AS/NZS ISO/IEC 27005:2024
ISO/IEC 27005:2022

Australian/New Zealand Standard™

Information security, cybersecurity and privacy protection — Guidance on managing information security risks

AS/NZS ISO/IEC 27005:2024

This Joint Australian/New Zealand Standard™ was prepared by Joint Technical Committee IT-012, Information security, cybersecurity and privacy protection. It was approved on behalf of Standards Australia's Standards Development and Accreditation Committee on 08 November 2024 and by the New Zealand Standards Approval Board on 02 October 2024.

This Standard was published on 22 November 2024.

The following are represented on Committee IT-012:

Australasian Society for Computers and Law
Australian Industry Group
Australian Information Industry Association
Australian Information Security Association
Australian Security Industry Association
Business Continuity Institute Australasia
Consumers' Federation of Australia
CSIRO
Cyber Security Cooperative Research Centre
Department of Defence (Australian Government)
Department of Internal Affairs
Energy Networks Australia
Engineers Australia
ISACA Melbourne
Joint Accreditation System of Australia & New Zealand
Ministry of Business, Innovation and Employment (MBIE)
Monash University
Office of the Victorian Information Commissioner
University of Waikato
University of Wollongong

This Standard was issued in draft form for comment as DR AS/NZS ISO/IEC 27005:2024.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

www.standards.govt.nz

ISBN 978 1 76139 912 1

AS/NZS ISO/IEC 27005:2024
ISO/IEC 27005:2022

Australian/New Zealand Standard™

Information security, cybersecurity and privacy protection — Guidance on managing information security risks

Originated as HB 231:2000.
Previous edition HB 231:2004.
Jointly revised and redesignated as AS/NZS ISO/IEC 27005:2012.
Second edition 2024.

Preface

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT-012 Information security, cybersecurity and privacy protection to supersede AS/NZS ISO/IEC 27005:2012, *Information technology — Security techniques — Information security risk management (ISO/IEC 27005:2011, MOD).*

The objective of this document is to provide guidance to assist organizations to —

(a) fulfil the requirements of AS/NZS ISO/IEC 27001 concerning actions to address information security risks; and

(b) perform information security risk management activities, specifically information security risk assessment and treatment.

This document is applicable to all organizations, regardless of type, size or sector.

This document is identical with, and has been reproduced from, ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*.

As this document has been reproduced from an international document, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

Contents