IT Risk and Security Governance Framework

IT Risk Framework | 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	IT Risk and Security Governance Framework
Document type	IT Risk Framework
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 IT Risk and Security Governance Framework (the framework) describes the architecture through which the Company governs technology and information security risk. It defines how technology risk is identified, assessed, controlled, assured, reported and escalated; who is accountable at each level; which forums exercise oversight; and how the supporting suite of strategies, policies, control standards and procedures fits together. It is a framework document: it establishes structures, accountabilities and interactions, and deliberately does not prescribe detailed control requirements, which are set in the subordinate documents identified in the Document Hierarchy section.

The framework exists to give the Board confidence that technology risk is managed within the appetite it has set; to give effect to the governance requirements of ISO/IEC 27001:2022 (Clauses 4-10) and the Govern function of the NIST Cybersecurity Framework 2.0; to apply the Basel Committee's Principles for Operational Resilience and for the Sound Management of Operational Risk to the Company's technology estate; and to ensure that accountability for technology and information security outcomes is clearly allocated, including under any senior manager accountability regime applicable in the Company's jurisdiction(s).

This framework is approved by the Board of Directors on the recommendation of the Board Risk Committee. It is owned by the Chief Information Security Officer, who must maintain it, monitor its operation and bring it back to the Board for re-approval at least annually or on any material change.

2. Scope

This framework applies to the Company and all of its subsidiaries and controlled entities, and to all directors, employees, contractors, secondees and consultants. It governs all technology and information security risk arising from information assets owned, operated or used by the Company, wherever located, including assets managed by related parties, third-party service providers and cloud service providers.

The framework covers all environments (production, non-production and development), all delivery channels, end-user computing, operational technology supporting premises and infrastructure, and technology supporting critical operations. It applies to technology change and project activity as well as business-as-usual operations.

The framework governs how technology risk is managed; it does not itself set control requirements. Detailed security controls are set in the Information Technology Security Policy, the IT Security Policy control standards and the IT Staff and Contractor Security Policy; strategic direction for the security capability is set in the Information Security Strategy. Enterprise-wide risk requirements that are not specific to technology remain governed by the Risk Management Framework and the Operational Risk Management Framework. Financial risks

(credit, market, liquidity) are out of scope except where technology failure is the cause of exposure.

Jurisdictional application: this framework states international best practice drawn from the standards cited in the Regulatory Framework section. The Company must map its requirements to the law and regulatory expectations of each jurisdiction in which it operates, including local licensing, outsourcing, data protection, data residency, incident notification and critical infrastructure obligations, and where local law or a local regulator imposes a stricter requirement, that stricter requirement prevails.

Materiality: for the purposes of this framework, a matter is material where it is an incident classified Severity 1 or Severity 2 under the Interaction with Incident Management, BCM and Operational Resilience section, affects a critical operation or a material service provider, involves personal data of more than [insert number] individuals, exceeds a financial impact of [insert amount under applicable local law], or is reasonably likely to require notification to a regulator in any operating jurisdiction. The Chief Information Security Officer must maintain the materiality thresholds as an appendix to this framework, approved annually by the Board Risk Committee, and they apply wherever this framework refers to a material change, control failure, incident or arrangement.

3. Definitions

Term	Definition
Technology risk	The risk of loss, disruption, regulatory breach or reputational damage arising from the failure, compromise, inadequacy or unavailability of information technology assets, systems, data or the processes and people that support them.
Information Security	The preservation of the confidentiality, integrity and availability of information assets and of the systems that store, process or transmit them, achieved through the application of governance, people, process and technology controls, consistent with ISO/IEC 27001:2022.
Information security management system (ISMS)	The set of interrelated policies, processes, roles and resources through which the Company establishes, implements, maintains and continually improves information security, structured on ISO/IEC 27001:2022.
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.
Critical Operation	An activity, process or service performed by the Company, or by a service provider on its behalf, which, if disrupted beyond the Company's impact tolerance, would cause material harm to depositors, customers or counterparties, pose a risk to the Company's safety and soundness, or impair its role in the financial system, consistent with the BCBS Principles for Operational Resilience.
Impact Tolerance	The Board-approved maximum level of disruption to a critical operation that the Company is willing to accept, assuming severe but plausible scenarios, expressed at a minimum as the maximum period of disruption, the maximum extent of data loss, and the minimum service level to be maintained while operating during disruption.
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.
Risk Appetite	The aggregate level and types of risk the Board is willing to accept, or to avoid, within the Company's risk capacity and in pursuit of its strategic objectives and business plan, as articulated in the Risk Appetite Statement consistent with the Financial Stability Board Principles for an Effective Risk Appetite Framework.
Inherent Risk	The level of risk inherent in an activity, process, function or auditable unit before taking into account the mitigating effect of any controls, assessed by reference to the likelihood of the risk occurring and the impact if it did.
Residual Risk	The level of risk that remains in an activity, process, function or auditable unit after taking into account the design and operating effectiveness of the controls that mitigate it.
Control	A policy, process, procedure, system,

	configuration, device, organisational arrangement or other practice designed and operated to maintain or modify risk, including preventive measures that stop a risk event or an instance of non-compliance from occurring and detective and corrective measures that identify it and reduce its impact.
Control library	The Company's authoritative register of technology and information security controls, recording each control's objective, owner, criticality, mapped risks and obligations, and assurance results.
Statement of Applicability	The document, maintained under ISO/IEC 27001:2022, recording which controls the Company has selected for its ISMS, the justification for their inclusion or exclusion, and their implementation status.
Key Risk Indicator (KRI)	A quantified, forward-looking metric with defined thresholds or tolerance levels used to monitor changes in the level or trend of a risk exposure or in control effectiveness, and to trigger escalation and management action where risk appetite may be approached or breached.
Three lines of accountability	The Company's model for allocating risk management responsibility: risk ownership and control operation (first line), risk oversight and challenge (second line), and independent assurance (third line).
Technology and Security Steering Committee (TSSC)	The executive management forum, referred to in this framework as the [Technology and Security Steering Committee], accountable for day-to-day governance of technology and security risk. Replace with the Company's actual forum name.
Obsolescence	The state of a technology asset that is no longer supported by its vendor or the Company, no longer receives security patches, or can no longer meet business or regulatory requirements.
Attestation	A formal written confirmation by an accountable individual or staff member that, to the best of their knowledge after due enquiry, stated obligations, controls or requirements have been met for their area of responsibility during the relevant period, or that a document has been read and understood or remains current,

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