SmartSuite

Framework / Cybersecurity / Other

ASIC Cybersecurity and Risk Management Guidance

ASIC Cybersecurity and Risk Management Guidance helps Australian financial sector entities strengthen cybersecurity and meet regulatory obligations.

What it is

ASIC Cybersecurity and Risk Management Guidance is a regulatory framework that assists organizations in strengthening cybersecurity practices, managing technology risks, and supporting compliance with Australian financial regulations. This guidance provides principles and expectations to help entities within the financial sector protect systems and sensitive data from cyber threats.

Developed and published by the Australian Securities and Investments Commission (ASIC), the guidance targets regulated entities such as financial services providers, market operators, and licensees. It covers key areas including security controls, risk assessment, incident response, ongoing monitoring, governance, and regulatory compliance obligations.

At a glance

PUBLISHER Australian Securities and Investments Commission (ASIC)	TYPE Guidance	VERSION Current ASIC cybersecurity and technology risk management guidance
EFFECTIVE 2023	DOMAIN Cybersecurity	FAMILY Other
REGION Australia	INDUSTRY Financial Services	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: https://www.asic.gov.au/regulatory-resources/

Why it matters

- **Strengthen cybersecurity oversight** Increase board and executive accountability for managing technology risks and prioritizing information security investments.
- **Enhance regulatory compliance** Ensure organizational practices remain consistent with evolving Australian financial regulations and supervisory expectations.
- **Promote operational resilience** Reduce the impact of cyber incidents by establishing robust processes for response, recovery, and continued business operations.
- **Improve threat detection and response** Enable faster identification and containment of cyber threats through enhanced monitoring and incident response capabilities.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports ASIC Cybersecurity Guidance

Governance and Accountability Hub

Track roles, oversight, policies, and recurring reporting for technology and cyber risk.

Risk Assessments and Treatment Plans

Run cyber and operational risk assessments and manage mitigations through closure.

Third-Party and Outsourcing Oversight

Manage vendor due diligence, contracts, monitoring, and contingency planning evidence.

Control Testing and Assurance Cadence

Schedule testing, capture results, and track remediation with verification.

Incident Response and Resilience Workflows

Run incidents and exercises with documented timelines, decisions, and improvements.

Supervisory Readiness Reporting

Provide leadership-ready reporting on posture, gaps, and remediation progress.

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 - Managed investments: Scheme property arrangements

Defines requirements for managed investment schemes, emphasizing cybersecurity and risk management practices.

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

Frequently asked questions

What is ASIC Cybersecurity and Risk Management Guidance used for?

ASIC Cybersecurity and Risk Management Guidance is designed to help financial sector organizations strengthen cybersecurity practices and manage technology risks. It supports compliance with Australian financial regulations and sets expectations for protecting critical systems and sensitive data from cyber threats.

Is compliance with ASIC Cybersecurity and Risk Management Guidance mandatory?

While ASIC's guidance itself is not legislation, regulated entities such as financial services providers, licensees, and market operators are expected to align with its principles under their statutory obligations. Non-compliance may result in regulatory scrutiny, enforcement action, or legal consequences.

Who does ASIC Cybersecurity and Risk Management Guidance apply to?

The guidance applies primarily to entities regulated by ASIC, including financial services providers, credit licensees, market participants, and operators. It is relevant to any organization under ASIC's jurisdiction that manages technology risk or handles sensitive financial information.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What security controls and risk management activities does the guidance require?

ASIC expects organizations to implement governance structures, risk assessments, security controls, incident response plans, ongoing monitoring, and third-party risk management. Control areas include access management, threat detection, vulnerability management, and continuous security improvements.

How do organizations implement ASIC Cybersecurity and Risk Management Guidance?

Implementation involves integrating risk management into governance processes, conducting regular risk assessments, mapping controls to ASIC expectations, and developing incident response and monitoring capabilities. Organizations must document procedures, test plans, and review their cybersecurity posture regularly.

How does ASIC Cybersecurity and Risk Management Guidance relate to other cybersecurity frameworks?

ASIC's guidance complements broader standards such as ISO 27001 or the NIST Cybersecurity Framework. Organizations often map ASIC requirements to these frameworks to harmonize risk management and meet both regulatory and international expectations.

What are the ongoing compliance requirements for ASIC Cybersecurity and Risk Management Guidance?

Ongoing compliance involves continuous monitoring of security controls, regular risk assessments, maintenance of incident response capabilities, audit preparation, and prompt reporting of material incidents to ASIC. Organizations must keep evidence of compliance activities and address identified deficiencies.

How would SmartSuite support ASIC Cybersecurity and Risk Management Guidance?

SmartSuite streamlines the management of ASIC guidance by enabling organizations to track risks, manage control libraries, automate evidence collection, and support audit processes. It provides dashboards for monitoring compliance posture, facilitates incident logging, and generates reports required for regulatory oversight.

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 Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.