

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](http://www.standards.org.au)

[www.standards.govt.nz](http://www.standards.govt.nz)

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.

## **COPYRIGHT**

Standards Australia Limited/Standards New Zealand 2024

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth) or the Copyright Act 1994 (New Zealand).

## 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

|  |           |
|--|-----------|
| <b>Preface</b> .....   | <b>ii</b> |
| <b>Foreword</b> .....  | <b>v</b>  |
| <b>Introduction</b> .....  | <b>vi</b> |
| <b>1 Scope</b> .....   | <b>1</b>  |
| <b>2 Normative references</b> .....  | <b>1</b>  |
| <b>3 Terms and definitions</b> .....   | <b>1</b>  |
| 3.1 Terms related to information security risk.....  | 1         |
| 3.2 Terms related to information security risk management.....   | 5         |
| <b>4 Structure of this document</b> .....  | <b>7</b>  |
| <b>5 Information security risk management</b> .....  | <b>7</b>  |
| 5.1 Information security risk management process.....  | 7         |
| 5.2 Information security risk management cycles.....   | 9         |
| <b>6 Context establishment</b> .....   | <b>9</b>  |
| 6.1 Organizational considerations.....   | 9         |
| 6.2 Identifying basic requirements of interested parties.....  | 10        |
| 6.3 Applying risk assessment.....  | 10        |
| 6.4 Establishing and maintaining information security risk criteria.....   | 11        |
| 6.4.1 General.....   | 11        |
| 6.4.2 Risk acceptance criteria.....  | 11        |
| 6.4.3 Criteria for performing information security risk assessments.....   | 13        |
| 6.5 Choosing an appropriate method.....  | 15        |
| <b>7 Information security risk assessment process</b> .....  | <b>16</b> |
| 7.1 General.....   | 16        |
| 7.2 Identifying information security risks.....  | 17        |
| 7.2.1 Identifying and describing information security risks.....   | 17        |
| 7.2.2 Identifying risk owners.....   | 18        |
| 7.3 Analysing information security risks.....  | 19        |
| 7.3.1 General.....   | 19        |
| 7.3.2 Assessing potential consequences.....  | 19        |
| 7.3.3 Assessing likelihood.....  | 20        |
| 7.3.4 Determining the levels of risk.....  | 22        |
| 7.4 Evaluating the information security risks.....   | 22        |
| 7.4.1 Comparing the results of risk analysis with the risk criteria.....   | 22        |
| 7.4.2 Prioritizing the analysed risks for risk treatment.....  | 23        |
| <b>8 Information security risk treatment process</b> .....   | <b>23</b> |
| 8.1 General.....   | 23        |
| 8.2 Selecting appropriate information security risk treatment options.....   | 23        |
| 8.3 Determining all controls that are necessary to implement the information security<br>risk treatment options..... | 24        |
| 8.4 Comparing the controls determined with those in ISO/IEC 27001:2022, Annex A.....                                 | 27        |
| 8.5 Producing a Statement of Applicability.....  | 27        |
| 8.6 Information security risk treatment plan.....  | 28        |
| 8.6.1 Formulation of the risk treatment plan.....  | 28        |
| 8.6.2 Approval by risk owners.....   | 29        |
| 8.6.3 Acceptance of the residual information security risks.....   | 30        |
| <b>9 Operation</b> .....   | <b>31</b> |
| 9.1 Performing information security risk assessment process.....   | 31        |
| 9.2 Performing information security risk treatment process.....  | 31        |
| <b>10 Leveraging related ISMS processes</b> .....  | <b>32</b> |
| 10.1 Context of the organization.....  | 32        |

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

- 
- [Looking for additional Standards? Visit Intertek Inform Infostore](#)
  - [Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation](#)
-