Right Fit For Risk (RFFR) – Finding the right sponsor

Background

The RFFR approach applies the international standard relevant to the protection of information assets. ISO 27001 covers the requirements for an Information Security Management System (ISMS).

An ISMS is a systematic approach to managing business information so that it remains secure and available when staff need it. It protects people, facilities and equipment, information and IT systems by applying a risk management process.

Ensuring the ISMS can be properly designed, implemented and operated over time can best be achieved by appointing the right sponsor.

RFFR sponsor

This person needs be sufficiently senior in authority to make decisions for the organisation, oversee the design and implementation of the ISMS and champion a continuous improvement process.

Working collaboratively with people across the organisation, the sponsor should also champion the ISMS to the organisation at the executive level.

Further reading

To find out more about the role of a Security Champion please refer to the following:

- Infosec - What is a Security Champion? Definition, Necessity and Employee Empowerment
- OWASP - https://owasp.org/about/
- Security Intelligence - Empower Your Employees to Become Security Awareness Champions

Need help?

If you require assistance after reviewing these documents, please email your questions to the Security Compliance Support mailbox via SecurityComplianceSupport@dese.gov.au and cc in your Account Manager.