator and a list of all assessors endorsed by the I-RAP.

**NOTE : Privacy Statement**

Information provided by applicants for the purpose of registration or re-registration under the I-RAP will only be used by SecureLink Pty Ltd and the Defence Signals Directorate for that purpose. The information provided by an applicant will not be disclosed to a third party without the consent of the applicant, unless that information is required to be disclosed by law, portfolio or statutory obligations.

## Appendix A Schedule of fees (Informative)

### A.1 General

This informative appendix advises the current schedule of fees that apply to the I-RAP at the time this document was published.

### A.2 Schedule of fees

The schedule of fees for undertaking and maintaining qualification and registration in the Program are contained in Table 1. They are indicative only and were accurate at the time of publication. Current fees are contained on the Register of Infosec Assessors website.

These fees may be varied at the discretion of the DSD.

**Table 1. — Schedule of fees**

<b>Activity</b>	<b>Fee</b>
Application	\$275.00
Qualification training and assessment	\$3,300.00
Maintenance training and assessment	\$1,650.00
Registration	\$2,200.00

NOTES:

1. The fees indicated in Table 1 include GST.
2. The details of payment methods and when payment is due are specified in the appropriate procedures contained in the following Appendices.

## Appendix B Assessor qualification procedure (Normative)

### B.1 General

This normative appendix specifies the procedures for assessor qualification.

### B.2 Initial contact

Initial contact by interested parties wishing information about the I-RAP will be made through the Infosec Registered Assessor Program Administrator. Contact Details are as follows:

<b>I-RAP Administrator:</b>	David Jarvis
<b>Telephone:</b>	(02) 6292 7350
<b>Facsimile:</b>	(02) 6292 7355
<b>Email:</b>	<a href="mailto:irap@securelink.com.au">irap@securelink.com.au</a>

The contact details for the I-RAP Administrator are also published on the I-RAP website at [www.irap.securelink.com.au](http://www.irap.securelink.com.au)

Initial contact concerning invitations to submit applications and advice about scheduled training and assessment will be initiated by the I-RAP administration. Potential candidates will be invited through targeted marketing and publication of application/training details on the I-RAP website.

### B.3 The Application

#### B.3.1 *Announcement of intake*

An invitation to submit Applications will be announced by the I-RAP administration periodically to align with the training and assessment schedule.

#### B.3.2 *Contents of the Application*

##### B.3.2.1 *Application contents*

A complete application must be submitted to meet the requirements for pre-qualification.

A complete application shall include all of the following:

- a) A complete application form,
- b) Evidence of pre-qualification criteria as described in Clause 7 of this Policy e.g. details of two (2) years relevant IT experience or appropriate academic qualifications and evidence of a minimum 1 year relevant IT experience,
- c) Two (2) photos suitable for use in Australian passports,

NOTE : The photos will be matched against the proof of personal identification and used for verification at assessments.

- d) Evidence of a current security which requires a criminal history check as detailed in B.3.3
- e) Evidence of personal identification equalling 100 EOI points (see Table 2), and
- f) The scheduled application fee and qualification, training and assessment fee.

### *B.3.2.2 The Application Form*

The application form will include the following information:

- a) Applicant details
- b) Employer/Business details
- c) Application contents details
- d) A brief CV for publication on the Register of Infosec Assessors upon qualification for endorsement and registration
- e) Payment details
- f) A Declaration of the following:
  - ◆ The contents of the application and accompanying documentation are true and correct,
  - ◆ Agreement to abide by the terms and conditions of the Infosec–Registered Assessor Program Policy and Procedures,
  - ◆ Consent for the I-RAP Administration to carry out verification of pre-qualification material as considered necessary,
  - ◆ Declaration that the candidate is an Australian Citizen, and
  - ◆ Consent to post Assessor contact details on the Register of Infosec Assessors

### *B.3.2.3 Required detail for pre-qualification criteria*

Where the applicant intends submitting relevant qualifications as their pre-qualification criteria, details of that criterion must include a copy of the degree or diploma issued following successful completion of an appropriate course as specified in Clause 7 of this Policy.

Submission of relevant IT experience must include all of the following details:

- a) Company name, address and phone number,
- b) Synopsis of the applicant’s duties,
- c) Employer contact name for verification, and
- d) Contact details for the named contact.

The I-RAP administration will carry out confirmation assessment of the information provided as considered necessary.

### *B.3.2.4 Required detail for identification*

The documents submitted to meet the identification requirements can include any combination of documents from Table 2. At least one of the documents chosen must contain a photograph that can be matched to the person named.

**Table 2. — Identification documents**

<b>Documentation</b>	<b>EOI Points</b>
Birth Certificate	70
Citizenship Certificate	70
Current Passport	70
Expired Passport (not cancelled and not expired for longer than 2 years from date of expiry)	70
Current Australian Drivers Licence	40
Identification Card issued to a Australian Government or State/Territory Government employee, contractor or other personnel	40
Document provided by current employer on employer letterhead and dated within the last 3 months prior to the application	35
If self employed, relevant documentation from the applicant's Registered Tax Agent/Accountant	35
Credit card tax invoice (two or more credit card tax invoices from the same financial institution will be counted as one)	25
Council rates notice	25
Record of a public utility (e.g. utilities accounts – telephone, gas, electricity, ISP provider)	25

Photocopies of the documentation will be accepted providing the information and photo on the ID are legible enough for comparison to the submitted photos. Acceptance of the photocopies is at the discretion of the I-RAP administration.

