AUSTRALIAN Cyber Collaboration Centre

ISM Fundamentals Training Course Contents

The Australian government **Information Security Manual (ISM)** outlines a cyber security framework that organisations can apply, using a risk management framework, to protect their information and communication technology (ICT) systems from cyber threats. It complements the **Protective Security Policy Framework (PSPF)** produced by the Australian government Attorney-General's department. The ISM and the PSPF provide guidelines and obligations for Commonwealth agencies in implementing appropriate controls in an ICT environment.

In addition, Commonwealth agencies should consider relevant guidance published specifically by or for them. The ISM is published by the Australian Cyber Security Centre (ACSC), the Australian government's lead organisation on national cyber security and a part of the Australian Signals Directorate (ASD). The **Digital Transformation Agency (DTA)** worked with other government bodies and industry to develop the **Cloud Assessment and Authorisation Publication**.

The **Essential Eight publication** provides a **mapping** between the *Essential* Eight Maturity Model and the security controls within the Information Security Manual (ISM). This mapping represents the minimum-security controls organisations must implement to meet the intent of the Essential Eight.

The ISM Fundamentals training provides participants with an introduction to the ISM. Participants will learn about the:

- Australian government Information Security Manual (ISM)
  - Explore the ISM and its sections, guidelines, and security controls and how to interpret the requirements of the ISM
  - How to apply the ISM Cyber Security Principles
  - How to use the ISM for non-Australian Government organisations
- Protective Security Policy Framework (PSPF)
  - How the ISM is used to meet the requirements of the PSPF
- Essential Eight Publication
- Risk Management Framework
  - How to apply risk-based approach to cyber security
- Threat Modelling
- Communication and emanation security threats
- Cryptography

- Sanitisation and Destruction
- Authentication
- Assessing security vulnerabilities and applying patches
- Architectural defences
- Cloud assessment and authorisation
- Choosing a product
- Other relevant documentation and guides

Who should attend this course?

- Chief Information Security Officers (CISOs)
- Chief Information Officers (CIOs)
- Cyber security professionals • Information Technology managers.
- IT Security Advisors of Australian Government Agencies
- IT Security Advisors of organisations supply cyber security products and services to Australian Government Agencies
- Entity Assessors for Australian Government Agencies