Information Security Strategy

IT Security Strategy | Global

Version 2.0 · July 2026 · Confidential — Internal Use

This document is a template intended to be reviewed, tailored and approved by your organisation before use.
Replace all references to “the Company” with your organisation’s name.

Document Control

Document name	Information Security Strategy
Document type	IT Security Strategy
Jurisdiction	Global
Owner	Chief Information Security Officer
Approved by	Board of Directors
Version	2.0
Effective date	July 2026
Review cycle	Annual
Next review due	July 2027
Classification	Confidential — Internal Use

Contents

1. Purpose

This Information Security Strategy sets the Company's three-year direction for protecting the confidentiality, integrity and availability of its information assets. It is the forward-looking companion to the Company's Information Technology Security Policy and supporting standards: where the policy suite states the controls the Company requires today, this Strategy states where the Company's information security capability must be in three years, why, and the sequenced investments that will get it there.

The Strategy exists to ensure that the Company's security capability keeps pace with the size and extent of the threats to its information assets — the expectation embedded in ISO/IEC 27001:2022, the NIST Cybersecurity Framework 2.0 and the cyber resilience guidance of the Financial Stability Board and the Basel Committee — rather than merely maintaining the controls of the past. It translates the Board's risk appetite for information security into a target state, a set of strategic pillars, a year-by-year initiative roadmap, an investment and resourcing approach, and the metrics by which the Board will judge progress.

This Strategy is approved by the Board of Directors and owned by the Chief Information Security Officer (CISO). It must be read together with the Information Technology Security Policy, the IT Risk and Security Governance Framework, the Risk Appetite Statement, the Operational Risk Policy and the Business Continuity Plan. The Company's IT Strategy is a separate document the Company must produce and maintain; it does not form part of this policy suite. Where this Strategy and the Information Technology Security Policy differ on a current control requirement, the policy prevails; where they differ on future direction, this Strategy prevails.

2. Scope

This Strategy applies to the Company and all of its controlled entities, and to all information assets owned, operated or used by the Company, including assets managed by third parties and related parties on the Company's behalf. It covers all environments — on-premises, cloud, software-as-a-service and end-user computing — and all channels through which the Company transacts with customers, counterparties and regulators.

The Strategy binds all directors, employees, contractors and secondees in respect of the strategic priorities and investment decisions it establishes. Delivery obligations fall principally on the CISO, the Chief Information Officer (CIO), the Chief Risk Officer (CRO) and the executives accountable for each strategic pillar as recorded in section 11.

- In scope: strategic direction, target state, maturity assessment approach, strategic pillars and roadmap, investment and resourcing approach, strategy-level metrics and Board reporting, and governance of the Strategy itself.
- Out of scope: detailed control requirements (Information Technology Security Policy and standards), incident response procedures (the Cyber Incident

Response Plan, a separate document the Company must produce), business continuity arrangements (Business Continuity Plan), and enterprise technology direction beyond security (the Company's IT Strategy, likewise a separate document the Company must produce).

Jurisdictional application. This Strategy states international best practice drawn from the frameworks listed in the Regulatory Framework section. The Company must map the requirements and commitments of this Strategy to the laws and regulatory requirements of each jurisdiction in which it operates — including licensing conditions, incident notification deadlines, data protection and data-residency requirements — and where the law of an operating jurisdiction imposes a stricter or additional requirement, local law prevails.