### ***B.3.3 Criminal History Check***

Applicants are to complete and submit a criminal records check to the AFP. Forms will be e-mailed to the applicant as part of the response to an application. The forms and any supporting material is to be sent directly to the AFP. DSD will be the recipient of the results.

Applicants already holding a relevant security clearance are not required to undergo a criminal history check. Applicants should provide evidence of their current security level and submit it with their application to the I-RAP Administrator for consideration.

### ***B.3.4 Application fee***

Payment of the scheduled application fee (plus the Qualification training and assessment fee – see Clause B.5.1.1) must accompany the application.

Payment of these fees may be by money order or cheque payable to SecureLink Pty Ltd or by electronic funds transfer. Indication of the method of payment and/or required credit card details will be included on the application form.

Where the candidate fails to meet the pre-qualification criteria of the program, the qualification, training and assessment fee will be refunded. Application fees will not be refunded.

Applicants still awaiting AFP Criminal History Check results at the time of training will be able to attend training and sit for the assessment. If this option is undertaken however and the applicant fails to meet the requirements of the AFP Criminal History check the I-RAP Administrator will not endorse the applicant as an assessor nor refund the training and assessment or application fees. Failure to meet the requirements of the criminal history check includes convictions relating to violence, fraud, theft, drug use/trafficking and frequent repeated traffic offences.

### ***B.3.5 Lodgement of the application***

Invitations to lodge applications will include an application closing date approximately 6 weeks prior to the scheduled qualification training and assessment. This is done to allow adequate time for the I-RAP Administrator to assess the pre-qualification criteria.

Applications must be lodged so that the I-RAP administration receives them either by close of business on the closing date or so that the application is postmarked or couriered on or before the closing date. Applications received after the closing date may not be accepted for the next scheduled training and assessment at the discretion of the I-RAP administration.

Applications should be lodged with the I-RAP Administrator at the following address

#### ***Postal Address***

Infosec–Registered Assessor Program Administrator  
C/o SecureLink Pty Ltd  
PO Box 208 Erindale Centre  
Canberra ACT 2903

### ***B.3.6 Application verification***

Once the application is verified to be complete and accompanying pre-qualification conditions confirmed, the I-RAP Administrator will contact the applicant with advice of their candidacy and confirm the training details.

Where the application is incomplete or pre-qualification conditions have not been met, the I-RAP administration will liaise with the applicant to complete the application. Where the application cannot be completed or pre – qualification cannot be met to the satisfaction of the I-RAP administration, the applicant will be notified and the training fee refunded.

Applicants wishing to dispute the decision of the I-RAP administration shall follow the dispute procedures contained in Appendix G of this Policy.

## **B.4 Training and assessment**

### ***B.4.1 Confirmation of training***

Once the application is verified to be complete and accompanying pre-qualification conditions confirmed, in addition to advice of their candidacy, the I-RAP Administrator will supply the applicant with confirmation details of the time, date, venue and identity of the I-RAP trainer for the next training and assessment session and will supply the training course materials required for

that session (see Appendix C for guidance to acquiring the assessment guides required for training).

## ***B.4.2 Training***

### ***B.4.2.1 Registration and identification***

Candidates attending the training session will be required to register and have their identity verified against the photos supplied with their application at the start of each session day. The I-RAP trainer will carry out this verification. In addition, the I-RAP trainer will verify the identity of the candidates each time they enter the training venue during the course of a session. Where the identity of the attendee cannot be verified, the attendee will not be admitted to that training session.

### ***B.4.2.2 Period of training***

The combined training and assessment sessions will take place over a period of 2 days with the training component taking 1.5 days. Candidates will be expected to arrive at least 15 minutes before the scheduled session start time to allow registration and identification.

### ***B.4.2.3 Training coverage***

Training coverage will include the following topics:

- ◆ A review of the ISM
- ◆ A review of risk assessment pertaining to information security
- ◆ Application of Australian Government policy
- ◆ Audit practices
- ◆ Infosec–Registered Assessor Program protocols
- ◆ Outline of work processes required for work within the scope of the I-RAP

#### NOTES:

1. Training course materials will be provided with confirmation of a successful application (see Clause B4.1).
2. The I-RAP training program is not intended to provide in depth instruction for auditing techniques, risk assessment application or detailed review of any of the reference documents including the ISM. The training program will reference them as they pertain to work within the scope of the program. Candidates are expected to understand the concepts and requirements of the reference documents prior to undertaking the I-RAP training.

## ***B.4.3 Assessment test***

### ***B.4.3.1 Period of assessment test***

The assessment test component will take place on the last half day of the training and assessment session. The test will be approximately three (3) hrs in duration.

#### *B.4.3.2 Assessment test structure*

The structure of the assessment test will be a combination of multiple-choice questions and short paragraph responses. Approximately 80 to 90% of the test will assess the candidate's knowledge of the tasks associated with the Australian Government work that assessors may undertake and approximately 10% will assess background knowledge components. The remainder of the test will assess the remaining topics of the training program.

#### *B.4.3.3 Assessment of results*

The test will be presented and presided over by the trainer. The test results will be collected by the trainer and returned to the I-RAP administration. The tests will be assessed by the I-RAP administration.

