Australian Government
Department of Employment and Workplace Relations

DEWR ISMS Scheme Overview

(Information Security Management Systems Scheme)

Disclaimer: *This document is provided for guidance purposes only. It is intended to assist Providers in understanding the department's cyber security accreditation approach and related expectations. It does not replace, amend, or override any contractual, legislative, regulatory, or policy requirements. Accreditation decisions will be based on the department's current accreditation framework, applicable contractual requirements, supporting evidence, and the circumstances of each Provider.*

What is it?

The DEWR ISMS Scheme is a certification standard that helps ensure organisations (known as Providers) delivering employment and skills services for the Australian Government handle personal and sensitive data securely and responsibly. Certification Bodies (CBs) independently assess Providers' Information Security Management Systems (ISMS) against the Scheme's requirements. Providers that meet these requirements can achieve DEWR ISMS Scheme certification. To maintain this certification, Providers must continue to meet the Scheme's requirements at all times. Failure to do so may result in certification being suspended or revoked.

Who is it for?

Certification Bodies (CBs): Accredited auditors (JASANZ-approved) who assess and certify a Providers ISMS.

DEWR (Department of Employment and Workplace Relations): The owner of the scheme.

Category 1 Providers: Australian organisations that assist people in finding jobs or gaining skills who handle sensitive participant or government data during this process. Under the current ESAF and RFFR requirements, Category 2, 3 and 4 Providers do not need to obtain independent certification against the DEWR ISMS Scheme or ISO/IEC 27001.

What does it do?

The DEWR ISMS Scheme sets clear requirements for how Providers are audited and certified for information security, ensuring their ISMS meets both international security standards (ISO/IEC 27001) and DEWR-specific Right Fit For Risk requirements.

The DEWR ISMS Scheme requires that auditors are skilled and experienced, especially with the Australian Government's Information Security Manual (ISM).

Additionally, the Scheme requires Providers to report any security breaches to DEWR within 24 hours.

What is the certification lifecycle?

Certification follows a structured lifecycle designed to assess, maintain, and validate a Provider's information security compliance. The process begins with an application, where the Provider submits key documentation, including security plans, strategies, and details of any previous security incidents. The Certification Body (CB) then reviews the submission and develops an audit plan tailored to the Provider's environment. This is followed by a formal audit of the Provider's Information Security Management System (ISMS) to determine compliance with both DEWR requirements and relevant international standards.

Where compliance is demonstrated, certification is granted and where deficiencies are identified, the Provider must remediate the issues before certification can be achieved. Following certification, ongoing surveillance activities are conducted annually to ensure continued compliance and to review any significant changes to the environment.

To maintain certification, Providers must undergo a comprehensive recertification audit every three years.

Key Takeaways for Providers

To meet the independent certification requirements for Right Fit For Risk (RFFR) Category 1, Providers can choose to obtain and maintain either DEWR ISMS Scheme certification or a valid ISO/IEC 27001 certification that satisfies the applicable requirements. Certification assessments consider compliance with ISO/IEC 27001, including the Annex A control set, as well as applicable Australian Government Information Security Manual (ISM) controls up to the OFFICIAL: Sensitive classification.

In addition, Providers must demonstrate compliance with the RFFR requirements, ensuring that both government-specific security obligations and internationally recognised information security practices are effectively implemented and maintained within their Information Security Management System (ISMS).

Further Information

Further information about the DEWR ISMS Scheme, including certification requirements and approved Certification Bodies, is available on the JASANZ website.

Further information about the Right Fit For Risk requirements is available on the DEWR website or contacting DEWR at SecurityComplianceSupport@dewr.gov.au.