SmartSuite

Framework / Cybersecurity / Other

ASIC Cybersecurity and Risk Management Guidance

ASIC's cyber resilience guidance is a set of good practices, Board questions, and survey reports that help licensees meet their cyber risk obligations.



What it is

ASIC Cybersecurity and Risk Management Guidance is the Australian Securities and Investments Commission's body of cyber resilience resources for the entities it regulates: good practices, key questions for Boards, and reports from its cyber self-assessment surveys. It is not a standalone standard. The obligations that bind licensees to manage cyber risk sit in the Corporations Act 2001, the National Consumer Credit Protection Act 2009, and the ASIC Market Integrity Rules, and ASIC supervises and enforces compliance with them.

At a glance

PUBLISHER
Australian Securities and Investments Commission (ASIC)

TYPE
Guidance

VERSION
ASIC cyber resilience good practices (asic.gov.au/cyber-resilience); latest ASIC Cyber pulse survey Report 776, November 2023

EFFECTIVE
Ongoing; good-practice guidance updated by ASIC reports (latest Report 776, November 2023)

DOMAIN
Cybersecurity

FAMILY
Other

REGION
Australia

INDUSTRY
Financial Services

ADOPTION MODEL
Regulatory Compliance

IMPLEMENTATION COMPLEXITY
High

Source: asic.gov.au/regulatory-resources/cyber-resilience

Why it matters

- **Board questions you can answer** ASIC's key questions for Boards cover the risk management framework, identifying cyber risk, monitoring and escalation triggers, controls, and response.
- **A maturity yardstick** The 2023 cyber pulse survey scored each function from 0 (incomplete) to 4 (optimising); the weighted average across 697 participants was 1.66.
- **A third-party focus** In the 2023 survey 44% of participants did not manage third-party or supply chain risk, so supplier oversight is a visible expectation.
- **Tested response plans** ASIC says an incident response plan should be tested and updated regularly and should identify regulatory reporting obligations and interactions with critical third parties.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ASIC Cybersecurity Guidance

Obligations and good practices register

Record the license obligations that drive cyber duties and the good practices ASIC lists, each with an owner.

Board questions tracker

Turn ASIC's key questions for Boards into recurring agenda items with answers and review dates.

Six-function maturity assessment

Score governance and risk management, identify, protect, detect, respond, and recover on the 0 to 4 scale and track improvements.

Third-party risk

Track suppliers with access to confidential information and their cyber controls using Third Party Risk Management.

Response plan testing

Schedule response plan tests, record results, and log the regulatory reporting steps that each plan identifies.

Board and maturity reporting

Use Enterprise Reporting for Board-level cyber risk and maturity views.

Common framework mappings

APRA CPS 234 | CIS Controls v8.1 | EU DORA | ISO 27001:2022 | MITRE ATT&CK | NIST CSF 2.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

ASIC Cybersecurity and Risk Management Guidance

Provides principles for strengthening cybersecurity and managing technology risks within Australian financial regulations.

asic.gov.au/regulatory-resources/cyber-resilience

ASIC Regulatory Guide 104 - Licensing: Meeting the general obligations

Outlines general obligations for financial services licensees, including risk management and cybersecurity.

asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-104-licensing-meeting-the-general-obligations

ASIC Regulatory Guide 133 — Funds management and custodial services: Holding assets

Sets minimum standards for asset holders, including the systems and controls for holding scheme assets.

asic.gov.au/regulatory-resources/find-a-document/regulatory-guides/rg-133-funds-management-and-custodial-services-holding-assets

Frequently asked questions

Is ASIC's cybersecurity guidance mandatory?

The guidance itself is not law. The obligations to manage cyber risk come from the Corporations Act 2001, the National Consumer Credit Protection Act 2009, and the ASIC Market Integrity Rules, and ASIC says it will take enforcement action when an AFS licensee does not meet them.

Which ASIC documents should a licensee read first?

RG 104 AFS licensing: Meeting the general obligations, Report 429 Cyber resilience: Health check (Section D and Appendix 2), the cyber resilience good practices, the key questions for Boards, and Report 776 for the latest survey findings.

What are the six functions in ASIC's cyber pulse survey?

Governance and risk management, identifying information assets, protecting information assets, detecting cyber security events, responding to cyber security incidents, and recovering from them. Maturity is scored from 0 (incomplete) to 4 (optimising).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What did ASIC's 2023 cyber pulse survey find?

Across 697 participants the weighted average maturity score was 1.66 out of 4. 44% did not manage third-party or supply chain risk, 33% had no cyber incident response plan, 58% had limited or no capability to protect confidential information adequately, and 20% had not adopted a cyber security standard.

Does ASIC require a specific framework such as NIST?

No. ASIC's good practices came from self-assessments against the NIST Cybersecurity Framework, and it says an entity should adopt a cyber security standard proportionate to its size, nature, and complexity.

License included / downloadable: Yes ASIC cybersecurity guidance and regulatory materials are publicly available through the Australian Securities and Investments Commission.

Full framework page and mappings: smartsuite.com/frameworks/asic-cybersecurity-and-risk-management-guidance

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.