#### *B.4.3.4 Notification of results*

Upon completion of assessment of the test, the I-RAP administration will notify the candidate of the results within 30 working days. Where the candidate has met the qualification criteria, the I-RAP administration will issue a certificate of achievement, register the candidate's business details on the Register of Infosec Assessors and issue an invoice for the scheduled registration fee.

Where the candidate does not meet the qualification criteria, the candidate will be notified by letter.

Candidates wishing to dispute the decision of the I-RAP administration shall follow the dispute procedures contained in Appendix G of this Policy.

### **B.5 Qualification fees**

#### *B.5.1.1 Qualification training and assessment fee*

Payment of the scheduled qualification training and assessment fee must accompany the application.

Payment of these fees may be by money order or cheque payable to SecureLink Pty Ltd or by electronic funds transfer. Indication of the method of payment and/or required details will be included on the application form.

The qualification training and assessment fee will be refunded only where the applicant's application is not successful or where the applicant voluntarily withdraws from the qualification program and notifies the I-RAP Administrator seven (7) days or more before commencement of the scheduled training session. Inability to attend for other reasons will be considered by the I-RAP administration and subsequent action agreed between the I-RAP administration and the candidate e.g. attending the next scheduled session.

#### *B.5.1.2 Registration fee*

The I-RAP administration will issue an invoice for the scheduled registration fee when the candidate successfully completes the qualification criteria of the Program (at the time of notification). Failure to comply with the terms of payment specified on the invoice shall be considered failure to comply with Item 3 of Clause 12.2 and endorsement will be withdrawn as specified in Clause 12.3.

## Appendix C Assessment guides/reference documents (Normative)

### C.1 General

This normative appendix provides details of the I-RAP assessment guides that will be used in I-RAP training and reference documents that contain the concepts that candidates need to understand prior to undertaking the I-RAP training.

### C.2 I-RAP assessment guides

The details of the I-RAP assessment guides that will be used in I-RAP training and candidates must acquire to reference when undertaking the I-RAP training are described in Table 3.

**Table 3. — I-RAP assessment guides**

Document Title	Source
I-RAP Gateway/CDS Assessment & PROTECTED Level FedLink Connection Guidelines & Checklist	Available free of charge from <a href="http://www.dsd.gov.au/">http://www.dsd.gov.au/</a> and select the I-RAP link
I-RAP System Review Guidelines & Checklist	
I-RAP FedLink Audit Guidelines & Checklist	
I-RAP Gatekeeper Guidelines & Checklist	

### C.3 Reference documents

The details of the reference documents that contain the concepts that candidates need to understand prior to undertaking the I-RAP training are described in Table 4. Candidates are expected to maintain their knowledge of the latest versions of the reference documents.

**Table 4. — Reference documents**

<b>Document Number</b>	<b>Title</b>	<b>Abstract</b>	<b>Source</b>
ISM	Australian Government Information Security Manual	The ISM is intended to provide guidance to all Australian Government Departments, organisations and personnel in the task of protecting classified or unclassified computer information and equipment. Specifically, it describes the steps to be taken to plan and implement the computer security measures required by the Protective Security Manual	Available free of charge from <a href="http://www.dsd.gov.au/library/index.html">http://www.dsd.gov.au/library/index.html</a> and scroll to “Infosec policy”.
ISO 27001	Information security management - Specification for information security management systems	Specifies the requirements for establishing, implementing and documenting information security management systems (ISMSs) and the requirements for security controls to be implemented according to the needs of individual organizations.	Available for purchase from SAI Global Business Publishing. For details see <a href="http://www.standards.com.au">http://www.standards.com.au</a> and use the web shop tool (enter the Standard number only)
AS/NZS ISO/IEC 17799	Information technology - Code of practice for information security management	Provides recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization.	Available for purchase from SAI Global Business Publishing. For details see <a href="http://www.standards.com.au">http://www.standards.com.au</a> and use the web shop tool (enter the Standard number only)
AS/NZS/ISO 31000:2009	Risk management	Provides a generic guide for establishing and implementing the risk management process, which involves establishing context, identification, analysis, evaluation, treatment, monitoring and review and consultation and communication. This Standard may be applied at every stage in the life of an activity, function, project or asset generated by any public, private or community enterprise or group.	Available for purchase from SAI Global Business Publishing. For details see <a href="http://www.standards.com.au">http://www.standards.com.au</a> and use the web shop tool (enter the Standard number only)
HB 231	Information security risk management guidelines	Provides a generic guide for the establishment and implementation of a risk management process for information security risks.	Available for purchase from SAI Global Business Publishing. For details see <a href="http://www.standards.com.au">http://www.standards.com.au</a> and use the web shop tool (enter the Standard number only)

## **Appendix D Registration renewal procedure (Normative)**

### **D.1 General**

This normative appendix specifies the procedures for assessor qualification confirmation and registration renewal being carried out.

### **D.2 Refresher training**

#### *D.2.1 Confirmation of training*

The I-RAP Administrator will supply the I-RAP registered assessor with advice that re-assessment is due and the details of the time, date, venue and identity of the I-RAP trainer for the next re-assessment session. This advice will be provided approximately two (2) months prior to the next scheduled re-assessment session to allow adequate warning to the assessor. Once the attendance of the assessor is verified, the I-RAP administration will supply the training materials required for that session.