3. Definitions

Term	Definition
Information Asset	Information in any form and the technology that stores, processes or transmits it, including data, software, hardware, network infrastructure, cloud services, supporting infrastructure and physical records, whether managed by the Company or by a related party or third-party service provider on its behalf.
Information Security Capability	The totality of resources, skills, controls, governance and management arrangements the Company maintains to preserve the confidentiality, integrity and availability of its information assets and to prevent, detect and respond to information security incidents, commensurate with the size and extent of the threats to those assets.
Cyber Resilience	The Company's ability to anticipate, withstand, contain and rapidly recover from cyber incidents while continuing to deliver its critical operations within Board-approved tolerance levels.
Strategic Pillar	One of the small number of enduring themes or multi-year programmes of work through which the Company organises its objectives and initiatives over the planning horizon and moves from its current state to its target state.
Maturity Assessment	A structured evaluation of the Company's security capability against a recognised model, in this Strategy the NIST Cybersecurity Framework 2.0 supported by ISO/IEC 27001:2022, producing an evidenced current-state rating and gap

	analysis.
Target State	The security posture, maturity ratings and capability set the Company intends to reach by the end of the three-year horizon of this Strategy.
Zero Trust	A security architecture and design approach in which no user, device or network location is implicitly trusted, and in which every access request is authenticated, authorised, encrypted and continuously evaluated against policy regardless of its origin.
Least Privilege	The principle that each identity, including users, service accounts and systems, is granted only the minimum access rights necessary to perform its authorised function, and for no longer than required.
Defence in Depth	The layering of independent preventive, detective and responsive controls so that the failure of any single control does not result in compromise.
Security Operations Centre (SOC)	The function (internal, outsourced or hybrid) that monitors security telemetry, triages alerts and initiates incident response on a continuous basis.
Data Loss Prevention (DLP)	Controls that discover, classify and monitor sensitive data and prevent its unauthorised movement outside approved channels.
Privileged Access	Access rights that exceed those granted to a standard user, including administrative rights over systems, networks, databases, security controls or cloud tenancies, break-glass and emergency accounts, and the ability to access bulk customer data.
Ransomware	Malicious software that encrypts or otherwise denies access to systems and data, typically combined with extortion demands and, increasingly, with data theft.
Data Extortion	The theft of sensitive data accompanied by a threat to publish, sell or notify affected parties unless payment is made, whether or not systems are also encrypted.
Supply-Chain Attack	A compromise achieved through a third-party product, service, software component or managed provider rather than by direct attack on the Company.
Material Information Security Incident	An information security incident that has

	materially affected, or has the potential to materially affect, financially or non-financially, the Company or the interests of its depositors, customers or other stakeholders, and which is therefore notifiable to the Company's prudential regulator or other authorities within the timeframe prescribed by applicable local law.
Material Service Provider	A third party, including an intra-group provider, on which the Company relies to deliver a critical operation or to manage a material risk, or whose failure or compromise would otherwise expose the Company to material operational, financial, technology or compliance risk, together with material subcontractors in its supply chain, as recorded in the Company's service provider register.
Cloud Security Posture Management (CSPM)	Tooling and processes that continuously assess cloud tenancy configurations against secure baselines and detect drift or exposure.
Threat-Led Penetration Testing	Controlled adversarial testing (including red-team exercises) that emulates the tactics of threat actors relevant to the Company in order to test prevention, detection and response end to end.
Security Culture	The shared attitudes, knowledge and behaviours of staff that determine how security is practised day to day, beyond formal controls and training completion.

4. Regulatory Framework

The key legislation, regulations and standards relevant to this document include (as amended from time to time):

Instrument / Standard	Relevance
ISO/IEC 27001:2022 Information Security Management Systems	The international benchmark for the Company's information security management system; this Strategy's target state includes an ISMS aligned to (or certified against) ISO/IEC 27001:2022.
ISO/IEC 27002:2022 Information Security Controls	The reference catalogue of controls used when setting control baselines, assessing gaps and specifying the outcomes of each strategic pillar.
NIST Cybersecurity Framework 2.0	The capability model against which the

End of preview

This is a preview extract. The complete document continues beyond the pages shown here.

The full document is supplied as a single, fully editable Microsoft Word (.docx) file immediately after purchase — including every remaining section, the definitions, the regulatory framework references and all appendices and templates.

Bracketed prompts such as [30 days] mark the points where your own thresholds, committee names and local regulatory references are inserted.

finance-policies.com