Australian Government
Department of Employment and Workplace Relations

DEWR ISMS Scheme - Issue 3

(Information Security Management Systems Scheme)

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.
- **Providers:** Australian organisations that assist people in finding jobs or gaining skills who handle sensitive participant or government data during this process.

What does it do?

- Sets clear requirements for how Providers are audited and certified for information security.
- Ensures Providers meet both international security standards (ISO/IEC 27001) and that DEWR-specific requirements (Right Fit For Risk) are met by the ISMS.
- Requires that auditors are skilled and experienced, especially with the Australian Government's Information Security Manual (ISM).
- Mandates that any security breaches are reported within 24 hours to DEWR.

How does certification work?

1. **Application:** Provider submits details like their security plans, strategies, and past incidents.
2. **Review:** CB checks the application and prepares an audit plan.
3. **Audit:** CB audits the Providers ISMS for compliance with DEWR's standards and international benchmarks.
4. **Certification:** If successful, the Provider gets certified. If not, they must address issues found.
5. **Surveillance:** Ongoing yearly checks and updates.
6. **Recertification:** Every 3 years.

Transition Rules (2025)

- All Providers must move to the latest version of ISO/IEC 27001:2022 as required by the DEWR Scheme Issue 3 by 31 October 2025.
- Existing certificates to earlier versions must be updated during routine audits.

Key Takeaways for Providers

- **Category 1** Providers must be certified (or already have ISO/IEC 27001 certification).
- **Category 2** Providers don't have to be certified but may choose to be.
- Certification considers ISO/IEC 27001 Annex A controls, ISM controls rated up to OFFICIAL: Sensitive, and RFFR Requirements.

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.