#### *D.2.2 Training*

##### *D.2.2.1 Registration and identification*

Candidates attending the re-assessment session will be required to register and have their identity verified against the photos supplied with their application at the start of the session. The I-RAP trainer will carry out this verification. In addition, the I-RAP trainer will verify the identity of the candidates each time they enter the training venue during the course of a session. Where the identity of the attendee cannot be verified, the attendee will not be admitted to that training session.

##### *D.2.2.2 Period of training*

The combined training and assessment sessions will take place over a period of one (1) day with the training component taking the majority of the day. Candidates will be expected to arrive at least 15 minutes before the scheduled session start time to allow registration and identification.

##### *D.2.2.3 Training coverage*

Training coverage will include any changes that have occurred to the following topics since the last assessment attended by the assessor:

- ◆ The ISM
- ◆ Risk assessment pertaining to information security
- ◆ Application of Australian Government policy
- ◆ Audit practices including any new I-RAP services that may be offered between registration and re-registration periods
- ◆ Infosec–Registered Assessor Program protocols
- ◆ Work processes required for work within the scope of the I-RAP

### ***D.2.3 Assessment test***

#### *D.2.3.1 Period of assessment test*

The assessment test component, if it has not been waived (see Clause 7.4), will take place as the final part of the training and assessment session. The duration of the test will depend on the session contents.

#### *D.2.3.2 Assessment test structure*

The test will consist of a combination of multiple-choice questions and short paragraph responses as deemed necessary. The test will assess the candidate's knowledge of the content of the training program.

#### *D.2.3.3 Assessment of results*

The test will be presented and presided over by the trainer. The test results will be collected by the trainer and returned to the I-RAP administration. The tests will be assessed by the I-RAP administration.

#### *D.2.3.4 Notification of results*

Upon completion of assessment of the assessment test, the I-RAP administration will notify the candidate of the results within 30 working days.

Where the candidate has met the re-assessment criteria of the Program, the I-RAP administration will update assessor status as being current to the next qualifying period and issue an invoice for the scheduled registration fee.

Where the candidate does not meet the qualification criteria, the candidate will be notified by letter.

Candidates wishing to dispute the decision of the I-RAP administration shall follow the dispute procedures contained in Appendix G of this Policy.

### **D.3 Registration update**

Where the candidate has met the re-assessment criteria of the Program, the I-RAP administration will update the candidate's business details and registration status on the Register of Infosec Assessors.

During the period between the expiry of the registration and assessment of the results of the re-assessment (30 days), the status of the assessor's registration will be specified "registration renewal is pending".

Where the candidate has not met the re-assessment criteria of the Program, the candidate will be offered the opportunity of re-doing the qualification training and assessment at the next scheduled qualification training and assessment (normally within three (3) months) at the normal qualification training and assessment fee.

#### **D.4 Renewal fees**

The renewal fees include the scheduled maintenance training and assessment fee and the scheduled registration fee.

The I-RAP administration will issue an invoice for the renewal fees when the candidate confirms their attendance for the refresher training.

The renewal fees will be refunded only where the candidate voluntarily withdraws from the re-assessment program and notifies the I-RAP Administrator seven (7) days or more before commencement of the scheduled training session. Inability to attend for other reasons will be considered by the I-RAP administration and subsequent action agreed between the I-RAP administration and the candidate e.g. attending the next scheduled session.

Where the candidate has completed the refresher training and does not meet the qualification criteria, the scheduled registration fee only will be refunded.

Where the candidate has completed the refresher training and meets the qualification criteria, failure to comply with the terms of payment specified on the invoice shall be considered failure to comply with Item 3 of Clause 12.2 and endorsement will not be granted or will be withdrawn as specified in Clause 12.3, whichever applies.

## **Appendix E Requirements for conducting activities within the scope of the I-RAP (Normative)**

### **E.1 General**

This normative appendix specifies the minimum requirements that I-RAP registered assessors must follow when conducting activities within the scope of the I-RAP.

### **E.2 Advertising and Promotion**

Registered Assessor's and their employer's advertising and promotion of their involvement in the Program shall be clear, truthful and accurate in content and should not be likely to mislead the customer, either by intent or otherwise; I-RAP Endorsement and Registration is restricted to individuals. I-RAP Registered assessors may advertise the fact that they are I-RAP registered. Employers of I-RAP registered assessors must not advertise that their organisation is I-RAP registered. Organisations may advertise that they have I-RAP registered assessors on staff.

Registered Assessors and their employers may, subject to terms and conditions, use the I-RAP Logo in their promotional material. Those intending to do so are required to contact the DSD I-RAP Manager. Contact Details are as follows:

**DSD I-RAP Manager:**

<b>Telephone:</b>	(02) 6265 0339
<b>Facsimile:</b>	(02) 6265 0328
<b>Email:</b>	irap@dsd.gov.au

### **E.3 Provision of services**

#### ***E.3.1 Execution of assessments***

The I-RAP registers individuals to perform specific ICT security functions. The I-RAP registered assessor undertaking a certification assignment within the scope of I-RAP with a view to issuing I-RAP certification must be the person who conducts the I-RAP assessment.

