Australian Government
Department of Defence

Defence Industry Security Office

What to expect during an audit

Defence Industry Security Office audits will review your existing security practices and highlight areas where security practices can be strengthened. The key benefit will be an uplift in security.

To assess your security maturity, our auditors must examine – and on some occasions retain for more detailed analysis – evidence of operations, functions, and processes. We also need you to demonstrate to our cyber auditors how ICT security controls are applied.

We ask that you be open and transparent and provide access to documents and assets. We should view each other as trusted partners seeking to improve security.

We've provided some information to help you prepare for an audit below.

What we look for during an audit

Security Governance

The following types of evidence will be sought and reviewed:

- policies, procedures and plans that cover:
  - risk management
  - security governance
  - business security risk assessments
  - security training
  - security incidents
  - insider threats
  - foreign contacts.
- training records, including for:
  - Security Officer training course (Levels 1–3 membership)
  - the security elements of induction training
  - annual security awareness training
  - COMSO training (where relevant).
- registers, including:
  - risk register that includes security considerations
  - security incident register
  - overseas travel register with completed travel forms.
- reports, including:
  - risk management reports, including escalation of serious residual risks
  - assurance program reports
  - annual security report.
- other relevant records, including:
  - Designated Security Assessed Positions (DSAP) list (Levels 1–3 membership)
  - signed acknowledgements of security policy and plans from personnel
  - notifications to Defence of changes affecting membership, including changes in foreign ownership control and influence.

Personnel Security

The following types of evidence will be sought and reviewed:

- confirmation of Security Officer's ability to sponsor security clearances and evidence that they are actively managing cleared personnel, including the Security Officer being nominated as sponsor for personnel.
- policies and procedures that cover:
  - personnel security
  - employment screening
  - ongoing assessment of personnel
  - separating personnel.

Physical security

The following types of evidence will be sought and reviewed:

- policies and procedures that cover physical security
- details of physical security and access controls at each location
- certification and accreditation certificates.

Additionally, a walkthrough will be conducted to verify that the physical security and access controls at each facility are present and functioning.

Information and Cyber Security

The following types of evidence will be sought and reviewed:

- policies and procedures that cover information and cyber security, and define the cyber security standard used to correspond with Defence
- accreditation certificates.

Additionally, a demonstration of key security controls deployed to the relevant network and endpoints that make up that network will be required.

For a more detailed look at what is expected across each of the four security domains, 'Audit Guides' can be found on the DISP DOSD dashboard. To access this dashboard, please contact your Defence contract manager. For further information on the audit process, please contact us at DISO.info@defence.gov.au.