Australian Government
Department of Employment and Workplace Relations

DEWR ISMS Scheme – Issue 3

(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 about?

The DEWR ISMS Scheme helps make sure that organisations (known as Providers) delivering employment and skills services for the Australian Government handle personal and sensitive data securely and responsibly. It does this by setting rules for how Certification Bodies (CBs) check these providers' Information Security Management Systems (ISMS).

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. The DEWR ISMS Scheme is not applicable to Category 2, 3 or 4 Providers.

What does it do?

It sets clear requirements for how Providers are audited and certified for information security, whilst ensuring Providers meet both international security standards (ISO/IEC 27001) and that DEWR-specific requirements (Right Fit For Risk) are met by the ISMS.

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

Additionally, the Scheme mandates that any security breaches are reported within 24 hours to DEWR.

How does certification work?

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 also undergo a comprehensive recertification audit every three years.

Key Takeaways for Providers

Category 1 Providers must obtain and maintain certification, unless they already hold 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 Right Fit For Risk (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

The DEWR ISMS Scheme is available on the JASANZ website.

Information supporting the Right Fit For Risk is available on the DEWR website or by reaching out to DEWR at SecurityComplianceSupport@dewr.gov.au.