This may be done with limited assistance from other individuals. Limited assistance from others would include aspects such as enlisting the help of individuals related to secretarial or administrative work to support the assessment work of the I-RAP registered assessor or particular subject matter experts to provide expert assistance in the gathering and/or collation of the required data, information or documentation pertinent to a system assessment for assessment by the I-RAP registered assessor. It is the responsibility of I-RAP registered assessors to satisfy themselves that the data, information or documentation provided by those subject matter experts is accurate and appropriate to enable a valid system assessment.

As specified in the DSD assessment guidance checklists, the formal I-RAP certification report includes sign off from the ITSA/ITSM of the Australian Government Dept./Agency or Australian Government Service Provider stating that, to the best of the ITSA/ITSM's knowledge, the I-RAP registered assessor who has signed the certification report has actively participated in conducting the assessment work leading to certification.

All ICT security system assessments undertaken by I-RAP registered assessors with a view to issuing I-RAP certification must be carried out and reported in accordance with Clauses E3.2 to E3.8 inclusive and in compliance with the Infosec-Registered Assessor Program.

### ***E.3.2 Reporting of assessments***

Assessors must provide the following to the Australian Government agency (or others) that has been assessed:

1. The results of all Australian Government agency ICT security system assessments they have carried out in accordance with Clauses E3.2 to E3.7 inclusive and in compliance with the Program, and
2. A DSD ICT security system compliance certificate, created by the assessor from the DSD ICT security system compliance certificate template, where the system meets the compliance requirements of the assessment type concerned.

The DSD system compliance certificate template is available from Documents page of the I-RAP Register of Infosec Assessors at [www.irap.securelink.com.au](http://www.irap.securelink.com.au) (see Clause E.4 for details).

Assessors must inform the DSD I-RAP Manager of the results of all Australian Government agency systems assessments they have carried out in accordance with Clauses E3.2 to E3.7 inclusive and in compliance with the Program. Copies of each assessment result and the DSD ICT security system compliance certificate, if applicable should be sent to:

DSD I-RAP Manager  
C/o Information Security Group  
Defence Signals Directorate  
Locked Bag 5076  
Kingston ACT 2604

### ***E.3.3 Gateway/CDS Assessments***

I-RAP registered assessors undertaking Gateway/CDS certification assignments must abide by the following rules:

1. Assessors must follow the guidance in DSD's Gateway/CDS Certification Checklist when conducting a Gateway/CDS Certification.
2. Assessors will be granted the right to issue Certifications that are consistent with DSD & best practice standards. A standard Certification template will be provided for this purpose (see E.3.1).
3. Assessors will ensure that the external firewall(s) are evaluated and configured and used according to their evaluated configuration. Evaluated configuration can be found on the Evaluated Products List (EPL) (<http://www.dsd.gov.au/Infosec/>) in the Certification Report attached to products that have completed evaluation. Where the firewall(s) are used in a non-evaluated configuration and assessors have sought DSD approval for the firewall(s) as provided for in the Checklist, assessors will ensure this activity and the results are clearly stated in the Checklist.
4. Assessors will ensure that, where appropriate, the Agency/Organisation under review is using evaluated products from DSD's EPL.

5. Assessors will review documentation required for DSD Gateway/CDS Certification. Documentation should be consistent with, and reflect means to implement, the measures identified within the Threat & Risk Assessment. Assessors must verify that potential risks are appropriately referenced and recognised within the Security Policy/Plan and are addressed at a procedural level.
6. Assessors need to verify that no data above the classification of the Gateway/CDS Certification resides on the network behind the gateway under review. For example, if an assessor is conducting an IN-CONFIDENCE Gateway/CDS assessment and ascertains that higher classified data resides on the network then an IN-CONFIDENCE Gateway/CDS Certification cannot proceed. If an assessor is unsure about this matter then they must contact DSD to discuss it before proceeding with the Gateway/CDS Certification.

#### ***E.3.4 Information system assessments***

I-RAP registered assessors undertaking Network/System Assessments must follow the guidelines contained in the *I-RAP System Review Guidelines & Checklist*.

DSD reserves the right to conduct Network/System reviews at IN-CONFIDENCE, PROTECTED, HIGHLY PROTECTED and RESTRICTED levels if it deems it appropriate to do so.

#### ***E.3.5 Gatekeeper assessments***

I-RAP registered assessors undertaking Gatekeeper Assessments must abide by the following rules:

1. Assessors must follow the guidelines contained in the *I-RAP Gatekeeper Guidelines & Checklist*.
2. Assessors must submit a report to DSD according to the reporting instructions contained within the *I-RAP Gatekeeper Guidelines & Checklist*.

#### ***E.3.6 FedLink audits***

I-RAP registered assessors undertaking FedLink Audits must abide by the following rules:

1. Assessors must conduct FedLink audits according to the requirements of the *I-RAP FedLink Audit Guidelines & Checklist*.
2. 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 compliance audit. Once FEDMAC has identified an agency for a FedLink compliance audit an I-RAP registered assessor can be engaged to perform the audit. Audits must be conducted against claims made in the claim for compliance Checklist in the *I-RAP FedLink Audit Guidelines & Checklist*.

#### ***E.3.7 FedLink connection assessments***

FedLink Connection Assessments are to examine if an Agency/Organisation has implemented the appropriate measures for connection to FedLink at PROTECTED level. FedLink Connection Assessments are to be treated as Gateway/CDS Assessments at the PROTECTED level.

