Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

Guidelines for authorising systems

Conducting accreditations

Accreditation

Accreditation is the process by which an authorising officer formally accepts security risks associated with the operation of a system and authorises it to operate.

Authorising officers

For TOP SECRET systems the authorising officer is Director-General Australian Signals Directorate (ASD), or their delegate.

For SECRET and below systems the authorising officer should be an organisation’s Chief Information Security Officer (CISO), or their delegate. Alternatively, an organisation’s Chief Security Officer (CSO), or their delegate, may be used depending on an organisation’s management structure.

For systems that process, store or communicate sensitive compartmented information the authorising officer is Director-General ASD, or their delegate.

For multinational and multi-organisation systems the authorising officer should be determined by a formal agreement between the parties involved.

For commercial providers providing services to organisations the authorising officer is the CISO of the supported organisation, or their delegate. Alternatively, an organisation’s CSO, or their delegate, may be used depending on an organisation’s management structure.

In all cases, the authorising officer should have an appropriate level of seniority and understanding of security risks they are accepting on behalf of the organisation.

Authorising systems to operate

Accreditation is the process by which an authorising officer formally accepts security risks associated with the operation of a system and authorises it to operate. In some cases however, an authorising officer may not accept all security risks due to individual security risks being inadequately identified and/or security controls being inadequately implemented. In such cases, the authorising officer may request further work be undertaken by the system owner. In the intervening time, the authorising officer may choose to authorise a system to operate for an interim period with caveats placed on its use.

Security Control: 0064; Revision: 7; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Security risks associated with the operation of a system are determined by a security assessment, and formally accepted by an authorising officer, before the system is authorised to operate.

Ongoing security risk management and monitoring

Business requirements and threat environments are dynamic. As such, system owners should ensure that their selection of security controls for systems remain both relevant and effective for their business requirements and the prevailing threat environment.

Regular monitoring of cyber threats, security risks and security controls associated with a system is beneficial in maintaining the security posture of the system; however, specific events may necessitate the system undergoing reaccreditation. These may include:

- changes in security policies relating to the system
- detection of new or emerging cyber threats to the system
- the discovery that security controls for the system are not as effective as planned
- a major cyber security incident involving the system
- major architectural changes to the system.

Security Control: 0809; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
When a change to a system or its environment impacts the security of a system, and is subsequently assessed as having increased its security risk profile, the system undergoes reaccreditation.

Conducting certifications

Certification

Certification is the process by which a security assessment is used to determine the security posture and security risks associated with the operation of a system.

Assessors

Security assessments for TOP SECRET systems can be undertaken by the Australian Cyber Security Centre (ACSC) or Information Security Registered Assessors Program (IRAP) assessors with appropriate security clearances.

Security assessments for SECRET and below systems can be undertaken by an organisation's own assessors or IRAP assessors with appropriate security clearances.

While a security assessment can be conducted by an organisation's own assessors, the organisation may choose to add an extra level of independence by engaging the services of an IRAP assessor.

In all cases, assessors should have an appropriate level of experience and understanding of the security controls and security risks they are assessing.

Security assessments

The purpose of a security assessment is to determine whether security controls for a system have been appropriately identified, implemented and are operating effectively. In conducting a security assessment, it is important that the system owner is aware of the extent of any testing that assessors may undertake in order to manage any risks associated with such activities.

When an assessor is engaged early in a system's development lifecycle, it may be beneficial to perform the security assessment in two phases. Initially to assess the selection and documentation of security controls for the system, and subsequently to assess their implementation. This allows for the identification of security risks earlier in the system's development lifecycle, thereby assisting to reduce the costs associated with any remediation activities.

Security Control: 0904; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Prior to the beginning of a security assessment, the system owner develops a Statement of Applicably (SoA) for their system which identifies the security controls that they have chosen to implement.

Security Control: 1531; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Prior to the beginning of a security assessment, a test plan is developed by assessors in consultation with the system owner.

Security Control: 0805; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
During a security assessment, the system is reviewed by assessors to determine whether security controls in the SoA are appropriate and have been implemented and are operating effectively.

Security Control: 1140; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
At the conclusion of a security assessment, a security assessment report is produced outlining the effectiveness of the implementation of security controls, the system's strengths and weaknesses, any recommended remediation activities, and an assessment of security risks associated with the operation of the system.

Gateway and cloud services

Commercial and government gateway and cloud services selected by the ACSC will need to undergo regular security assessments to determine their security posture and security risks associated with their use.

Security Control: 0100; Revision: 8; Updated: Sep-18; Applicability: O, P; Priority: Must
Commercial and government gateway and cloud services selected by the ACSC undergo a joint security assessment by ACSC and IRAP assessors at least every two years.

Further information

The IRAP website lists the range of activities IRAP assessors are authorised to perform. This information is available at https://www.cyber.gov.au/government/programs/information-security-registered-assessors-program-irap/.