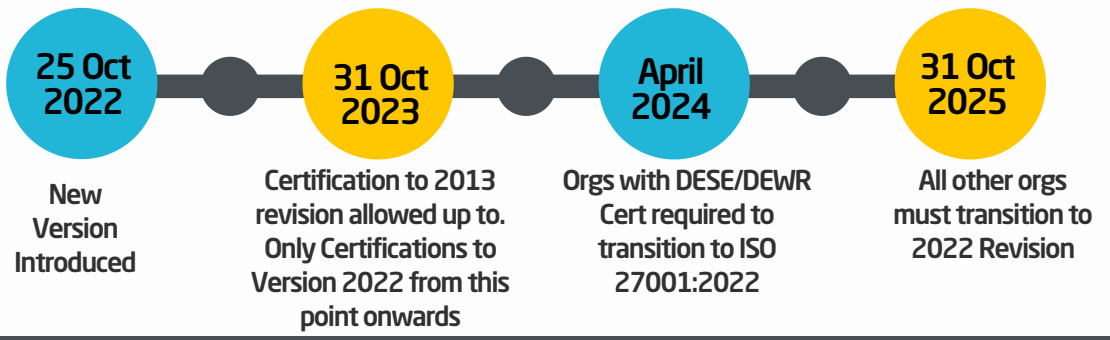# ISO 27001:2022 INFORMATION SECURITY STANDARD

ISO 27001:2022 is the latest standard which has been updated to reflect a strategic investment in information security, offering a comprehensive framework to protect sensitive data, mitigate risks, and enhance overall cybersecurity posture. By adopting the standard, it builds trust with clients, partners, and customers, showcasing a commitment to data protection and provides a robust security management system, ensuring stakeholders that their information assets are well-protected.

KEY CHANGES

There are some key changes between ISO 27001:2022 and ISO I27001:2013 that will need to be addressed to ensure continual compliance.
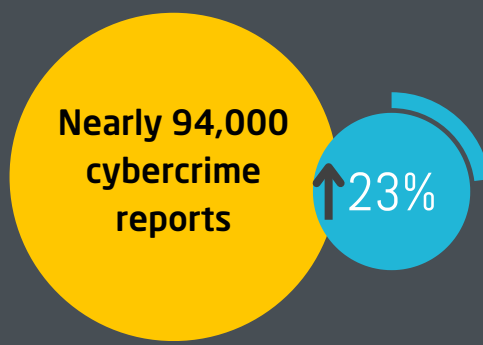
TIMELINE

Australian Orgs that are certified to DESE/DEWR and have ISO27001:2013 will be required to transition to ISO 27001:2022 in 2024 or risk losing certification.
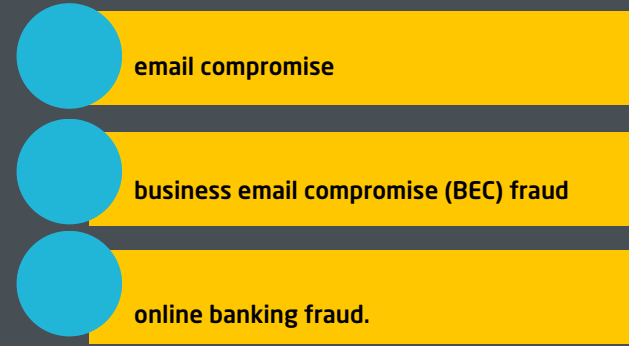
25 Oct 2022
New Version Introduced

31 Oct 2023
Certification to 2013 revision allowed up to. Only Certifications to Version 2022 from this point onwards

April 2024
Orgs with DESE/DEWR Cert required to transition to ISO 27001:2022

31 Oct 2025
All other orgs must transition to 2022 Revision

CYBER STATS AUSTRALIA 2023

Average cost of cybercrime per report

Small business	$46,000
Medium business	$97,200
Large business	$71,600

Nearly 94,000 cybercrime reports

↑ 23%

Top 3 cybercrime types for business
- email compromise
- business email compromise (BEC) fraud
- online banking fraud.
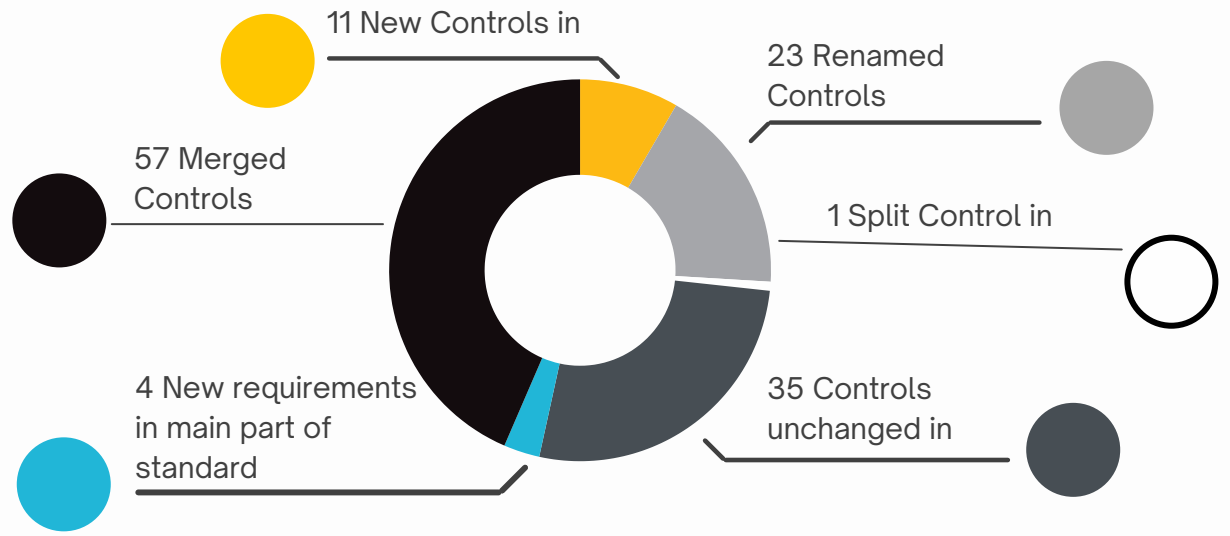
cyber-threat-report-july-2022-june-2023

CHANGES IN ANNEX A

Changes between Revision 2013 and 2022 have been applied Annexure A

- 11 New Controls in
- 23 Renamed Controls
- 57 Merged Controls
- 1 Split Control in
- 4 New requirements in main part of standard
- 35 Controls unchanged in

MAIN CHANGES TO STANDARD

New controls have been added in the following catergories

4.2 Understanding needs of interested Parties	**4.4** Information Security Management Systems
5.3 Organisation RACI	**6.2** Objectives and Planning
6.3 Planning of changes	**7.4** Communication
8.1 Operational Planning and control	**9.3** Management Review
10 Improvement Position of Clauses	

NEW SECURITY CONTROLS

New controls have been added in the following catergories

A.5.7 Threat Intelligence	**A.5.23** Info Sec for use of Cloud Services
A.5.30 ICT Readiness for Business Continuity	**A.7.4** Physical Security Monitoring
A.8.9 Configuration Management	**A.8.10** Information Deletion
A.8.11 Data Masking	**A.8.12** Data Leakage Prevention
A.8.16 Monitoring Activities	**A.8.23** Web Filtering
A.8.28 Secure Coding	

https://saiassurance.com.au/iso-27001