**E.3.8 *Physical security reviews***

The PSM states that the responsibility for the certification of physical security measures lies with the Agency's Security Advisor (ASA). While an ASA may, at their discretion, allow an I-RAP registered assessor to undertake the review, only the ASA can certify the measures as appropriate.

**E.4 Provision of the DSD ICT security system compliance certificate template**

As stated in Clause E3.1, the DSD ICT security system compliance certificate template and a sample certificate are available on the Documents page of the RIA. Access to the template is confined to I-RAP registered assessors by the use of document security protection.

It shall be the responsibility of the assessor to ensure that the latest version of the template is used to issue compliance certificates. The certificate template should reside on the RIA and not in personal folders to ensure the latest version is always issued and to maintain security.

The I-RAP Administrator will liaise with the endorsed assessor, when the assessor qualifies for endorsement, to provide a unique combination of AssessorID and password (initially advised by the I-RAP Administrator but the password may be changed by choice of the assessor wherever possible, within the constraints of RIA programming). It shall be the assessor's responsibility to maintain the security of their AssessorID and password. Where the assessor believes their access security has been compromised, the assessor shall advise the I-RAP administrator without delay to arrange for the compromised information to be made inoperative and replacement access security to be issued.

## **Appendix F Withdrawal of endorsement procedures (Normative)**

### **F.1 General**

This normative appendix specifies the procedures for the withdrawal of I-RAP registration.

### **F.2 Handling considerations for withdrawal of I-RAP registration**

Consideration of withdrawal of I-RAP endorsed assessor registration shall be carried out in the following manner:

1. Any advice of items 3 to 9 in Clause 12 applying to an I-RAP endorsed assessor will be reported to the DSD I-RAP Manager and entered in the Complaints and Disputes Log.
2. The assessor against whom the complaint has been made will be advised in writing of the allegations by the I-RAP Administrator and requested to submit a response.
3. Once the response, and any supporting information, has been received the DSD I-RAP Manager will review all relevant material.
4. If deemed necessary the DSD I-RAP Manager, in conjunction with the I-RAP Administrator where appropriate, may interview a complainant (where the consideration arises from a complaint) and/or the I-RAP endorsed assessor, and may seek submissions from third parties.
5. After considering the submissions the DSD I-RAP Manager can make the determination whether to withdraw I-RAP registration.
6. In all cases the I-RAP endorsed assessor will be advised of the outcome of the deliberations in writing. Where an approval is withdrawn the I-RAP Administrator will advise the assessor of the reasons for withdrawal and what action is required for reinstatement.

### **F.3 Notice of withdrawal of I-RAP registration**

Upon completion of the consideration of withdrawal the following operations will be carried out:

1. The details of how the consideration of withdrawal was resolved and when the assessor was advised will be entered in the Complaints and Disputes Log.
2. Details of all endorsements that are withdrawn in accordance with items 3 to 9 of Clause 12.2 will be noted on the register for 12 months after the date of withdrawal, unless the approval is reinstated.

### **F.4 Appeals against withdrawal of I-RAP registration**

If the I-RAP endorsed assessor, or a complainant (where the consideration arises from a complaint) is dissatisfied with the determination, they may lodge an appeal with the Assistant Secretary of the Information Security Group – DSD via the I-RAP Administrator. Such an appeal must be in writing and be within one month of the original decision. Appeals may include additional supporting documentation. (The procedure for handling an appeal will be similar to that of a dispute.)

Following a review, the decision of the Assistant Secretary of the Information Security Group – DSD is final.

## **Appendix G Complaints and dispute procedures (Normative)**

### **G.1 General**

This normative appendix specifies the procedures for handling complaints and disputes.

The resolution of complaints and disputes is confined to complaints about the Program or disputes arising from interactions between candidates or registered assessors and the I-RAP administration. It is anticipated that disputes will originate from candidates disputing application or assessment results provided by the I-RAP and complaints will originate from users of the Program having concerns about the operation of the program or third parties having used the services of I-RAP registered assessors and considering them to be unsuitable for I-RAP endorsement.

### **G.2 Complaints**

#### ***G.2.1 Lodgement of complaints***

Complaints must be lodged in writing, addressed to:

Infosec–Registered Assessor Program Administrator  
C/o SecureLink Pty Ltd  
PO Box 208 Erindale Centre  
Canberra ACT 2903

The complaint must state as clearly as possible what the issues are and what solution is desired.

#### ***G.2.2 Handling of general complaints***

Complaints of a general nature shall be handled in the following manner:

1. When a complaint is received, The I-RAP Administrator will determine if it is legal in nature. If it is legal in nature the procedure in Clause G2.4 will be followed. Otherwise the I-RAP Administrator will enter the details of the complaint in the Complaints and Disputes Log, recording the following:
  - ◆ Date received
  - ◆ The complainant details
  - ◆ The complaint
2. The I-RAP Administrator, in conjunction with the DSD I-RAP Manager where appropriate, will determine whether the complaint has substance.
3. The I-RAP Administrator will then acknowledge receipt of the complaint to the complainant within two weeks of receipt.
4. If the complaint is deemed to be without substance, the complainant will be advised that the complaint has not been upheld, and the reasons supplied. This advice will be recorded in the Complaints and Disputes Log. The complainant may submit a further submission, including subsidiary information addressing the reasons given for the complaint's dismissal. The I-RAP Administrator, in conjunction with the DSD I-RAP Manager where appropriate, will then reconsider the complaint.

5. If the complaint is deemed to have substance, as far as possible, the time frame for resolving the complaint will be agreed with the complainant and this time frame will be recorded in the Complaints and Disputes Log.
6. The I-RAP Administrator, in conjunction with the DSD I-RAP Manager where appropriate, will review the complaint. This review will address the nature of the complaint, the area of concern and the severity of the issue.
7. If deemed necessary the I-RAP Administrator, in conjunction with the DSD I-RAP Manager where appropriate, may interview the complainant and may seek submissions from third parties.
8. If the complaint is taking longer to resolve than agreed, the I-RAP Administrator will advise the complainant and the advice and it was advised will be recorded in the Complaints and Disputes Log.
9. After considering the submissions the I-RAP Administrator, in conjunction with the DSD I-RAP Manager where appropriate, can make the determination as to whether the complaint has or has not been substantiated.
10. In the latter case the complainant is advised in writing (see point 3 above) and the I-RAP Administrator will enter details of the advice and when the complainant was advised in the Complaints and Disputes Log.
11. If the complaint has been substantiated the complainant is advised in writing, setting out the decision and any subsequent consequences and the I-RAP Administrator will enter details of how it was resolved and when the complainant was advised in the Complaints and Disputes Log.

### ***G.2.3 Handling of complaints about I-RAP endorsed assessors***

Complaints about the conduct of I-RAP endorsed assessors shall be handled in the following manner:

1. When a complaint is received, the I-RAP Administrator will enter the details of the complaint in the Complaints and Disputes Log, recording the following:
  - ◆ Date received
  - ◆ The complainant details
  - ◆ The complaint
2. The I-RAP Administrator will acknowledge receipt of the complaint to the complainant within two weeks of receipt.
3. The assessor against whom the complaint has been made will be advised in writing of the allegations and requested to submit a response.
4. Once the response, and any supporting information, has been received the I-RAP Administrator, in conjunction with the DSD I-RAP Manager where appropriate, will review all relevant material.
5. If deemed necessary the I-RAP Administrator, in conjunction with the DSD I-RAP Manager where appropriate, may interview the complainant and/or the I-RAP endorsed assessor, and may seek submissions from third parties.
6. After considering the submissions the I-RAP Administrator, in conjunction with the DSD I-RAP Manager where appropriate, can make the determination as to whether the complaint has or has not been substantiated.

7. In the latter case the complainant and the I-RAP endorsed assessor will be advised in writing (see point 3 above) and the I-RAP Administrator will enter details of the advice and when the complainant and the I-RAP endorsed assessor were advised in the Complaints and Disputes Log.
8. If the complaint has been substantiated, the DSD I-RAP Manager must determine an appropriate level of action. This could include:
  - ◆ A warning.
  - ◆ An audit of the assessor and their activities.
  - ◆ Disciplinary action (may include withdrawal of I-RAP registration).
9. If a warning is decided the I-RAP Administrator will inform the I-RAP endorsed assessor, including suggestions for improvement.
10. If an audit (i.e. gather objective evidence) is considered necessary the DSD I-RAP Manager will initiate the audit and will consider the results of the audit before making a final determination.
11. If the complaint is clear-cut and the I-RAP endorsed assessor has obviously broken their conditions of accreditation, the DSD I-RAP Manager will decide the appropriate level of discipline required.
12. In all cases the complainant and the I-RAP endorsed assessor will be advised of the outcome of the complaint in writing. The details of how it was resolved and when the complainant and assessor were advised will be entered in the Complaints and Disputes Log.

#### ***G.2.4 Legal complaints***

A legal complaint should be considered as any complaint that contains a threat of legal action or brings into question the legality of an I-RAP activity. For example; a complaint that the activity of the I-RAP breaches the Privacy Act would be considered a legal complaint. Where it is unclear whether the complaint is legal in nature, the I-RAP Administrator will seek advice from the DSD Legal Officer (via the DSD I-RAP Manager).

Complaints that are legal in nature shall be handled in the following manner:

1. The I-RAP Administrator will advise the DSD Legal Officer of the complaint immediately.
2. The I-RAP Administrator will then acknowledge receipt of the complaint to the complainant within two working days of receipt and advise that the Program's Legal Officers are dealing with it.
3. The I-RAP Administrator will enter the details of the complaint in the Complaints and Disputes Log, recording the following:
  - ◆ Date received
  - ◆ The complainant details including that it is legal in nature
  - ◆ The complaint
  - ◆ The Legal Officer handling the complaint
4. The Legal Officer will then determine the time frame for a response and personally advise the complainant.
5. Once the Legal Officer has agreed on a resolution, a written description will be provided to the I-RAP Administrator setting out the decision, when the complainant was advised and any subsequent consequences and the I-RAP Administrator will enter details of how it was resolved and when the complainant was advised in the Complaints and Disputes Log.

### ***G.2.5 Complaint appeals***

If either the complainant or the I-RAP endorsed assessor, where involved with a complaint, is dissatisfied with the result they may lodge an appeal with the Assistant Secretary of the Information Security Group – DSD via the I-RAP Administrator. Such an appeal must be in writing and be within one month of the original decision. Appeals may include additional supporting documentation. (The procedure for handling an appeal will be similar to that of a dispute.)

Following a review, the decision of the Assistant Secretary of the Information Security Group – DSD is final.

## **G.3 Disputes**

### ***G.3.1 Advice of disputes***

Disputes must be advised in writing, addressed to:

Infosec–Registered Assessor Program Administrator  
C/o SecureLink Pty Ltd  
PO Box 208 Erindale Centre  
Canberra ACT 2903

This advice must be provided within one (1) month after becoming aware of the action or other matter that is the subject of the dispute. The advice must state as clearly as possible what the issues are and what solution is desired. Where the dispute is appealing a rejection of I-RAP endorsement, the advice should set out the grounds for the appeal, including any counter response to the reasons given for the rejection.

### ***G.3.2 Handling of operational disputes***

Operational disputes shall be handled in the following manner:

1. When advice of a dispute is received, The I-RAP Administrator will determine if it is legal in nature. If it is legal in nature the procedure in Clause G3.3 will be followed. Otherwise the I-RAP Administrator will enter the details of the dispute in the Complaints and Disputes Log, recording the following:
  - ◆ Date received
  - ◆ Details of the party advising the dispute
  - ◆ The dispute and requested solution
2. The I-RAP Administrator will then acknowledge receipt of the dispute to the person lodging the dispute within two weeks of receipt.
3. The means of resolving the dispute will be by discussion between the I-RAP Administrator, in conjunction with the DSD I-RAP Manager where appropriate, and the person lodging the dispute. The I-RAP Administrator will initiate the discussion by contacting the person that provided the dispute advice. A decision to resolve the dispute based on the discussions will then be drafted by the I-RAP Administrator.
4. Once the I-RAP administration and the DSD have agreed on a resolution, a written response will be provided to the person who lodged the dispute within one (1) month, setting out the decision and any subsequent consequences and the I-RAP Administrator will enter details of how it was resolved and when the resolution was advised in the Complaints and Disputes Log.

### ***G.3.3 Handling of disputes against an application or assessment results***

Disputes appealing application or assessment results shall be handled in the following manner:

1. When advice of a dispute is received, the I-RAP Administrator will enter the details of the appeal in the Complaints and Disputes Log, recording the following:
  - ◆ Date received
  - ◆ Details of the party advising the dispute
  - ◆ The dispute and requested solution
2. The I-RAP Administrator will then acknowledge receipt of the appeal to the person lodging the dispute within two weeks of receipt.
3. Within two weeks of receiving the appeal the I-RAP Administrator will contact the DSD I-RAP Manager, providing a copy of the dispute for the DSD's consideration.
4. In addition, the I-RAP Administrator will supply to the DSD I-RAP Manager, as soon as practicable, the original application or test results, as applicable, and all supporting documents.
5. The I-RAP Administrator will have one (1) month to submit any amplification of their decision, including counter arguments to the appellant.
6. Once all material is available, and within two (2) months of the date of the original appeal, the DSD I-RAP Manager will consider the application.
7. Criteria used for consideration will include technical competence, integrity and character, procedural issues and natural justice principles.
8. If deemed necessary the DSD I-RAP Manager may interview the appellant and/or the I-RAP Administrator, and may seek submissions from third parties.
9. After reviewing the appeal, the DSD I-RAP Manager will advise the I-RAP Administrator as soon as possible of its decision.
10. The I-RAP Administrator will advise in writing, to the person lodging the dispute, of the decision and record the decision and provision of any advice in the Complaints and Disputes Log.

### ***G.3.4 Legal disputes***

A legal dispute should be considered as any dispute that contains a threat of legal action or brings into question the legality of an I-RAP activity. For example; a dispute that the activity of the I-RAP impacts on loss of revenue by an assessor, who may seek compensation, would be considered a legal dispute. Where it is unclear whether the dispute is legal in nature, the I-RAP Administrator will seek advice from the DSD Legal Officer (via the DSD I-RAP Manager).

Disputes that are legal in nature shall be handled in the following manner:

1. The I-RAP Administrator will advise the DSD Legal Officer of the dispute immediately.
2. The I-RAP Administrator will then acknowledge receipt of the dispute to the complainant within two working days of receipt and advise that the Program’s Legal Officers are dealing with it.
3. The I-RAP Administrator will enter the details of the dispute in the Complaints and Disputes Log, recording the following:
  - ◆ Date received
  - ◆ The complainant details including that it is legal in nature
  - ◆ The complaint
  - ◆ The Legal Officer handling the dispute
4. The Legal Officer will initiate dispute resolution negotiations by contacting the person that provided the dispute advice.
5. Once the Legal Officer has agreed on a resolution, a written description will be provided to the I-RAP Administrator setting out the decision, when it was resolved and any subsequent consequences and the I-RAP Administrator will enter details of how and when it was resolved in the Complaints and Disputes Log.

#### *G.3.5 Dispute appeals*

If the person lodging the dispute is dissatisfied with the result they may lodge an appeal with the Assistant Secretary of the Information Security Group – DSD via the I-RAP Administrator. Such an appeal must be in writing and be within one (1) month of the original decision. Appeals may include additional supporting documentation.

Following a review, the decision of the Assistant Secretary of the Information Security Group – DSD is final.

End of Document